

# LAW ENFORCEMENT INTELLIGENCE

A Guide for  
State, Local, and Tribal  
Law Enforcement  
Agencies

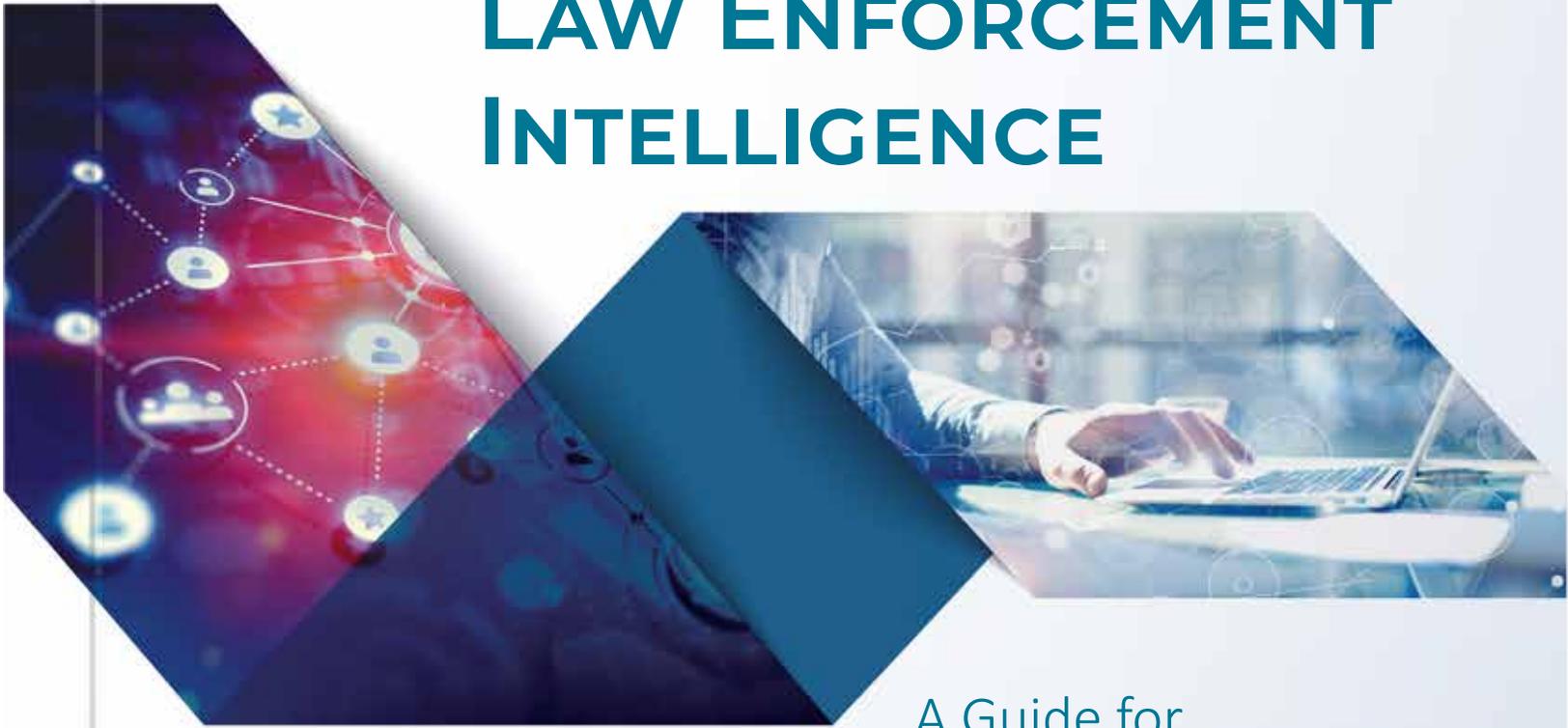
*Third Edition*

David L. Carter, Ph.D.  
Michigan State University  
Institute for Intergovernmental  
Research



This project was supported by Grant No. 2017-D6-BX-0001 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice and the U.S. Department of Homeland Security.

# LAW ENFORCEMENT INTELLIGENCE



*Third Edition*

A Guide for  
State, Local, and Tribal  
Law Enforcement  
Agencies

David L. Carter, Ph.D.  
Michigan State University  
Institute for Intergovernmental Research

Copyright © 2022 by David L. Carter. All rights reserved.

The opinions expressed in this document are the author's own and are not necessarily the view or policy of the U.S. Department of Homeland Security (DHS), the U.S. Department of Justice (DOJ), or the Institute for Intergovernmental Research (IIR).



# EXECUTIVE SUMMARY

The first edition of the Intelligence Guide was prepared in the aftermath of the September 11, 2001, terrorist attacks and was intended to provide guidance to law enforcement agencies across the country on the role of an intelligence capacity and how to develop that capacity. Not surprisingly, it had a strong counterterrorism focus. The second edition of the guide reflected a significant number of developments and changes that occurred over the five years since the first edition was published. Significantly more developments in the domestic intelligence enterprise were reflected in that edition, including a much broader focus on intelligence applications. Despite the evolution, the intent of the Intelligence Guide remains the same: to be a policy-oriented discussion of current initiatives, national standards, and best practices for law enforcement intelligence in state, local, and tribal agencies.

The reader should note that, as the title implies, the information and perspectives in this guide are focused on state, local, and tribal law enforcement (SLTLE) practices, policy, law, and applications. Some U.S. government or federal definitions and practices are not used because they do not have the same applicability to SLTLE. Similarly, the common acronym referring to state, local, tribal, and territorial (SLTT) is not used because there are regulations, policies, and practices that apply somewhat differently to territorial law enforcement agencies; those agencies should refer to local sources, particularly on the law and associated regulations.

**Chapter 1** provides definitions and context for the current state of the domestic intelligence enterprise for law enforcement. It also provides a discussion of homeland security—or “all-threats, all-hazards”—intelligence, crime

gun intelligence, forensic intelligence, gang intelligence, and fire service and public health/medical intelligence. The discussion provides context between law enforcement intelligence and the Intelligence Community while demonstrating intelligence applications for different types of crimes and illustrating their relationships to crime analysis.

**Chapter 2** is a historical perspective that has multiple purposes. First, it provides a discussion of past abuses by law enforcement intelligence. It is important to understand the problems of the past to prevent them in the future. Next, this chapter provides a framework for national recommendations and professional standards for the practice of intelligence. Finally, the discussion identifies the various working groups and committees that are framing the current intelligence model and the relationship of those groups to federal agencies and professional law enforcement organizations.

Fundamental to all types of intelligence is a system for managing the information flow for analysis. This is alternately called the intelligence process or the intelligence cycle. **Chapter 3** is a descriptive discussion of each phase of the intelligence cycle and the processes as they apply to law enforcement agencies. While there are different models for the intelligence process, this discussion relies on the model used in the *National Criminal Intelligence Sharing Plan*.

**Chapter 4, Technology and Intelligence**, is a new chapter in the third edition. While recognizing the wide range of technology that has been used in law enforcement intelligence for decades, this chapter provides a five-point model for technological applications in intelligence, with a core focus on new and emerging technological applications ranging from different forms of networking to advancements in information collection/surveillance technologies and the use of artificial intelligence for different types of information analysis. Beyond the use of these technologies, both legal and ethical concerns about their use are also examined.

Recommendations from the *National Criminal Intelligence Sharing Plan* and various professional organizations have urged law enforcement agencies to adopt intelligence-led policing (ILP). The challenge, however, is that there is no universally accepted definition or process for understanding and implementing ILP. **Chapters 5 and 6** amalgamate the diverse literature on ILP to provide a holistic view. Chapter 5 focuses on the concept of ILP as it applies to American law enforcement, with a perspective on the British approach, from which the concept originated. The chapter also includes a discussion from the latest empirical research on ILP. Chapter 6 focuses on the organizational and administrative processes for the implementation of ILP.

There is no issue more topical (or more controversial) in law enforcement intelligence than the protection of privacy, civil rights, and civil liberties (P/CRCL). **Chapter 7** provides a broad examination of the issues by identifying the concerns expressed by community members and illustrating some of the problems facing intelligence operations through the use of two federal civil rights cases. Integrated in the chapter is a detailed discussion of 28 CFR Part 23 and its application for placing information that identifies individuals or organizations in a criminal intelligence records system. The discussion expands the issues further by a detailed discussion of intelligence records and civil rights liability as well as a discussion of First and Fourth Amendment issues of collecting information from social media for the intelligence process. The chapter ends with a discussion on how a law enforcement agency can immunize itself against civil rights lawsuits related to the intelligence function.

As a mechanism to enhance widespread information sharing among SLTLE agencies, the intelligence fusion concept rapidly grew. Fusion centers have not only grown, but they have matured to become critical primary intelligence and information resources for law enforcement agencies. **Chapter 8** describes the fusion concept and the processes by which a fusion center operates. This chapter also addresses the concerns that critics have expressed about fusion centers in addition to a review of the scientific research on the effectiveness of fusion centers.

Every major national standard for intelligence—the *National Criminal Intelligence Sharing Plan*, the *Fusion Center Guidelines*, *Baseline Capabilities for State and Major Urban Area Fusion Centers*, the *Information Sharing Environment Implementation Plan* and the Department of Homeland Security’s *Target Capabilities List*—has recommended establishing a public-private partnership (PPP) for information sharing to support the intelligence function. Few, however, have established a substantive information sharing relationship with the private sector. There are difficult hurdles to establish such a relationship; however, it is certainly possible. **Chapter 9** discusses the recommendations, issues, processes, and illustrations for making public-private partnerships for intelligence (P3I) a reality.

At the heart of all intelligence activities is the need to manage a wide array of information. A number of critical issues in this process are important to understand. **Chapter 10** provides a comprehensive discussion of these issues, relying on best practices and national standards. In a logically organized approach, the key topics discussed are suspicious activity reporting (SAR); the information collection process, including the development of a collection plan; defining intelligence requirements and their role; the role of analysis (from a consumer’s perspective); and intelligence outputs. With the increase of different information sharing initiatives, one of the challenges has been to ensure that the right information gets into the hands of the right people, who can use the information to develop policy and operational responses. This chapter includes a discussion of information sharing practices to avoid.

Directly building on the material of Chapter 10 and given the increased emphasis on identifying threats, notably from school shootings and mass violence, this edition has a new discussion on *threat assessments* in **Chapter 11** followed by a discussion of *intelligence products*, including options for products. The purpose and processes for conducting threat assessments and how to communicate those findings are discussed.

Open sources have long been used in the intelligence process, and the growth of networking has made open sources even more valuable to the intelligence process. Moreover, since the last edition of the Intelligence Guide, social media has exploded as a potential treasure trove of important raw information, while crime on the Darknet has increased exponentially. These issues are discussed in detail in **Chapter 12**, along with a discussion of using open source information as “the source of first resort” in any intelligence endeavor. The reasons are that open sources are easier and faster, pose less risk to civil rights, and are less controversial for the agency.

There is a wide—and confusing—array of federal intelligence resources: networks, systems, analytic services, processes, applications, and products available to SLTLE that seem to constantly evolve. Many have a specialized expertise or limited area of application, while others are very broad in their application. **Chapter 13** discusses federal intelligence resources, starting with a discussion of classified information, including a description of the process for an SLTLE officer to obtain a federal security clearance. Most law enforcement officers, however, will not have clearances and will be dealing with Sensitive But Unclassified (SBU) information. Hence, a discussion is provided with the meaning and rules for SBU information sharing. Importantly, SBU information is going through a transition to be categorized as Controlled Unclassified Information (CUI). This is a U.S. governmentwide transition that has some distinct issues for sharing and storing the information. The chapter provides a discussion of CUI and the guidelines imposed for its use. The last part of the chapter is essentially a catalog of diverse federal information and intelligence systems and resources.

One of the recommendations of the *National Criminal Intelligence Sharing Plan* is that every law enforcement agency, regardless of size, develop an intelligence capacity. For some agencies, this will be an entire unit, while, for other agencies, it will be a part-time assignment for one person. In either case, there are management issues related to the intelligence function. **Chapter 14** focuses on management issues that have relative uniqueness to the intelligence function. It begins with a comprehensive list of factors to consider in developing the intelligence capacity. This is followed by a detailed description of developing a concept of operations (ConOps), which serves as the road map for developing and implementing the intelligence function. Finally, a wide range of management issues are discussed, from developing policies to human resources issues.

The final chapter examines critical issues and challenges for the future and a model for implementing change. The guide also includes comprehensive resources for all aspects of intelligence, a list of acronyms, a glossary of intelligence terms, and appendices to support the various discussions. Included in the appendices are two intelligence audit checklists.

Collectively, the guide is intended to provide information that will aid a law enforcement agency in developing and operating an intelligence function that is efficient, effective, and lawful.



# PREFACE

When the first edition of this guide was published in 2004, it documented unprecedented changes in law enforcement intelligence that occurred largely in response to the September 11, 2001, terrorist attacks. Indeed, the new initiatives reflected philosophical and operational changes that represented a geometric evolution in law enforcement intelligence in only three short years. The first edition of the guide described a broad array of cutting-edge issues and practices, though at the time it seemed implausible that such dramatic changes would occur again.

When the second edition was published in 2009, there had been significant growth in the intelligence function in the interceding five years. Fusion centers were developed, many new guidelines and best practices were developed by the Criminal Intelligence Coordinating Council and Global Justice Information Sharing Initiative, new intelligence training and resources were made available through the U.S. Departments of Justice and Homeland Security, and increasing numbers of agencies across the country began developing an intelligence capacity.

A decade later, with this third edition, we have seen many intelligence practices mature with greater integration of the intelligence process in crime fighting beyond terrorism. The use of intelligence analysis in real-time crime centers, the integration of intelligence analysis and crime analysis, and reliance on the intelligence process to aid in the prevention of mass violence are illustrations. The rapid growth of technology and social media have also brought new applications and challenges to the intelligence process, which had to integrate operational practices and legal protections. In addition, we have significant changes in resources and practices available from federal partners, which enhance the intelligence capabilities of state, local, and tribal law enforcement (SLTLE).

The intent of the third edition of the Intelligence Guide is to describe these and many more changes in the philosophy, national standards, and practice of law enforcement intelligence while maintaining the core goal of being a primer on all things intelligence for the law enforcement community.

This guide is intended to support policy in law enforcement agencies. It is not meant as an academic work, nor is it intended to look at theoretical issues or arguments. It is not directed as a guide to the Intelligence Community except to explain the roles, responsibilities, and restrictions of their SLTLE partners. It does seek to objectively provide the best knowledge and practice of law enforcement intelligence at the time of publication.

In completing this third edition, I want to thank the U.S. Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A), the U.S. Department of Justice (DOJ) Bureau of Justice Assistance (BJA), and the DOJ Office of Community Oriented Policing Services (COPS Office) for their support, guidance, and expertise on this project, as well as Ms. Gina Hartsfield, President and Chief Executive Officer (CEO) of the Institute for Intergovernmental Research (IIR), and Ms. Michelle Miller, Senior Vice President/Executive Senior Manager of Planning and Programs of IIR, for their work in finalizing the project support. I also want to thank Ms. Christina Abernathy, Manager/Senior Research Associate of IIR, for managing the project and coordinating the reviews of the chapters.

I expressly want to thank those who volunteered to review the guide: Mr. Van Godsey, Midwest HIDTA, and Mr. Patrick Baldwin, Southern Nevada Counter-Terrorism Center. I know you were a little surprised when you discovered the size of the document. Both reviews were detailed and extremely helpful in fine-tuning the contents of the guide.

I sincerely appreciate the assistance from friends whose work went well beyond “a little help,” particularly reading and reviewing drafts. I thank Mr. Monte McKee and the late Mr. Phil Ramer, both senior research associates of IIR, for their reviews, ideas, and suggestions. Their taking the time to review and provide assistance to me while working on projects of their own was truly appreciated. Despite his early reviews of material, Phil never saw this guide come to completion, but he had always been a staunch supporter and an invaluable resource for me and the law enforcement intelligence community. Phil was a friend, a mentor, and a character—he is truly missed.

I also thank the membership of the Criminal Intelligence Coordinating Council (CICC) and the Global Advisory Committee (GAC) for taking the time to review this guide to ensure that it reflects the information needed by the law enforcement intelligence community. Many people assisted me in the preparation of this guide—their contributions, large and small, helped in developing the comprehensive contents. While I hope not to leave anyone out, I particularly want to thank Mr. Mike Sena, Executive Director of the Northern California Regional Intelligence Center and Chair of the CICC for his input and support; Mr. Adam Walker and Ms. Susan Bower of DHS for coordinating the project and reviewing the material; Mr. Kevin Saupp for his detailed and thoughtful reviews, as well as Mr. Kevin Peters, Mr. Alex McClain, Ms. Catalina McCarthy, and Mr. Charles Robinson, all of DHS, as well as Ms. Sarah Estill of the COPS Office, who reviewed chapters that could rely on their specific expertise. I also appreciate the comprehensive review of Judge Barbara Mack, who aided in identifying issues to clarify and refine the text. I want to also thank Dr. Tim Best and Mr. Tom L’Esperance for providing internal IIR reviews. My thanks also to Ms. Linda Vannoy and Ms. Heidi Aaron of IIR for taking on the task of creating professional figures used to illustrate facets of the guide’s discussions.

Importantly, I thank my wife Karen and children Hilary, Jeremy, and Lauren, who put up with the time I worked on this and other projects—you are always in my thoughts. Finally, I dedicate this Intelligence Guide to my grandchildren: Shey O’Donnell, Teagan O’Donnell, Alex Rios, Olivia Rios, Austin Carter, and Logan Carter. You are all very special to me and always make me smile.

David L. Carter, Ph.D.  
Michigan State University  
Institute for Intergovernmental Research

# TABLE OF CONTENTS



<b>EXECUTIVE SUMMARY</b> .....	<b>III</b>
<b>PREFACE</b> .....	<b>VII</b>
<b>CHAPTER 1: UNDERSTANDING CONTEMPORARY LAW ENFORCEMENT INTELLIGENCE: CONCEPTS AND DEFINITIONS</b> .....	<b>1</b>
Perspective.....	3
Concepts and Definitions.....	4
Defining Intelligence .....	5
Law Enforcement Intelligence .....	6
The Structure and Responsibilities of U.S. Intelligence From the Perspective of Law Enforcement: The Domestic Intelligence Enterprise.....	10
National Security Intelligence and the Intelligence Community .....	11
Homeland Security Intelligence.....	14
Associated Intelligence Initiatives .....	18
Fire Service Intelligence .....	18
Public Health/Medical Intelligence.....	19
Crime Gun Intelligence .....	20
Forensic Lab Intelligence .....	22
Gang Intelligence .....	23

Crime Analysis and Intelligence Analysis: Understanding Their Differences and Interdependence .....	25
Understanding Crime Analysis.....	26
The Foundation for Change .....	27
An Example .....	28
Conclusions .....	30
Chapter Annex 1-1: Law Enforcement Intelligence and Homeland Security Intelligence Case Study.....	31

**CHAPTER 2: A BRIEF HISTORY OF LAW ENFORCEMENT INTELLIGENCE: PAST PRACTICE AND RECOMMENDATIONS FOR CHANGE .....35**

Law Enforcement Intelligence: The Years of Evolution .....	36
Congressional Inquiries of Intelligence Activities.....	39
<b>National Crime Commissions and New Initiatives Influencing the Evolution of SLTLE Intelligence .....</b>	<b>40</b>
The Commissions and Their Purpose .....	40
The National Crime Commissions and Law Enforcement Intelligence .....	44
<b>The Impact of Professional Associations.....</b>	<b>50</b>
Law Enforcement Intelligence Units (LEIUs) .....	50
International Association of Law Enforcement Intelligence Analysts (IALEIA) .....	51
International Association of Crime Analysts (IACA) .....	52
<b>Law Enforcement Intelligence Initiatives in the First Decade of the Post-9/11 Environment .....</b>	<b>52</b>
Collateral Developments .....	58
Implications.....	59
The Intelligence Evolution Refined.....	60
Reforming Law Enforcement Intelligence at the State, Local, and Tribal Levels .....	62
Conclusions .....	63

**CHAPTER 3: THE INTELLIGENCE PROCESS (CYCLE) FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT .....65**

Planning and Direction .....	68
Collection .....	70
Processing/Collation .....	71
Analysis .....	75
Dissemination .....	76
Reevaluation .....	80
Conclusions .....	81

**CHAPTER 4: TECHNOLOGY AND INTELLIGENCE.....83**

Facial Recognition: CICC Recommendation.....	84
Emerging Technologies and Law Enforcement Intelligence: A Perspective.....	84
<b>Technology Uses for the Intelligence Process .....</b>	<b>85</b>
Information Collection, Surveillance, and Identification.....	85
Social Media.....	92
<b>Case Illustration—The Social Media Aspect of the Christchurch, New Zealand, Mosque Attacks .....</b>	<b>94</b>
Analysis of Quantitative and Qualitative Raw Information, Particularly With Artificial Intelligence (AI)	
Applications.....	96
Technology for Information and Intelligence Sharing/Dissemination .....	98
Accountability of the Intelligence Process .....	99
Conclusions .....	99

<b>CHAPTER 5: INTELLIGENCE-LED POLICING: HISTORICAL FOUNDATION AND CONCEPT .....</b>	<b>101</b>
Conceptual Foundations.....	102
Defining ILP .....	102
<b>Fundamental Perspectives on the History of ILP: The British Experience .....</b>	<b>104</b>
Perspective 1: The Current State of American Law Enforcement Intelligence.....	104
Perspective 2: The British National Intelligence Model and Challenges in Adapting It to U.S. Law Enforcement .....	105
Comparing U.S. and UK Law Enforcement Intelligence .....	107
<b>ILP, Community Policing, Problem Solving, and CompStat.....</b>	<b>108</b>
Comparing ILP and CompStat.....	109
Ethical Issues.....	112
Civil Rights and ILP .....	112
Public Education.....	112
Community Members as Law Enforcement Volunteers .....	114
A Quick Review of Relevant ILP Research.....	115
<b>Conclusions .....</b>	<b>117</b>
<b>CHAPTER 6: DEVELOPING AND IMPLEMENTING INTELLIGENCE-LED POLICING .....</b>	<b>119</b>
Establishing a Framework for Strategic Priorities and Information Processing: The Information Management Plan .....	120
The Information Management Plan .....	121
Establishing Strategic Priorities for Intelligence-Led Policing .....	121
Intelligence Requirements.....	124
Collection Plan .....	125
Analysis .....	126
Intelligence Products .....	126
Operational Responses.....	126
Review of the Process.....	127
Summary.....	127
Organizational Infrastructure for ILP .....	128
Commitment.....	128
Partnerships .....	130
Information Sharing Processes .....	133
Operational Plan .....	134
Analytic Capability .....	135
Tactical and Strategic Response Alternatives .....	135
Next Steps: Implementation .....	136
Self-Assessment of an Agency’s Intelligence Capacity.....	136
The Implementation Starting Point .....	139
Conclusions .....	141
<b>CHAPTER 7: PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE LAW ENFORCEMENT INTELLIGENCE PROCESS .....</b>	<b>143</b>
A Perspective on the Organizational Framework.....	144
Privacy, Civil Rights, and Civil Liberties: A Foundation .....	145
<b>Increased Scrutiny of Law Enforcement Intelligence: The Challenge of Balancing P/CRCL and Community Safety .....</b>	<b>146</b>
Lawsuits and Decrees Related to Law Enforcement Intelligence Activities.....	148
Civil Rights Example: First Amendment Freedom of Expression—Two Views .....	154

The Need for More Controls of Intelligence Inquiries Than Criminal Investigations.....	155
<b>Maintaining Privacy in the Intelligence Process .....</b>	<b>157</b>
Locational Privacy .....	159
<b>Issues of Information Collection and Social Media .....</b>	<b>160</b>
Social Media and the First Amendment.....	160
Social Media and the Reasonable Expectation of Privacy.....	164
<b>28 CFR Part 23—Criminal Intelligence Operating Policies.....</b>	<b>167</b>
<b>Federal Civil Rights Liability and Intelligence .....</b>	<b>172</b>
<b>Steps to Ensure Protection of P/CRCL .....</b>	<b>175</b>
<b>Conclusions .....</b>	<b>177</b>
<b>Chapter Annex 7-1: Protecting Civil Rights and Immunizing an Agency From Liability     in the Law Enforcement Intelligence Process .....</b>	<b>179</b>
<b>CHAPTER 8: THE INTELLIGENCE FUSION PROCESS .....</b>	<b>181</b>
Historical Perspective.....	182
Refining the Fusion Center Concept.....	183
Baseline Capabilities for Fusion Centers .....	186
<b>What Is Intelligence Fusion? .....</b>	<b>187</b>
Why Fusion Centers? .....	189
Fusion Centers and the Crime Laboratory: An Analogy .....	191
Fusion Centers and the Information Sharing Environment (ISE) .....	191
<b>Operationalizing the Fusion Process .....</b>	<b>192</b>
Is There a Role for the Private Sector? .....	194
<b>Concerns About Fusion Centers .....</b>	<b>194</b>
Fusion Centers and Civil Rights Issues.....	199
Can Federal Criminal Intelligence Be Shared With Fusion Centers?.....	201
<b>Developing the Fusion Center .....</b>	<b>202</b>
Outputs of the Fusion Center .....	205
<b>Research and Fusion Centers .....</b>	<b>206</b>
<b>Conclusions .....</b>	<b>209</b>
<b>Chapter Annex 8-1: Developing a Memorandum of Understanding.....</b>	<b>210</b>
<b>CHAPTER 9: DEVELOPING PUBLIC-PRIVATE PARTNERSHIPS FOR LAW ENFORCEMENT INTELLIGENCE (P3I).....</b>	<b>213</b>
Background and Perspective .....	215
U.S. National Standards and Recommendations for Public-Private Partnerships .....	216
P3I and the Intelligence Process.....	219
The Information Sharing Environment and the Private Sector .....	220
<b>Fundamental Principles of P3I .....</b>	<b>222</b>
Types of Partnerships.....	224
Obstacles to Law Enforcement-Private Partnerships .....	226
Two Critical Issues to Resolve: Sharing Criminal Information and Private Proprietary Information/Intellectual Property.....	229
Developing a Successful P3I .....	230
InfraGard .....	232
Security/Police Information Network (SPIN): Nassau County, New York.....	234
<b>Homeland Security, Information Sharing, and the Private Sector.....</b>	<b>236</b>
Critical Infrastructure Sector Partnership.....	236
Critical Infrastructure Partnership Advisory Council .....	237

Special Note: Terrorism Early Warning (TEW) Group .....	237
Looking Ahead for TEWs .....	238
A Critical Challenge for Partnerships: Technology Companies .....	239
Conclusions .....	241
Chapter Annex 9-1: Public-Private Partnership Exercise .....	242
<b>CHAPTER 10: MANAGING INFORMATION: A CLOSER LOOK AT SUSPICIOUS ACTIVITY REPORTS, INTELLIGENCE REQUIREMENTS, COLLECTION, AND ANALYSIS .....</b>	<b>245</b>
Suspicious Activity Reporting .....	245
The Debate: Should SARs Be Limited to Terrorism Information? .....	247
Nationwide SAR Initiative (NSI).....	249
Suspicious Activity Reporting Processes in State and Local Agencies .....	251
SARs and Personally Identifiable Information .....	256
Establishing Controls on Suspicious Activity Reports/Information .....	257
Policy Recommendations for Developing and Managing a Suspicious Activity Reporting System .....	258
Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) .....	259
Summary .....	260
Intelligence Requirements .....	260
Filling Gaps/Fulfilling Requirements .....	262
Applying the Requirements to State and Local Law Enforcement.....	263
Comparing Intelligence Requirements and Crime Analysis: An Analogy.....	264
Requirements and Strategic Priorities.....	264
Typologies of Requirements .....	265
Requirements and Criminal Evidence .....	267
Summary .....	267
Collection .....	267
Collecting Information From Corrections Agencies .....	269
Summary .....	270
Analysis .....	270
Analytic Tools .....	274
Predictive Analysis .....	277
Qualitative Methods of Predictive Analysis.....	278
Summary .....	281
Conclusions .....	281
Chapter Annex 10-1: Global Justice Information Sharing Initiative.....	283
<b>CHAPTER 11: THREAT ASSESSMENTS AND INTELLIGENCE PRODUCTS.....</b>	<b>287</b>
Threat Assessments and Targeted Violence.....	288
The Threat Environment.....	290
Understanding Threats and Risk.....	292
The Character of Threat Assessments.....	293
Criteria for Assessing Threats .....	295
Methods.....	296
Research and the Scientific Method .....	299
Critical Thinking .....	300
Intelligence Products.....	301
Practices to Avoid With Intelligence Products .....	304
Threat Assessment Products .....	305
The Threat Assessment Briefing.....	307

Conclusions .....	308
Chapter Annex 11-1: Threat Assessment Information Collection Template .....	309
<b>CHAPTER 12: OPEN SOURCE INFORMATION AND INTELLIGENCE.....</b>	<b>315</b>
Understanding “Open Source” .....	316
Why Is There Value in Open Source Information? .....	316
Definitions and Categorizations.....	317
Source of First Resort.....	318
Open Source and Law Enforcement Intelligence—“Tradecraft” .....	320
Law Enforcement Applications of Open Source .....	320
Open Sources and Civil Rights .....	322
Attribution and Copyrighted Materials in Intelligence Products and Training Materials .....	324
Metrics for Open Source Use .....	326
Online Open Source Content for the Intelligence Process .....	327
Open Source Information Identifying People and Organizations From Subscription Services and the Media... ..	327
Social Networking and Issues for Open Source.....	329
Newsletters, Blogs, Message Boards, and White Papers .....	330
Wikis.....	332
RSS Feeds .....	332
Grey Literature and Grey Information .....	332
The Deep Web and the Dark Web/Darknet .....	333
Putting the Darknet in Context .....	337
A Broadened Perspective of Open Source for Law Enforcement .....	338
Homeland Security Intelligence and Open Sources .....	338
Open Source Processes and Protocols .....	339
Using an Open Source Collection Plan .....	339
Techniques and Tools .....	340
The Need to Determine Accuracy, Reliability, and Validity .....	341
Avoiding Traffic Analysis: Becoming Anonymous on the Web.....	342
The Investment of Critical Thought and Time.....	343
Conclusions .....	343
Chapter Annex 12-1: Eclectic Websites Found Useful for Intelligence.....	344
Chapter Annex 12-2: The Pre-Search Development Plan.....	346
<b>CHAPTER 13: USING FEDERAL AND NATIONAL AGENCIES AND RESOURCES TO SUPPORT THE INTELLIGENCE PROCESS AND INFORMATION SHARING .....</b>	<b>347</b>
What Is Needed to Start? .....	348
A Perspective on Federal Law Enforcement Intelligence Resources .....	348
Classified Information .....	349
Security Clearances for SLTLE Personnel .....	351
Sensitive But Unclassified (SBU) and Controlled Unclassified Information (CUI).....	353
Sensitive But Unclassified (SBU) Information.....	354
Controlled Unclassified Information (CUI) .....	355
Summary .....	356
Federal and National Intelligence Resources .....	357
Department of Homeland Security, Office of Intelligence and Analysis (DHS I&A).....	358
Federal Bureau of Investigation (FBI) Intelligence Initiatives.....	359
Drug Enforcement Administration (DEA) .....	363
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) .....	365

Office of the Director of National Intelligence (ODNI) .....	365
Regional Information Sharing Systems (RISS).....	366
Financial Crimes Enforcement Network (FinCEN).....	368
High Intensity Drug Trafficking Areas (HIDTAs).....	369
Criminal Intelligence Coordinating Council (CICC) .....	369
Deconfliction .....	370
A Unified Message on Law Enforcement Information Sharing.....	371
International Criminal Police Organization (INTERPOL) .....	372
Summary .....	373
<b>Conclusions .....</b>	<b>373</b>
<b>Chapter Annex 13-1: FBI Process and Information for State, Local, and Tribal Law Enforcement</b>	
Personnel to Obtain a Security Clearance .....	374
<b>CHAPTER 14: MANAGEMENT AND HUMAN RESOURCE ISSUES FOR THE</b>	
<b>INTELLIGENCE FUNCTION .....</b>	<b>377</b>
Foundation .....	378
<b>A Checklist of Considerations for Developing or Reengineering the Law Enforcement Intelligence Capacity .....</b>	<b>379</b>
Administration and Management .....	379
Develop the Intelligence Unit’s Infrastructure .....	380
Staffing .....	382
Training.....	383
Information Management and Information Sharing.....	384
Implementation and Assessment .....	385
<b>Developing the Concept of Operations .....</b>	<b>385</b>
Contents of a Concept of Operations.....	387
The ConOps Next Step .....	392
<b>Implementing and Managing the Intelligence Structure .....</b>	<b>392</b>
Establishing an Organizational Framework .....	393
“Chartering” an Intelligence Unit .....	393
Auditing the Intelligence Function .....	395
Establishing and Managing Partnerships.....	396
Program Evaluation.....	397
Sources for Intelligence Management and Resource Trends .....	399
<b>Human Resource Issues .....</b>	<b>400</b>
Staffing .....	401
Training.....	402
Federal Law Enforcement Training Centers (FLETC).....	405
DHS-Approved Intelligence Training .....	405
<b>Intelligence Courses in Higher Education .....</b>	<b>406</b>
<b>Conclusions .....</b>	<b>406</b>
<b>Chapter Annex 14-1: Ten Simple Steps to Adopt the National Criminal Intelligence Sharing Plan .....</b>	<b>407</b>
<b>Chapter Annex 14-2: Why Law Enforcement Agencies Need an Analytic Function .....</b>	<b>409</b>
<b>CHAPTER 15: SUMMARY, CONCLUSIONS, AND NEXT STEPS.....</b>	<b>411</b>
Challenges for the Future.....	412
Challenges to Address .....	413
<b>Implementing Change: The R-Cubed Approach .....</b>	<b>414</b>
Reassessing .....	414
Refocusing.....	415

Reallocating.....	416
Conclusions .....	416
Bibliography .....	417
<b>APPENDIX A: ACRONYMS FOR LAW ENFORCEMENT INTELLIGENCE .....</b>	<b>427</b>
<b>APPENDIX B: GLOSSARY OF TERMS FOR LAW ENFORCEMENT INTELLIGENCE.....</b>	<b>435</b>
Glossary of Law Enforcement Intelligence Terms .....	436
Glossary of Terms Expressly Related to Terrorism and Criminal Extremism .....	449
<b>APPENDIX C: INTELLIGENCE UNIT MANAGEMENT AUDIT.....</b>	<b>451</b>
Audit Criteria for the Law Enforcement Intelligence Function .....	451
Section A: Meeting National Standards.....	452
Section B: Management issues.....	452
Section C: Personnel .....	457
Section D: Fiscal Management .....	458
Section E: Unit Evaluation.....	458
Section F: Collection .....	459
Section G: Technology and Networking .....	459
Section H: Legal Issues.....	460
<b>APPENDIX D: LEIU AUDIT CHECKLIST FOR THE CRIMINAL INTELLIGENCE FUNCTION .....</b>	<b>463</b>
Introduction .....	464
References .....	468
<b>APPENDIX E: BIOGRAPHY OF DR. DAVID L. CARTER.....</b>	<b>469</b>

## LIST OF FIGURES

- 1-1 Classes of Intelligence
- 1-2 Diverse Information Collected for Intelligence Analysis
- 1-3 Comparative Illustrations of Information and Intelligence
- 1-4 Structure of the U.S. Domestic Intelligence Enterprise
- 1-5 Law Enforcement and National Security Intelligence Authority Comparison
- 1-6 Key Terms and Acronyms for Crime Gun Intelligence
- 3-1 Intelligence Process According to NCISP
- 3-2 Intelligence Process and Subprocesses
- 3-3 Processing and Collation Activities
- 3-4 Examples of Reliability and Validity Rating Scales
- 5-1 Comparison of CompStat and Intelligence-Led Policing
- 6-1 Three Phases of ILP Development in an SLTLE Organization
- 6-2 Components of the Information Management Plan
- 6-3 Structure of the Information Management Plan
- 6-4 Components of ILP
- 6-5 ILP Continuum of Variables
- 6-6 ILP Subcontinuums of Variables
- 7-1 Intelligence Records Submission Decision Tree
- 7-2 Strategies to Ensure Civil Rights Protections
- 8-1 Organizational Interrelationships and Responsibilities for the Fusion Process and ISE
- 8-2 The Fusion Process
- 9-1 Establishing a Public-Private Partnership for Intelligence
- 9-2 Nassau County, New York, Police Department SPIN Project Diagram
- 10-1 Defined Criminal Activity and Potential Terrorism Nexus Activity
- 10-2 Potential Criminal Activity or Non-Criminal Activities Requiring Additional Information During Vetting
- 10-3 Suspicious Activity Reporting Model for the Public
- 10-4 Characterizations of Law Enforcement Intelligence Requirements
- 10-5 The Analytic Process
- 10-6 Critical Characteristics of Information Quality
- 10-7 Illustrations of Analytic Charting
- 11-1 Threat Assessment Components for Planning and Direction
- 11-2 Simplified Threat Assessment Illustration
- 11-3 Characteristics of Intelligence Products
- 11-4 Attributes of Intelligence Products
- 12-1 Examples of a Darknet Market Place
- 12-2 Example of Fields to Limit Search
- 12-3 Google Translation Screenshot
- 13-1 Steps in the FBI Security Clearance Process for SLTLE Personnel
- 13-2 Illustrations of FOUO Document Markings
- 13-3 Illustration of the CUI Marking
- 14-1 Process for the Development of a Concept of Operations

## LIST OF TABLES

2-1	Summary of National Crime Commissions
2-2	Significant Post-9/11 Law Enforcement Intelligence Initiatives
4-1	Technology and Information Collection Applications
4-2	Information Collection Technology and Legal/Ethical Issues
5-1	Examples of Topics in a Public Education Program
5-2	Examples of Actions the Public Can Take
6-1	Example of ILP Strategic Priorities
6-2	Organizational Self-Assessment Factors of an Intelligence-Led Policing Capacity
7-1	Counter Positions on First Amendment Information Collection
7-2	Questions to Determine Whether Records Must Comply With 28 CFR Part 23 Regulations
8-1	Topic Areas Included in the <i>Fusion Center Guidelines</i>
8-2	Analogy of Crime Lab and Fusion Center
9-1	Sectors of Private Industry
9-2	Sample Components of a Release and Nondisclosure Agreement Regarding Proprietary Information
10-1	Interpretation and Illustration of the Rumsfeld Quote
10-2	Traditional Collection Versus Requirements-Driven Collection
11-1	Differences Between Investigations and Intelligence Reports
11-2	Case/Investigative Intelligence Versus Intelligence Products
12-1	Comparison of Expressive Statements and Statements With a Criminal Nexus
12-2	Examples of Information Attainable From Subscription Database Services
13-1	Information Categories for Classified Information
13-2	Information Categories Prohibited or Limited for Classification
14-1	Sample Issues for Intelligence Unit Policy Development
14-2	Sample Mission Statement and Goals of an LEIU
14-3	Sample Provisions for a Partnership Agreement
14-4	Intelligence Training Categories and Descriptions

# CHAPTER 1

## UNDERSTANDING CONTEMPORARY LAW ENFORCEMENT INTELLIGENCE: CONCEPTS AND DEFINITIONS



To protect the United States from criminal threats to our security and safety, current initiatives at the federal, state, local, and tribal levels have sought to develop a “culture of information sharing.”<sup>1</sup> This is a significant challenge that requires the integration of law, policy, procedure, regulation, training, and organizational change.

The *National Strategy for Information Sharing* focuses on three core principles:

- ◆ **Information as a national asset.** Departments and agencies have achieved an unprecedented ability to gather, store, and use information consistent with their missions and applicable legal authorities. They have corresponding obligations to make information available to any agency, department, or partner with a relevant national security mission and to manage that information in a manner that is lawful and protects individual rights. This requires a continued maturation of information security, access, and safeguarding policies and processes.
- ◆ **Information sharing and safeguarding requires shared risk management.** Building trust in sharing and safeguarding requires the ability to manage rather than avoid risk to national security increases when the approach to sharing is inconsistent, fragmented, or managed from a single-agency perspective. Risk decreases, however, with sound policies and standards, increased awareness and comprehensive training, effective governance, and enhanced accountability.

<sup>1</sup> See: *Information Sharing Environment Implementation Plan*. (2006). Washington, DC: Program Manager-Information Sharing Environment.

- ◆ **Information informs decision making.** Informed decision making requires the ability to discover, retrieve, and use accurate, relevant, timely, and actionable information. Likewise, our national security depends on an ability to make information easily accessible to federal, state, local, tribal, territorial, private sector, and foreign partners in a trusted manner, given the appropriate mission context. The objective is to increase the usefulness of information in operations through the consistent application of policies, guidelines, exchange standards, and common frameworks, while always respecting privacy and individual rights.<sup>2</sup>

To achieve the culture of information sharing, every law enforcement agency in the United States, regardless of size,<sup>3</sup> must have the capacity to understand the implications of information collection, analysis, and intelligence sharing. Each agency must have an organized mechanism to receive and manage intelligence as well as a mechanism to report and share critical information with other law enforcement agencies. In addition, it is recommended that law enforcement agencies develop lines of communication and information-sharing protocols with the private sector, particularly those related to critical infrastructure, as well as with those private entities that are potential targets of terrorists and criminal enterprises.

Not every agency has the staff or resources to create a formal intelligence unit, nor is it necessary in smaller agencies. Even without an intelligence unit, a law enforcement organization must have the ability to effectively consume the information and intelligence products being shared by a wide range of organizations at all levels of government. State, local, and tribal law enforcement (SLTLE) will be most effective when a single source in each agency is the conduit of critical information, whether it is the Terrorist Intelligence Unit of the Los Angeles Police Department, the sole intelligence analyst of the Lansing, Michigan, Police Department, or the patrol sergeant who understands the language of intelligence and is the information sharing contact point in the Mercedes, Texas, Police Department. Hence, each law enforcement agency must have an understanding of its intelligence management capabilities regardless of its size or organizational structure. This includes ensuring that law enforcement chief executives understand and support their agencies' intelligence function as well as ensuring that line officers both understand and engage the intelligence process.

This document describes common language and processes to develop and employ an intelligence capacity in SLTLE agencies across the United States as well as articulate a uniform understanding of concepts, issues, and terminology for law enforcement intelligence. While terrorism issues have been the most pervasive since September 11, 2001 (or post-9/11), the discussion of intelligence in this guide is directed toward "all crimes, all threats, and all hazards." As such, the principles of intelligence discussed in this document apply beyond terrorism and include organized crime, gangs, repeat offenders, targeted violence, entrepreneurial crime, and all other forms of criminal threats to our communities.

Drug trafficking and the associated crime of money laundering, for example, continue to be a significant challenge for law enforcement. Transnational computer crime, particularly Internet fraud, identity theft cartels, and global black marketeering of stolen and counterfeit goods, are entrepreneurial crime problems that are increasingly involving SLTLE agencies to investigate simply because of the volume of criminal incidents. Similarly, local law enforcement is being increasingly drawn into domestic terrorism, mass violence, human trafficking, trafficking in antiquities, trafficking in endangered species, and the often-associated crimes related to counterfeiting of official documents, such as passports, visas, driver's licenses, social security cards, and credit cards. Even the trafficking of counterfeit consumer goods and parts has increased, often bringing a new profile of criminal into the realm of entrepreneurial crime. In addition, the application of intelligence to gang violence and homicides in America's communities is an important focus. All require an intelligence capacity for SLTLE, as does the continuation of more traditional organized

---

2 *National Strategy for Information Sharing*. (2012). Washington, DC: Executive Office of the President, pp. 6–7. [https://www.dhs.gov/sites/default/files/publications/15\\_1026\\_NSI\\_National-Strategy-Information-Sharing-Safeguarding.pdf](https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf)

3 *National Criminal Intelligence Sharing Plan, Version 2.0*. (2013). <https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>

crime activities such as auto theft, cargo theft, and virtually any other scheme that can produce profit for an organized criminal entity.

To be effective, the law enforcement community must interpret intelligence-related language in a consistent manner. In addition, common standards, policies, and practices will help expedite intelligence sharing while at the same time protecting the privacy of citizens and preserving hard-won community policing relationships.

## PERSPECTIVE

At the outset, law enforcement officers must understand the concept of law enforcement intelligence, its distinction from national security intelligence and the potential problems a SLTLE agency can face when the two types of intelligence overlap. A law enforcement executive needs to understand what is meant by a contemporary “intelligence function” and how that function can be fulfilled through the use of different organizational models. Related executive decisions focus on staffing, particularly when there are fiscal limitations. Complicating this mission are two new intelligence responsibilities that emerged post-9/11: (1) Information sharing with the Intelligence Community (IC) as part of the Information Sharing Environment (ISE) and (2) developing a capacity for homeland security—or “all-threats and all-hazards”—intelligence.

Another important, and pervasive, challenge is to ensure that all new intelligence initiatives fully protect the privacy and civil rights of all persons. Critical issues and new initiatives for this responsibility are also discussed throughout the guide, with one chapter devoted specifically to this issue.

These issues pose a wide range of important questions: What kinds of information does the law enforcement agency need from the federal government to most effectively counter terrorism? How are those needs determined? How is the information requested? When and in what form will the information be received? Will a security clearance be needed to review the information that an executive requests? Beyond terrorism, what types of threats exist within in a community? How are these threats identified? What kinds of threats are included in all-threats and all-hazards intelligence? What are the best sources and methods (i.e., a collection plan) available to understand these threats and develop actionable intelligence? How do we engage the community and private sector in the intelligence process? What are the limitations on information collection and dissemination between law enforcement and the community and private sector? The answers are not easy, but they are attainable.

From a policy and process perspective, what is meant by information sharing? What information can be collected? What information can be retained in a criminal intelligence records system? How long may the records be retained? When does a person transcend the threshold of exercising his or her rights to posing a threat to community safety? What resources exist to aid an SLTLE agency in accomplishing its intelligence goals? How can the entire law enforcement agency be integrated into the intelligence function? If a law enforcement organization is to be effective, the answers to these questions must be a product of written policy.

The intent of this document is to provide answers—or at least alternatives—to these questions. To begin the process, every law enforcement administrator must recognize that intelligence and information sharing can be effective in preventing—or at least mitigating—terrorism, criminal enterprises, gangs, and other forms of continuing criminality. To realize these ends, however, the intelligence process for law enforcement at all levels of government requires the following:

- ◆ Reengineering some of the organization’s structure and processes to be consistent with national initiatives and national standards of good practice in law enforcement intelligence
- ◆ Developing a shared vision of the terrorist or criminal threat
- ◆ Being a participant in unified messaging of critical intelligence-related initiatives

- ◆ Establishing a commitment to participate and follow through with threat information
- ◆ Overcoming difficulties of conceptualizing intelligence processes that some personnel find difficult to grasp because of its disparity from traditional LE assignments/functions
- ◆ Committing resources, time, and energy from an agency to the intelligence function
- ◆ Establishing policies and practices that protect individuals' civil rights and privacy
- ◆ Embracing and using contemporary technology, including electronic access to information and an electronic communications capability through a secure connection, and embracing new and emerging technologies (described in a later chapter)
- ◆ Having proactive people using creative thought to identify what we do not know about terrorism and criminal enterprises
- ◆ Requiring a law enforcement agency to think globally and act locally
- ◆ Engaging in public-private partnerships for intelligence
- ◆ Engaging the community to participate in the intelligence process, in particular to report suspicious activities
- ◆ Ensuring that the intelligence function is transparent and avoiding secrecy of intelligence operations, both externally and internally
- ◆ Maintaining commitment and patience

The amount of change in the law enforcement intelligence process that has occurred over the past two decades is significant. The roles and responsibilities for state, local, and tribal law enforcement are challenging from operational, policy, and fiscal perspectives. Despite these challenges, comprehensive plans and new resources have become available to achieve the goal of protecting our communities.

## CONCEPTS AND DEFINITIONS

In the purest sense, intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.

There are essentially two broad purposes for the law enforcement intelligence function:

1. **Prevention.** This involves gaining or developing information related to threats of terrorism or crime and using this information to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threat. In state and local law enforcement, there are three generally accepted types of intelligence that are specifically prevention-oriented:
  - a. Case/Investigative Intelligence. Actionable intelligence in support of an immediate or ongoing criminal investigation.
  - b. Tactical Intelligence. Actionable intelligence about imminent or near-term threats that is disseminated to the line functions of a law enforcement agency for purposes of developing and implementing preventive and/or mitigating response plans and activities.
  - c. Operational Intelligence. Actionable intelligence about *long-term threats* that are used to develop and implement preventive responses. Most commonly, operational intelligence is used for long-term inquiries related to suspected criminal enterprises and complex multijurisdictional criminality.

2. **Planning and Resource Allocation.** The intelligence function provides information to decision makers about the changing nature of threats, the characteristics and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention.

- a. This is known as *strategic* intelligence—it provides an assessment of the changing threat picture to the management of a law enforcement agency for purposes of developing plans and allocating resources to meet the demands of emerging threats.

While investigation<sup>4</sup> is clearly related to the information collection<sup>5</sup> and intelligence processes, the intelligence function is often more exploratory and more broadly focused than a criminal investigation, per se. For example, a law enforcement agency may have a reasonable suspicion to believe that a person or a group of people has the intent, capacity, and resolve to commit a crime or terrorist act. Evidence, however, may fall short of the probable-cause standard for arrest. Moreover, there may be a compelling community safety reason to keep an inquiry open to identify other criminal threats and weapons that may be used. From another perspective, in an investigation with many potential suspects and a diverse array of evidence (that is sometimes contradictory), the analytic processes of intelligence can help lend focus to the investigation.

Because of this broader role, the need to keep information secure, and the necessity of keeping records that identify individuals and organizations for whom evidence of criminal involvement is uncertain or tangential,<sup>6</sup> rigid guidelines must be followed. These guidelines are designed to protect the constitutional rights of people in the United States while at the same time permitting law enforcement agencies to proceed with an inquiry for purposes of community safety. The guidelines are also designed to facilitate accurate and secure information sharing between law enforcement agencies because the nature of terrorism and criminal enterprise threats is inherently multijurisdictional. Further, if law enforcement agencies at all strata of government subscribe to the same guidelines, information sharing can be more widespread because there is greater certainty that regardless with whom the information is shared, the security and integrity of the records will remain intact.

## DEFINING INTELLIGENCE

There are many misconceptions about the meaning and application of “intelligence,” not only among the lay public but also within law enforcement. Some colloquial uses of the term provide an intuitive understanding, such as “Officer Rios collected some good intelligence.” However, these uses lack precision and are unable to account for the diverse applications and rules associated with the intelligence process.

As a primer, there are two broad classes of intelligence as illustrated in Figure 1-1. The first category is the discipline of intelligence, which refers to the set of rules, processes, and lexicon of the intelligence function. This guide is solely about the discipline of intelligence. Within the framework of the discipline, there are three core types of intelligence of concern for the present discussion<sup>7</sup>: (1) law enforcement (or criminal<sup>8</sup>) intelligence; (2) homeland security—also

---

4 “Investigation” is defined as the pursuit of information based on leads and evidence associated with a particularly defined criminal act to identify and apprehend criminal offenders for prosecution in a criminal trial.

5 “Information collection” in the context of law enforcement intelligence is the capture of information and data to determine

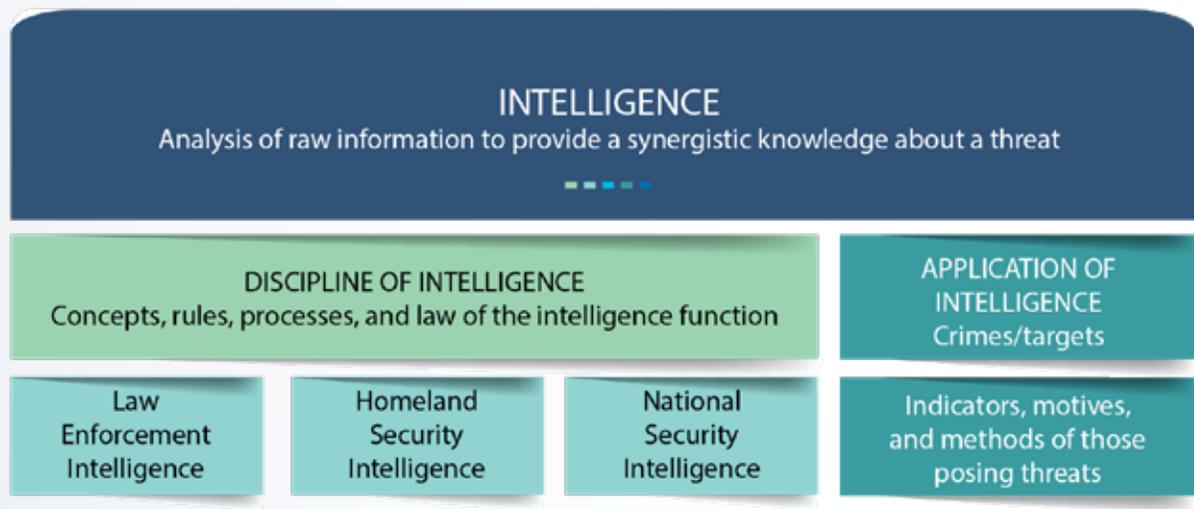
6 This includes information that would be in the intelligence records system “temporary file” as well as “noncriminal identifying information” as applied through 28 CFR Part 23, which will be discussed in detail later.

7 This is not an exclusive categorization of intelligence; the discipline of intelligence may be divided into other categories also. For example, national security intelligence may be divided into policy intelligence and military intelligence. One may also consider business intelligence, geospatial intelligence, or cyber intelligence, among others. The categorization used above is the best model to illustrate critical points for the current discussion.

8 The author uses the phrase “law enforcement intelligence” because there is a realm of study in the field of criminal psychology that addresses criminal intelligence as it relates to the criminal personality and the propensity and processes by which criminals behave.

known as all-threats and all-hazards—intelligence; and (3) national security intelligence. While there are important similarities across these three categories, there are also distinct differences. These critical factors are discussed throughout this guide as they specifically relate to SLTLE agencies.

FIGURE 1-1: CLASSES OF INTELLIGENCE



The second broad class is the application of intelligence. This type of intelligence deals with knowledge related to a specific crime type. For example, intelligence analysis that produces information about new methods and indicators in the uses of firearms in mass violence attacks is the application of intelligence. Another illustration would be indicators drawn from an analysis of international financial transactions that are characteristic of a money-laundering enterprise. An essential ingredient for the application of intelligence is an understanding of the nature and constituent elements of the crime phenomenon of concern. For example, if a community is threatened by multijurisdictional gang activity that operates as a criminal enterprise, then an understanding of the gang culture, signs, symbols, hierarchy, and other gang-specific characteristics is essential for analysts, as well as for officers striving to be effective in combating crime. While the two classes of intelligence are inextricably linked for purposes of training and application, it is nonetheless important for the student of intelligence to understand the unique aspects of each.

With an understanding of the classes of intelligence, attention will be directed toward the definitions of each.

## LAW ENFORCEMENT INTELLIGENCE

This guide uses definitions based on generally accepted practice and standards by the law enforcement Intelligence Community at the local, state, and tribal levels. This does not mean that other definitions of terms are wrong, but this approach provides a common understanding of words and concepts most applicable to the targeted audience of this guide.

Before defining intelligence, it is essential to understand the meaning of “information” in the context of this process. Information may be defined as “pieces of raw, unanalyzed data that identifies persons, organizations, evidence, contraband, events or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.”<sup>9</sup> As will be seen, information is collected as the currency that produces intelligence.

9 Global Intelligence Working Group. (2004). *Criminal Intelligence for the Chief Executive*. A Training Program for the Chief Executive. Glossary.

The phrase “law enforcement intelligence,” used synonymously with “criminal intelligence,” refers to the fundamental law enforcement responsibility to enforce the criminal law. Often, the phrase is used improperly. Too often, intelligence is erroneously viewed as pieces of information about people, places, or events that can be used to provide insight about criminality or crime threats. It is further complicated by the failure to distinguish between the different types of intelligence.

Pieces of information gathered from diverse sources—such as wiretaps, informants, banking records, or surveillance (see Figure 1-2)—are simply raw data that frequently have limited inherent meaning. The term “intelligence” is used when a wide array of raw information is assessed for validity and reliability, reviewed for materiality to the issues at question, and given meaning through the application of inductive or deductive logic. Law enforcement intelligence, therefore, is *the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality*. The need for carefully analyzed, reliable information is essential because both policy and operational decisions are made using intelligence; therefore, a vigilant process must be in place to ensure that decisions are made on objective, informed criteria, rather than on presumed criteria.

FIGURE 1-2: DIVERSE INFORMATION COLLECTED FOR INTELLIGENCE ANALYSIS



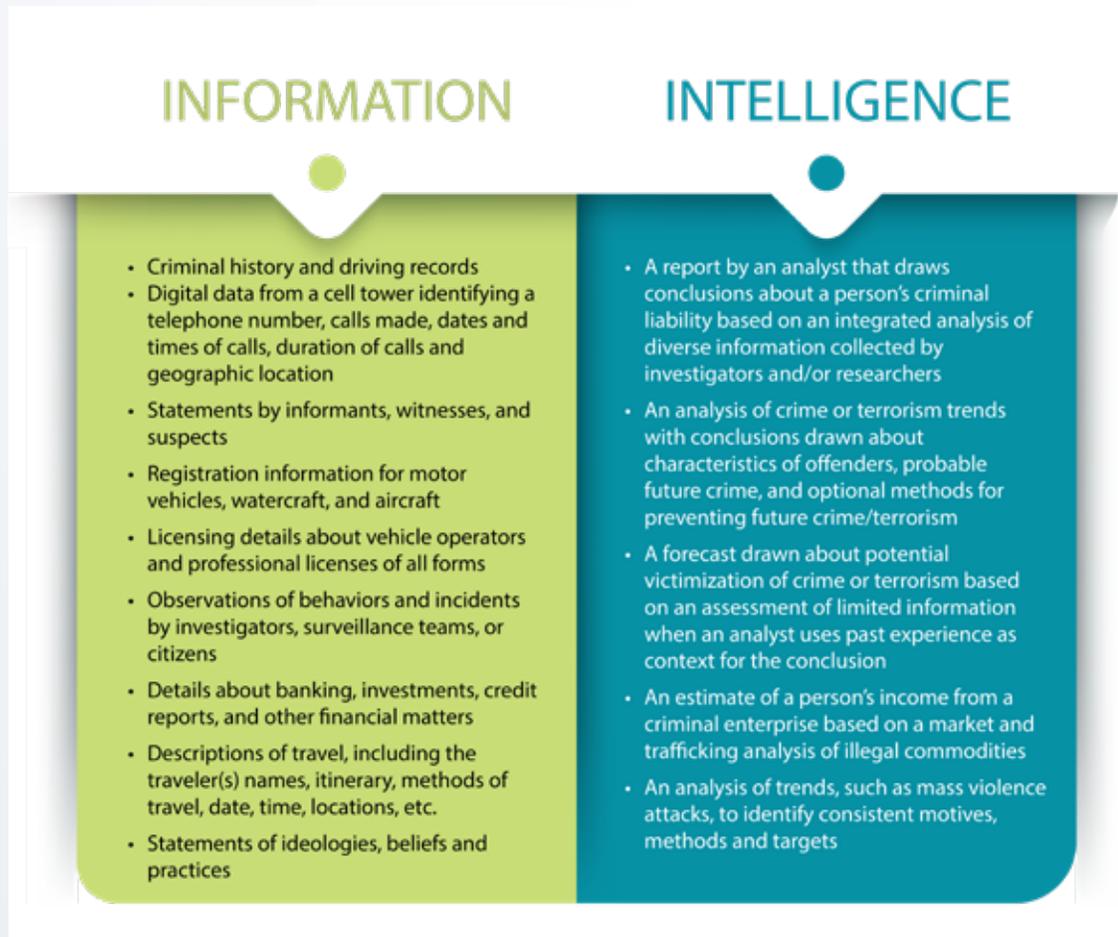
Often, the terms “information sharing” and “intelligence sharing” are used interchangeably by persons who do not understand the subtleties, yet importance, of the distinction. In the strictest sense, intelligence professionals should take care to use terms appropriately because, as will be seen in later discussions, there are different regulatory and legal implications for “intelligence” than for “information.” (See Figure 1-3.) As such, the subtleties of language can become an important factor, should the management of a law enforcement agency’s intelligence records come under scrutiny.

**Definitions in context.** State and local law enforcement have consistently defined law enforcement intelligence as containing the critical element of analysis before any information can be characterized as intelligence. For example, the IACP Criminal Intelligence Sharing Plan funded by the Office of Community Oriented Policing Services observed that:

...intelligence is the combination of credible information with quality analysis—information that has been evaluated and from which conclusions have been drawn.<sup>10</sup>

FIGURE 1-3: COMPARATIVE ILLUSTRATIONS OF INFORMATION AND INTELLIGENCE

Similarly, the Global Intelligence Working Group, a project funded by the Office of Justice Programs and part of the Global Justice Information Sharing Initiative, discusses law enforcement intelligence by observing:



...the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at both the tactical and strategic levels.<sup>11</sup>

Following a consistent vision, the International Association of Law Enforcement Intelligence Analysts (IALEIA) states that intelligence is an analytic process:

...deriving meaning from fact. It is taking information collected in the course of an investigation, or from internal or external files, and arriving at something more than was evident before. This could be leads in a case, a more accurate view of a crime problem, a forecast of future crime levels, or a hypothesis of who may have committed a crime or a strategy to prevent crime.<sup>12</sup>

In creating standards for state, local, and tribal law enforcement, the Commission on Accreditation of Law Enforcement Agencies (CALEA) seeks to provide specific guidance on policies and practices that ensures efficacy and

10 International Association of Chiefs of Police. (2002). *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Federal, State, and Local Levels*. A summit report. Alexandria, VA: IACP. p. v.

11 Global Intelligence Working Group. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: Office of Justice Programs, p. 6.

12 International Association of Law Enforcement Intelligence Analysts. (undated). *Successful Law Enforcement Using Analytic Methods*. Internet-published document. p. 2.

protection from liability on all aspects of law enforcement duties. With respect to intelligence, CALEA's standards note:

Certain essential activities should be accomplished by an intelligence function, to include a procedure that permits the continuous flow of raw data into a central point from all sources; a secure records system in which evaluated data are properly cross-referenced to reflect relationships and to ensure complete and rapid retrieval; a system of analysis capable of developing intelligence from both the records system and other data sources; and a system for dissemination of information to appropriate components.<sup>13</sup>

It is clear not only from these discussions, but also from the legacy of law enforcement intelligence from various national crime commissions examining intelligence-related activities at the state and local levels, that a common thread exists: Information must be analyzed before it is classified as intelligence. Chapter 2 will show that there is a fundamental reason for this: Regulations applying to state, local, and tribal intelligence records<sup>14</sup> must meet standards of assessment that do not apply to federal agencies.<sup>15</sup> As a consequence, the analytic component is essential for the definition.

It is often stated that for every rule, there is an exception. The definition of law enforcement intelligence fits this axiom. As a matter of functional practicality, the Federal Bureau of Investigation (FBI) Intelligence Branch categorizes intelligence somewhat differently. As observed by one FBI intelligence official in a confidential interview:

In the law enforcement/national security business, [intelligence] is information about those who would do us harm in the form of terrorist acts or other crimes, be they property crimes or violent crimes. . . . [The FBI] produces both "raw" (or unevaluated intelligence) and "finished" intelligence products (those that report intelligence that has had some degree of analysis).

Given the nature of the FBI Intelligence Branch responsibilities and the need to get the critical threat information into the hands of the law enforcement community quickly, this definition is more appropriate for its role. Law enforcement executives need to be aware of the different roles and the different context when interpreting information. These differences are not in conflict; rather, they coexist to support the different missions and responsibilities of agencies at all levels of government. Similarly, the need for a different approach to the intelligence cycle exists for the FBI compared with SLTLE because of different intelligence demands.

The remedy is simple: Those responsible for the intelligence function need to understand these differences and apply policies and practices (described later) that are most appropriate for the types of intelligence being produced and consumed.

---

13 Commission on Accreditation of Law Enforcement Agencies. (2002). *Standards for Law Enforcement Accreditation*. "Standard 51.1.1 – Criminal Intelligence." Washington, DC: CALEA.

14 Most notably, 28 CFR Part 23 as well as various court decisions.

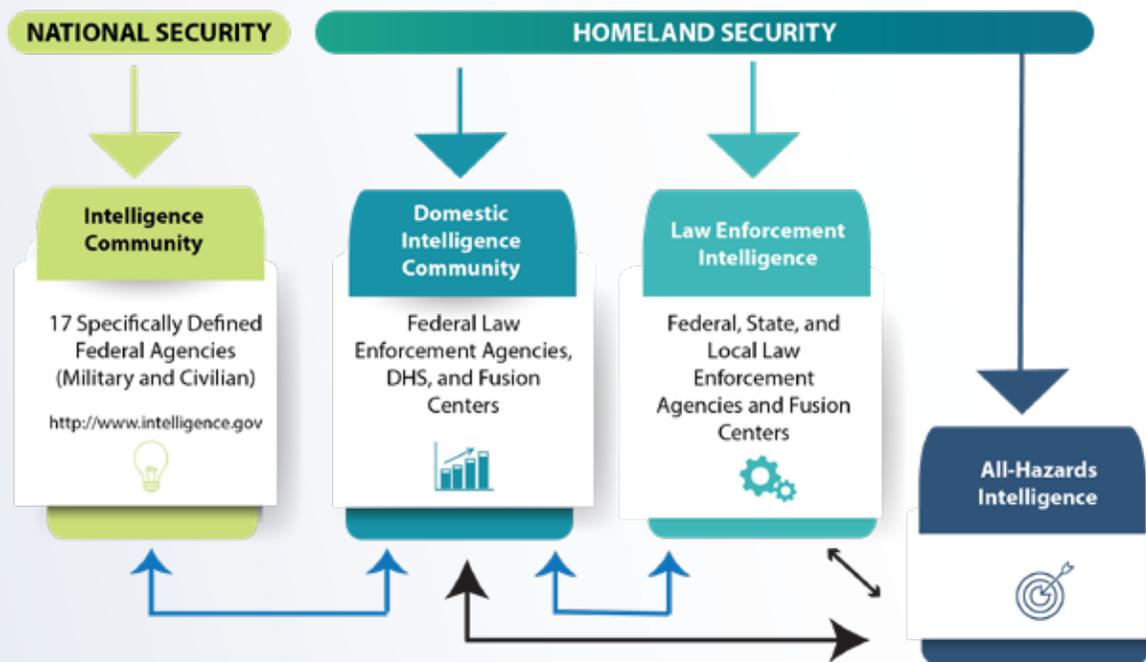
15 These issues are described in detail in later discussions.

## THE STRUCTURE AND RESPONSIBILITIES OF U.S. INTELLIGENCE FROM THE PERSPECTIVE OF LAW ENFORCEMENT: THE DOMESTIC INTELLIGENCE ENTERPRISE

The security of the United States—both internationally and domestically—relies heavily on the government’s ability to collect and analyze diverse amounts of information to identify threats and develop ways to intervene or suppress those threats. This is at the conceptual heart of the intelligence enterprise; however, that enterprise is not a single monolithic entity. Rather, it is a series of entities, each having different responsibilities and differing forms of authority to fulfill those responsibilities. Each also has its own restrictions on the types of information that can be collected and retained as well as the method of collection.

The federal government tends to conceptualize the intelligence structure as being national security centric. Indeed, that is a primary role of the federal government, and making distinctions between foreign intelligence and military intelligence serves a functional purpose, particularly for policymaking.<sup>16</sup> However, for the current discussion, the perspective is different because of a focus on the intelligence enterprise from the perspective of state, local, and tribal law enforcement. From this view, the distinctions between the character of national security intelligence as well as the disciplines of intelligence—also known as the “int’s”<sup>17</sup>—have little importance because they have little relevance to the responsibilities of state, local, and tribal law enforcement.

**FIGURE 1-4: STRUCTURE OF THE U.S. DOMESTIC INTELLIGENCE ENTERPRISE**



While the intelligence enterprise in the United States has always had different dimensions, the post-9/11 environment has made these structures more complex as a result of new laws, regulations, and programs. The structural evolution of the intelligence enterprise continues as executive branch agencies often struggle with implementing policy and programs from complex laws. Beyond these new initiatives—most of which have their genesis in counterterrorism—there is also an evolving philosophy of intelligence and its application that is notably evident in law enforcement.

<sup>16</sup> For example, see Randol, M. A. (2009). *Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches*. Washington, DC: Congressional Research Service. Retrieval from: <http://www.fas.org/sgp/crs/intel/RL33616.pdf>.

<sup>17</sup> The “int’s” are established disciplines of information collection used by the IC, such as Human Intelligence (HUMINT), Signals Intelligence (SIGINT), or Imagery Intelligence (IMINT), among others. While an integral part of IC operations, they are not used in law enforcement. See [https://www.doctrine.af.mil/Portals/61/documents/AFDP\\_2-0/2-0-D14-ISR-Intel-Disciplines.pdf](https://www.doctrine.af.mil/Portals/61/documents/AFDP_2-0/2-0-D14-ISR-Intel-Disciplines.pdf).

There is a growing appreciation of how intelligence analysis can aid in managing crime, particularly when integrated with other data-driven, problem-solving police initiatives. Whether it is the Central Intelligence Agency (CIA) or a local police department, the structure of the U.S. intelligence enterprise is evolving.

To provide insight into these changes, the current discussion examines intelligence structures currently in the United States. There are two broad intelligence goals in the United States: the maintenance of national security and homeland security. Both require different authority and methods, but there is also some overlap in their responsibilities. This overlap requires some degree of information sharing, but the nature and types of information shared are dependent on who the target of the information collection was; the method with which the information was collected; the types and locations of the threats involved; whether and how the information is classified; and strategies necessary to stop the threat. Because of these various factors, the structure of intelligence, particularly domestically, has been developed in overlapping layers, notably over the last 15 years, for effective and lawful information sharing. To be certain, this is still a work in progress, yet the picture is becoming more focused. Figure 1-4 illustrates the functional structures of the U.S. intelligence enterprise and the relationships between these different types of intelligence. It should be noted that this structure is based on functions, not particular agencies. Typically, multiple agencies have responsibilities for each function.

## NATIONAL SECURITY INTELLIGENCE AND THE INTELLIGENCE COMMUNITY

In understanding the broad arena of intelligence, some perspective of national security intelligence (NSI) is useful for SLTLE agencies. This primer is meant to familiarize the law enforcement reader with basic terms, concepts, and issues; it is not intended as an exhaustive description.

NSI may be defined as “the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States’ sovereign principles.”<sup>18</sup> NSI seeks to maintain the United States as a free, capitalist republic with its laws and constitutional foundation intact and to identify and neutralize threats or actions that undermine the United States’ sovereign principles.

NSI embodies both policy intelligence and military intelligence. Policy intelligence is concerned with threatening actions and activities of entities hostile to the United States, while military intelligence focuses on hostile entities, weapons systems, warfare capabilities, and order of battle. Since the fall of the Soviet Union and the rise of threats from terrorist groups, both policy and military intelligence have evolved to grapple with the character of changing threats. The organizations responsible for NSI are collectively known as the Intelligence Community (IC).

The IC is a federation of executive branch agencies and organizations that work within their own specific missions as well as in an integrated fashion to conduct threat assessment and intelligence activities necessary for effective foreign relations and the protection of U.S. national security. These activities include the following:

- ◆ Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities
- ◆ Production and dissemination of intelligence related to national security and the protection of U.S. sovereign principles from interference by foreign entities
- ◆ Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States; international terrorist and international narcotics activities; and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents
- ◆ Administrative and support activities within the United States and abroad necessary for the performance of authorized activities such as foreign relations; and diplomacy, trade, and the protection of our allies’ interests

18 Carter, D. L. (2002). *Law Enforcement Intelligence Operations*. 8th ed. Tallahassee, FL: SMC Sciences, Inc. .

- ◆ Such other intelligence and activities as the President may direct as related to national security and the U.S. relationship with foreign entities

Thus, the NSI goal is performed by the IC, a coalition of 17 agencies and organizations within the Executive Branch of the federal government that work both independently and collaboratively to gather the information necessary to conduct foreign relations and national security activities. The primary IC mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities need to perform their articulated duties.<sup>19</sup> The 17 IC member agencies are:

- ◆ Air Force Intelligence
- ◆ Army Intelligence
- ◆ Central Intelligence Agency
- ◆ Coast Guard Intelligence
- ◆ Defense Intelligence Agency
- ◆ Department of Energy
- ◆ Department of Homeland Security
- ◆ Department of State
- ◆ Department of the Treasury
- ◆ Drug Enforcement Administration
- ◆ Federal Bureau of Investigation
- ◆ Marine Corps Intelligence
- ◆ National Geospatial-Intelligence Agency
- ◆ National Reconnaissance Office
- ◆ National Security Agency
- ◆ Navy Intelligence
- ◆ Office of the Director of National Intelligence

Members of the IC collect and assess information regarding international terrorist and narcotics activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States and its sovereignty. As needed, the President may also direct the IC to carry out special activities to protect U.S. security interests against foreign threats. National security activities, with some exceptions for the FBI, DHS, and DEA, do not involve invocation of the criminal justice system; hence protections afforded through civil rights and civil liberties protections of the U.S. Constitution do not typically apply. Therefore, traditional protections of civil rights, civil liberties, and privacy do not have the same restrictions to IC operations as they do to domestic intelligence activities.

SLTLE agencies have no direct jurisdiction as related to NSI; however, this does not mean that they will not encounter NSI or receive collection tasks to support NSI. Indeed, given that the FBI is a member of the IC, there is a strong likelihood that SLTLE officers serving on a Joint Terrorism Task Force (JTTF) will encounter or be exposed to NSI. Similarly, since the Drug Enforcement Administration (DEA) is also a member of the IC, officers working on an Organized Crime Drug Enforcement Task Force (OCDETF) may also encounter this intelligence. In both instances, typically the officers will have top-secret security clearances providing access to classified documents that may provide additional insights about the information, including the source of the information and the method of collection. Nonetheless, it is a slippery slope for SLTLE officers to rely on this information for a criminal investigation because there is a strong likelihood that the methods of collecting the NSI would not meet constitutional muster in a criminal trial.

Even if it appears that constitutional standards may be met, there are other potential problems with using the information in a criminal enquiry. Since the accused in a criminal proceeding has the right to be confronted by his or her accusers, the exercise of this right could compromise sensitive sources and methods. While the Classified

---

<sup>19</sup> <http://www.intelligence.gov/>

Information Procedures Act<sup>20</sup> (CIPA) provides a mechanism to deal with the process, some find it cumbersome and observe that it may result in greater complications than would otherwise be necessary.<sup>21</sup>

The next issue deals with constitutional law. If information is collected from NSI sources in a manner inconsistent with the U.S. Constitution, it is likely, based on the “Fruits of the Poisonous Tree Doctrine,” that any subsequent evidence developed during the course of the investigation will be subject to the Exclusionary Rule. Consequently, the evidence will be inadmissible.

A final issue with respect to state, local, and tribal officers’ access to NSI is liability. Specifically, if, in a criminal investigation, SLTLE officers use NSI that was collected in a manner inconsistent with constitutional standards, or if that information (including personal records) was kept as intelligence records that were under the custodianship of a state, local, or tribal law enforcement officer, it is possible that the officer(s) and the chain of command (through vicarious liability) of that officer’s agency could be liable under 42 USC 1983, *Civil Action for Deprivation of Civil Rights*. As most officers are well aware, under this provision if a state or local officer, acting under the color of state law, violates the civil rights of a person, the officer and his or her chain of command may be sued in federal court. Even though that officer may be working on a federal task force under the supervision of a federal officer, such as an FBI Supervisory Special Agent (SSA), the applicable test is whether the officer is paid by and bound by the employment rules of his or her state or local employing jurisdiction.<sup>22</sup>

Based on authorities from the National Security Act of 1947, Executive Order 12333,<sup>23</sup> various executive directives, and the *U.S. Attorney General’s Guidelines*, the FBI is the lead agency in domestic intelligence collection. It is important that SLTLE understand the distinction between the authority of IC agencies to collect and retain information and that of SLTLE agencies.

Another challenge emerges with the Information Sharing Environment (ISE), created by the Intelligence Reform and Terrorism Prevention Act of 2004.<sup>24</sup> The ISE seeks to share all information related to terrorist threats to the homeland.<sup>25</sup> The challenge arises particularly if SLTLE agencies collect or retain information related to a national security threat rather than a crime. SLTLE agencies’ sole jurisdiction as related to intelligence is based in their statutory authority to enforce the criminal law. As such, there is extensive constitutional rigidity and judicial scrutiny of their processes as well as the information that is collected and retained in a criminal intelligence records system (See Figure 1-5). Conversely, constitutional protections do not attach in the same way to the collection and retention of information by the IC. As a result, these agencies have greater latitude in the types of information they possess.

The processes are complicated further with regard to the collection of information domestically (i.e., within the territory of the United States) as related to national security threats. The primary responsibility for collecting domestic information for national security falls within the authority of the U.S. Department of Homeland Security, the FBI, and DEA, which can produce intelligence for dissemination to SLTLE. U.S. foreign intelligence agencies, however, are prohibited from working with state and local law enforcement in a manner that could be interpreted as “tasking intelligence collection.” As a result, SLTLE agencies should rely on their relationships with the DHS, the FBI, and DEA

20 <https://www.justice.gov/jm/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa>

21 The author has elected not to discuss CIPA in any detail because it deals with federal investigations rather than state, local, and tribal criminal investigations. Those interested in further exploring CIPA should see <https://www.justice.gov/jm/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa>.

22 The FBI and the DEA may keep such records in their custody based on their national security responsibilities. While it is possible to hold a federal officer liable based on what is known as a Bivens suit—derived from the case of *Bivens v. Six Unknown Agents* 403 US 388 (1971)—it would be difficult, particularly under the conditions of counterterrorism.

23 <https://www.intelligence.gov/ic-on-the-record-database/results/692-the-truth-about-executive-order-12333>

24 <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282>

25 Legislation passed by Congress after the September 11, 2001, attacks—notably the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)—limited many intelligence initiatives related to SLTLE to terrorism and tended not to apply the initiatives to other forms of international criminality.

on matters of domestic intelligence, notably where those matters involve international terrorism activity and/or international drug trafficking, since these are addressed uniquely in federal law.

Effective policy and processes must be implemented and enforced to ensure that SLTLE agencies do not maintain improper information about individuals and organizations in their records systems as a product of the ISE. (These issues will be discussed in greater detail in the chapter on civil rights.)

The lessons learned from this brief review of national security intelligence are threefold:

1. State, local, and tribal law enforcement officers have no jurisdiction to collect or manage national security intelligence.
2. Use of NSI in a criminal investigation by a state, local, or tribal law enforcement officer could derail the prosecution of a case because of civil rights protections.
3. Use of NSI in a criminal investigation by an SLTLE officer and/or retention of NSI in a records system or in the personal records of an SLTLE officer could open the possibility of civil liability from a Section 1983 lawsuit.

**FIGURE 1-5: LAW ENFORCEMENT AND NATIONAL SECURITY INTELLIGENCE AUTHORITY COMPARISON**



To the student of national security intelligence, this discussion may seem to place disproportionately little attention on the IC, given its complex structure and broad applications. However, the purpose of this discussion was to focus on law enforcement—particularly at the state, local, and tribal levels—and provide perspective on their role in the broader intelligence structure.

## HOMELAND SECURITY INTELLIGENCE

Homeland security intelligence emerged post-9/11 as the new U.S. Department of Homeland Security began defining its missions and responsibilities. It integrates well-established law enforcement responsibilities—most notably, the order maintenance function of law enforcement.<sup>26</sup> These new intelligence responsibilities have emerged within

<sup>26</sup> For a discussion of order maintenance responsibilities, see Carter, D. L. (2000). *The Police and the Community*. 7th ed. Upper Saddle River, NJ: Prentice Hall.

the homeland security framework that intelligence activities at the state, local, and tribal levels must assess threats posed by all hazards. While there are certainly gray areas within this framework, the key factor for law enforcement agencies is focusing on threats posed by hazards that have implications for public safety and order maintenance responsibilities. Within this context, the author defines homeland security intelligence as *the collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat*.

For example, a public health emergency or natural disaster will necessarily involve a law enforcement agency to assist in maintaining order and executing operations to maintain public order until the crisis is resolved. Homeland security intelligence may identify community safety vulnerabilities emerging from the emergency/disaster and pass this information to law enforcement agencies so that appropriate precautions can be put in place. In yet other cases, information may begin as homeland security intelligence and then become law enforcement intelligence, such as a general threat to critical infrastructure, which evolves into a threat where an individual is identified. If an individual is identified as related to a critical infrastructure threat, then in all likelihood a criminal nexus has emerged, and a law enforcement intelligence inquiry may proceed jointly with homeland security intelligence.

This form of intelligence presents many challenges because it is not purely criminal yet addresses responsibilities that law enforcement agencies have to manage within their communities. Homeland security intelligence is not clearly delineated, either as a matter of law or policy. Yet it is increasingly prevalent because of the impact of DHS responsibilities, initially within the arena of critical infrastructure but expanding into areas of domestic terrorism and targeted violence.<sup>27</sup>

Homeland security is predominantly focused on maintaining security inside the United States, largely through the use of security intervention strategies and criminal law enforcement. Each type of homeland security intelligence has a different focus. The domestic intelligence enterprise is largely driven by federal law enforcement agencies—most notably, the FBI and Homeland Security Investigations (HSI)—and the fusion centers originally intended to protect America from terrorist attacks, although in most of the fusion centers, the responsibility has been broadened to include other criminal threats to the community. However, virtually every federal law enforcement agency has responsibilities related to homeland security, whether it is preventing illegal entries of people into the United States, unlawful trafficking in firearms or controlled substances, environmental threats from the illegal dumping of hazardous chemicals, cyberattacks, or any of a myriad of other threats to America. There is some type of intelligence component in each of these threat examples. These federal agencies use two-way information sharing with the IC (almost always classified information) to identify domestic threats to the United States. Typically, however, these investigations must have a criminal nexus because of constitutional requirements.

The amount of intelligence that is being produced has increased geometrically over recent years, and virtually all agencies have some type of intelligence capacity that simply did not exist a few years ago. For example, a document produced by DHS stated that that department alone produced more than 50 different intelligence products.<sup>28</sup> With a significant portion of federal law enforcement threat information being based on IC information, there is an increasingly blurry distinction between the types of information that is being shared between federal law enforcement intelligence and national security intelligence. It becomes even more problematic when that information is further shared with state and local law enforcement. This is of significant concern to many civil libertarians, who believe that this process weakens protections to Americans' civil rights, civil liberties, and privacy.

Consider this scenario: CIA informants, supported by National Security Agency intercepts, determine that there is a high probability that Afghan heroin will be smuggled through the African route into the United States at the New York,

---

27 <https://www.dhs.gov/publication/dhs-strategic-framework-counterterrorism-and-targeted-violence>

28 Office of the Under Secretary for Intelligence and Analysis. (2012). *DHS Intelligence Enterprise Product Line Brochure*. Washington, DC: Department of Homeland Security.

Baltimore, and Miami ports of entry. The information is shared with DEA's Office of National Security Intelligence,<sup>29</sup> which, in turn, shares it with DEA task forces in those jurisdictions, including state and local law enforcement officers. The concern is that domestic law enforcement actions may be taken on information that was collected by the IC in a manner that does not meet constitutional protections.

There is uncertainty on these types of relationships, as noted in a Congressional Research Service Report:

The fundamental policy governing the relationship between law enforcement and intelligence needs to be addressed by the Attorney General and the DCI [Director of Central Intelligence], in conjunction with the congressional oversight committees. Confusion is apparent on both sides as to what the proper role (and authority) of intelligence agencies is in circumstances [involving crimes].<sup>30</sup>

The Congressional Research Service goes on to note:

A fundamental issue that faces both Congress and the U.S. public remains the need to balance the advantages to be gained by sharing information from all sources with the possibility that the availability of data accumulations could be used to undermine lawful political or religious activities. An unstable balance between these two separate goals—often portrayed as competing—greatly complicated the counterterrorism and counterintelligence effort prior to 9/11.<sup>31</sup>

The ongoing lack of clarity between national security intelligence and homeland security intelligence is further aggravated by the fact that two IC members—the FBI and DEA—have law enforcement as a primary mission.

Another key component of the domestic intelligence enterprise is the network of fusion centers.<sup>32</sup> For the current discussion, the role of the fusion centers is essentially to serve as an analytic clearinghouse of threat information that is a primary information flow conduit among state, local, and tribal law enforcement and the remainder of the domestic intelligence enterprise. While they are entities of state and local government, the fusion centers—in particular, the primary state fusion center—hold an important role for the domestic intelligence enterprise. This has been reinforced by the Program Manager's Office of the Information Sharing Environment<sup>33</sup> (PM-ISE), which observed:

... fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial, and private sector partners. To support these information sharing efforts, federal agencies have significantly improved coordinating the planning and provision of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding, in support of the National Network of Fusion Centers.<sup>34</sup>

While the phrase “homeland security” often evokes imagery of terrorism, in reality having a secure homeland also includes the maintenance of public order and suppressing crime. Increasingly, law enforcement agencies have recognized the value that analysis provides in support of policing operations. The growth of CompStat,<sup>35</sup> evidence-

---

29 <https://www.dni.gov/files/documents/ppd-28/DEA.pdf>

30 Best, R. A. (2007). *Sharing Law Enforcement and Intelligence Information: The Congressional Role*. Washington, DC: Congressional Research Service, p. 4.

31 *Ibid.*, p. 14.

32 For locations of the fusion centers and related information, see <https://nfcausa.org/>.

33 <https://www.dni.gov/index.php/check-the-status-of-a-request/201-about/organization/information-sharing-environment/378-who-we-are-ise>

34 <https://www.odni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/ise-archive/ise-blog/2292-supporting-the-national-network-of-fusion-centers>

35 <https://www.policefoundation.org/publication/compstat-in-practice-an-in-depth-analysis-of-three-cities/>

based policing,<sup>36</sup> smart policing,<sup>37</sup> hot-spot analysis,<sup>38</sup> place-based crime analysis,<sup>39</sup> and the expansion of law enforcement intelligence units<sup>40</sup> are all indicative of this expanded appreciation for the value of analysis. Indeed, the Bureau of Justice Assistance (BJA) Law Enforcement Forecasting Group (LEFG) produced a white paper on the importance of analysis to effective law enforcement, both now and in the future.<sup>41</sup> This growth in analysis by law enforcement agencies was not, however, driven by terrorism, but by crime. Hence, with guidance and structure from new intelligence processes derived from post-9/11 intelligence initiatives, law enforcement agencies built on this new foundation of intelligence for crime control.

Contemporary intelligence units located in law enforcement agencies (as opposed to the fusion centers, per se) are predominantly driven by local public safety needs as compared with terrorism prevention and critical infrastructure protection.<sup>42</sup> While American law enforcement personnel are concerned about the prevention of terrorism, they also recognize that their most common daily threat comes from local serious crimes such as homicide, gang violence, and drug trafficking. As such, there is a stronger motivation to develop an intelligence capability that will address these threats as compared with terrorist threats. For example, the Palm Beach County, Florida, Sheriff's Office developed a county fusion center primarily to deal with homicides and aggravated assaults committed by gang members.<sup>43</sup> As another illustration, a recent BJA homicide project found that homicide investigators were increasingly relying on intelligence analysis to support their investigations.<sup>44</sup>

Law enforcement intelligence shares Sensitive But Unclassified<sup>45</sup> (SBU) information with the domestic intelligence enterprise, typically through fusion centers. Because of the statutory authority of law enforcement officers and the fact that criminal justice processes are used to investigate potential offenders, there are rigid regulations on the collection and retention of information about individuals who are the targets of intelligence inquiries. To retain this information, there must be a demonstrated nexus of a person's behavior that meets the standard of reasonable suspicion, not mere suspicion. Information that does not meet this standard must be purged from the criminal intelligence records system, even if an individual's behavior is unpopular or offensive (such as expressing a white nationalist ideology or espousing anti-government rhetoric). For the current discussion, the important distinction rests in the legal requirements imposed on law enforcement intelligence that are not applicable to national security intelligence.

All-hazards intelligence typically involves the collection, analysis, and sharing of information that poses a public health or public safety threat to the community. Since this information is typically about conditions—such as an epidemic, hazardous materials release/exposure, natural disasters, or other noncriminal public safety threats—rather than the behavior of individuals, constitutional restrictions typically do not apply.

There is a clear movement toward integrating all-hazards intelligence within fusion centers and law enforcement intelligence operations—but it is an uncomfortable fit.

---

36 <https://www.ncjrs.gov/pdffiles1/nij/237723.pdf>

37 <https://www.smart-policing.com/>

38 <https://nij.ojp.gov/topics/articles/hot-spot-policing-can-reduce-crime>

39 <https://cebcp.org/crime-and-place/>

40 Carter, D. L., et al. (2011). *Understanding the Intelligence Practices of State, Local and Tribal Law Enforcement Agencies*. A grant report to the National Institute of Justice. Retrieval at <https://www.ncjrs.gov/pdffiles1/nij/grants/238561.pdf>.

41 <https://www.bja.gov/Publications/LEFGIncreasingAnalyticCapacity.pdf>

42 Some major urban area fusion centers tend to have more of a crime focus than the primary state fusion centers, but the mission and practices vary widely across the United States.

43 *Reducing Crime Through Intelligence Led Policing*. (2012). Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance. Retrieval from <https://www.bja.gov/Publications/ReducingCrimeThroughILP.pdf>.

44 Carter, D. L. (2013). *Homicide Process Mapping: Best Practices for Increasing Homicide Clearances*. Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance.

45 [http://www.dhs.gov/xlibrary/assets/foia/mgmt\\_directive\\_110421\\_safeguarding\\_sensitive\\_but\\_unclassified\\_information.pdf](http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf)

Policymakers are also aware that the fast shift from traditional threats to the new “all-hazards” approach has generated new bureaucratic and cultural tensions. The different information cultures and worlds do not know each other or fully understand each other’s research methodologies and have little or no experience working together. The all-hazards world requires agility and ability to work in cross-disciplinary teams. Policymakers also feel the pressure from a public that is more sophisticated due to information technology, and, in the aftermath of Hurricane Katrina in the United States and catastrophic floods and terrorist incidents in Europe, demands more competent government responses.<sup>46</sup>

Part of the rationale for all-threats and all-hazards intelligence is the recognition that in most American communities, law enforcement is the only readily available 24/7/365 public service agency. As a result, having a constant all-threats and all-hazards threat stream of information is a logical alternative. Similarly, when a disaster occurs, law enforcement agencies always respond, not just to investigate, but also to help maintain public order and public safety. While not always embraced by law enforcement, when objectively viewed, all-threats and all-hazards intelligence is a reasonable responsibility to be incorporated into the American law enforcement intelligence structure.

## ASSOCIATED INTELLIGENCE INITIATIVES

While the range of activities that could be encompassed by homeland security intelligence is broad, there are two initiatives that are moving forward with greater rapidity: Fire Service Intelligence and Public Health/Medical Intelligence.

### FIRE SERVICE INTELLIGENCE

This initiative is in its infancy but is epitomized by this observation from *Fire Chief* magazine:

Does the fire service, or emergency services in general, have a role in the world of intelligence? This question probably would never have been asked prior to September 11, 2001, but it is being asked now. Given that firefighters are among the country’s first responders to terrorist incidents, natural disasters, industrial accidents and everyday emergencies, the answer is a resounding yes.<sup>47</sup>

Asking law enforcement about the fire service role in intelligence operations does not evoke a response with the same vigor. The reason, for the most part, is uncertainty: Law enforcement is uncertain about the types of information it can and should share with the fire service, although there is an effort to integrate fire service information in fusion centers.<sup>48</sup> There may also be a unique role the fire service holds beyond the private sector.

Exploration has resulted in an initiative known as the Fire Service Intelligence Enterprise. Based on a test program from the Fire Department of New York (FDNY), along with joint efforts from within DHS—the Office of Intelligence & Analysis and FEMA—the concept continues to be further explored.

Though not a federally sanctioned establishment or organization, its establishment by state and local fire service officials and industry groups was a result of advice and support provided by the State and Local Program Office to the New York City Fire Department (FDNY) and FEMA’s United States Fire Administration (USFA). This relationship contributed to a draft approach for state and local fire services to share threat and related information among the country’s nearly 1.2 million firefighters and EMS customers. I&A continues working with the USFA and the National Fire Academy in Emmitsburg,

---

46 Laipson, E. (2008). *New Information and Intelligence Needs in the 21st Century Threat Environment*. Washington, DC: The Stimson Center, p. 40. Retrieval from: [https://www.stimson.org/wp-content/files/file-attachments/SEMA-DHS\\_FINAL\\_1.pdf](https://www.stimson.org/wp-content/files/file-attachments/SEMA-DHS_FINAL_1.pdf)

47 Pitts, D. (January 1, 2008). “Getting the 411.” *Fire Chief*.

48 Fusion Center Integration with Fire Service: A Baseline Capabilities appendix which identifies recommended actions for fusion centers to effectively integrate the fire service into the fusion process. <https://bja.ojp.gov/library/publications/fire-service-integration-fusion-centers>

Maryland, to incorporate intelligence training into their course curriculum and ensure our first responders better understand the events surrounding or leading up to their involvement in an incident.<sup>49</sup>

The objective of this initiative is to integrate the fire service into existing information sharing efforts between both DHS and local law enforcement, primarily through a fusion center. The law enforcement agency would pursue a direct information sharing relationship with the fire service according to a directive of the *National Response Plan* (NRP). The NRP mandates the alignment of federal coordinating structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management.<sup>50</sup> Taking it a step farther, one fire service lieutenant has recommended that state fire service offices establish a threat liaison officer<sup>51</sup> (TLO) to serve as the primary conduit for law enforcement-fire service information sharing.<sup>52</sup> Indeed, the Criminal Intelligence Coordinating Council added the fire service as a member in 2017.<sup>53</sup>

By sharing pre-incident information and intelligence and real-time incident updates, situational awareness will be enhanced to support the preparedness efforts of both local fire departments and DHS. Rapid and comprehensive information sharing also is imperative to establishing a common operational picture on the local and national levels during a major incident.<sup>54</sup>

The difficulty for the fire service intelligence concept is that it predominantly exists within the all-threats and all-hazards framework of intelligence, about which law enforcement is still attempting to identify and resolve its intelligence role. Further, the issues of information sharing and civil rights remain difficult to unequivocally resolve. Similarly, some members of the fire service are not overly enthusiastic about being associated with the law enforcement intelligence function.

Amalgamating the fusion concept with the all-threats and all-hazards approach to intelligence requires a critical review of operating processes, responsibilities, and roles. The jury is out on whether this will be a fruitful initiative. Nonetheless, law enforcement executives and intelligence commanders should be aware of the fire service intelligence concept and explore the role, if any, it holds in the local law enforcement intelligence structure.

## PUBLIC HEALTH/MEDICAL INTELLIGENCE

A growing component of the all-threats and all-hazards responsibility in homeland security intelligence deals with public health threats. This all-encompassing intelligence assesses public health trends, organizations, and related events that can affect the health of a community.<sup>55</sup> There has been significant growth in the military on medical intelligence where the focus is broader, notably looking at foreign medical trends. Comprehensive resources on medical intelligence can be found at:

---

49 Tomarchio, J. (April 17, 2008). *Focus on Fusion Centers: A Progress Report*. Prepared statement before the Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration, Committee on Homeland Security and government Affairs, United States Senate, p. 7.

50 Ibid.

51 Also referred to as fusion liaison officer (FLO), terrorism liaison officer, or intelligence liaison officer (ILO), the roles of each are essentially the same. <https://leb.fbi.gov/articles/featured-articles/terror-liaison-officer-training>

52 Covert, J. M. (2012). *Evolving the Local Fire Service Intelligence Enterprise in New York State: Implementing a Threat Liaison Officer Program*. Monterey, CA: Naval Postgraduate School. <https://www.hsdl.org/?abstract&did=732019>. A similar program was proposed in California for a fire TLO to be assigned to the state's fusion centers. <https://osfm.fire.ca.gov/media/2656/tlo-courseplan.pdf>

53 While it goes beyond the scope of the current discussion, the reader should also be aware of the National Incident Management System (NIMS): Intelligence/Investigations Function Guidance and Field Operations Guide. [https://www.fema.gov/sites/default/files/2020-07/fema\\_nims\\_intelligence-investigations-function-guidance-oct-2013.pdf](https://www.fema.gov/sites/default/files/2020-07/fema_nims_intelligence-investigations-function-guidance-oct-2013.pdf)

54 Pitts, op. cit.

55 See <http://publichealthintelligence.org/>.

- ◆ The National Center for Medical Intelligence<sup>56</sup>
- ◆ The WWW Virtual Library collection on Epidemiology<sup>57</sup>
- ◆ The Centers for Disease Control and Prevention (CDC) WONDER Database of Health and Risks<sup>58</sup>
- ◆ Overdose Detection Mapping Application Program<sup>59</sup>
- ◆ Public Health and Medical Integration for Fusion Centers: A Baseline Capabilities appendix, which identifies the recommended actions for fusion centers to integrate the public health and health care (PH/HC) community into the fusion process.<sup>60</sup>

Increasingly, as related to law enforcement, research has examined violence as a public health issue.<sup>61</sup> The use of threat analytics as well as violence trends, following an epidemiology model, has shown promise to develop violence intervention programs. Similarly, the opioid crisis has found traditional law enforcement processes ineffective in dealing with abusers and has focused more on a public health approach.<sup>62</sup>

With respect to public health intelligence, the significant points to note are as follows:

1. There is a distinct trend toward public intelligence as a tool to assist in the protection of our communities.
2. Medical intelligence will become an increasingly important intelligence responsibility as a result of the all-threats and all-hazards mandate.
3. There is a role for public health intelligence in violence suppression.
4. There are resources to assist in identifying public health threats.

## CRIME GUN INTELLIGENCE

Over the last several years, with increasing levels of violent crime,<sup>63</sup> including many gang-related homicides and an alarming increase of both school shootings and mass-casualty shootings, new initiatives to deal with violent firearms-related crime were developed. The National Public Safety Partnership<sup>64</sup> (PSP) was created by the BJA to bring focused and diverse resources and initiatives to member jurisdictions in order to reduce violence. The National Institute of Justice<sup>65</sup> (NIJ) funded various scientific research projects to learn what works in combatting violent crime as did the National Science Foundation and a number of think tanks.<sup>66</sup> Collectively, it was clear that violence by firearms was disproportionately high, often committed with illegally obtained weapons.

56 [https://military.wikia.org/wiki/National\\_Center\\_for\\_Medical\\_Intelligence](https://military.wikia.org/wiki/National_Center_for_Medical_Intelligence)

57 <https://guides.indlibrary.org/c.php?g=360100&p=2430986>

58 <http://wonder.cdc.gov/>

59 <http://www.odmap.org/>

60 <https://it.ojp.gov/gist/159/Health-Security--Public-Health-and-Medical-Integration-for-Fusion-Centers>

61 Dahlberg, L. L., & Mercy, J. A. (February 2009). "History of Violence as a Public Health Issue." *AMA Virtual Mentor*, Volume 11, No. 2: 167–172. [https://www.cdc.gov/violenceprevention/pdf/history\\_violence-a.pdf](https://www.cdc.gov/violenceprevention/pdf/history_violence-a.pdf)

62 <http://onlinemph.unr.edu/resources/articles/how-are-public-health-officials-fighting-the-crisis-of-opioid-addiction/>

63 James, N. (2018). *Recent Violent Crime Trends in the United States*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/misc/R45236.pdf>

64 <https://www.nationalpublicsafetypartnership.org/> The initiative was originally developed as the Violence Reduction Network (VRN).

65 <https://www.nij.gov/topics/crime/violent/Pages/welcome.aspx>

66 As one example, see [https://www.nsf.gov/discoveries/disc\\_summ.jsp?cntn\\_id=139074&org=NSF&from=news](https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=139074&org=NSF&from=news).

FIGURE 1-6: KEY TERMS AND ACRONYMS FOR CRIME GUN INTELLIGENCE<sup>67</sup>

<b>CRIME GUN</b>	Any firearm possessed or used, or intended to be used, during or in relation to a crime
<b>ETRACE</b>	Electronic Tracing System. Internet-based system that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center (NTC).
<b>NIBIN</b>	National Integrated Ballistic Information Network. ATF's NIBIN is the only interstate ballistic identification system that allows law enforcement partners to associate ammunition casings, crime guns, and crime scenes.
<b>NIBIN LEAD</b>	A linkage of two or more gun crimes (shooting, crime gun recovery) through the utilization of NIBIN technology.
<b>NIBIN HIT</b>	A confirmed linkage of two or more gun crimes (shooting, crime gun recovery) through the utilization of NIBIN technology made by two certified firearms examiners.
<b>CGI TARGETING</b>	This is the definitive outcome of CGIC, which enables the identification of violent offenders, gun crime trends, gun crime density areas, at risk Federal Firearm Licensees (FFLs) or gun dealers, and crime gun sources. The process enables precise investigative and enforcement strategies and enhances prosecution efforts.

While there was a wide range of expertise and technologies available for investigating crime guns, these efforts were not cohesively integrated. Moreover, a number of the resources—particularly at the Bureau of Alcohol, Tobacco, Firearms and Explosives<sup>68</sup> (ATF)—were underutilized.

As a result, an effort led by the ATF and supported by BJA developed new initiatives to identify, investigate, and prosecute both criminals who use firearms and their illicit sources of guns. This initiative is known as crime gun intelligence. It builds on virtually all aspects of intelligence-led policing (ILP) by relying on the analysis of a diverse array of information ranging from traditional investigative methods to data analysis; pattern analysis of information gathered from acoustical gunfire detection systems;<sup>69</sup> and forensic analysis of firearms, casings, and gunfire residue, added to other information collection methods used in the intelligence process (e.g., social media analysis, suspicious activity reports, various law enforcement databases). At the heart of crime gun intelligence are the multiagency regional crime gun intelligence centers<sup>70</sup> (CGICs), where local agencies are funded by BJA to participate in the initiative. The CGICs collectively leverage the intelligence, technology, and community engagement of the participating local agencies to prevent violent crime and more efficiently conduct investigations when gun crimes occur.<sup>71</sup> At the centers, data from firearms-related crimes and ballistics evaluations from the National Integrated

67 <https://crimegunintelcenters.org/cgic-concept/>

68 <https://www.atf.gov/>

69 <https://www.forbes.com/sites/quora/2017/05/15/how-can-acoustic-gunshot-detection-systems-help-law-enforcement/#606901fc755c>

70 <https://crimegunintelcenters.org/>

71 <https://www.bja.gov/local-law-enforcement-cgic-integration-initiative/index.html>

Ballistics Information Network<sup>72</sup> (NIBIN) are analyzed. The CGICs' goal is to provide timely and accurate intelligence to investigators to assist in the identification of firearms offenders and their sources of crime guns.

In an evaluation of the CGIC initiative in three cities—Denver, Milwaukee, and Chicago—the Police Executive Research Forum found that:

NIBIN and crime gun intelligence centers are promising programs that provide an important way to combine information from various technologies and sources to link and solve gun-related crimes that might otherwise go unsolved. The CGIC model stresses the importance of providing feedback to all involved in the process, which is important to its sustainability. CGIC programs further the goal of identifying and targeting the most violent offenders for prosecution and removing them from the streets before they can commit additional acts of violence. PERF's findings indicate promise, especially in cities with significant levels of gun-related crime.<sup>73</sup>

SLTLE intelligence initiatives and fusion centers that are not part of a CGIC can nonetheless use their methodology to more effectively deal with firearms-related crimes in their respective jurisdictions. Communications with ATF and the CGIC have revealed some terminology that is somewhat unique to this initiative and that may be of value for SLTLE intelligence personnel. These terms are summarized in Figure 1-6: Key Terms and Acronyms for Crime Gun Intelligence, the processes used, and the resources available should be part of the arsenal available to any SLTLE intelligence unit.

## FORENSIC LAB INTELLIGENCE

Forensic laboratories across the United States are being armed with increasingly sophisticated technologies they can use to help solve cases and bring criminals to justice. Innovations from forensic science research and development (R&D) are bringing new techniques to crime solving and increasing the reliability and efficiency of forensic testing.<sup>74</sup> Crime labs have historically provided an assessment of physical evidence to either validate the explicit nature of the evidence or provide insight on what the evidence tells investigators about the commission of crime. Accreditation<sup>75</sup> of forensic labs adds to validity of their findings, which, in turn, adds value and reliability in their forensic analysis.

Considering recent observations about physical and digital evidence collection associated with illegal narcotics, the opioid epidemic, cybercrimes, and gun-related violence, the submission of evidence to forensic laboratories and resulting analysis creates an opportunity for building upon improvements in intelligence. Forensic labs hold a significant amount of data and engage in a wide variety of scientific disciplines in analyzing evidence. Because the scientific process is closely aligned with the intelligence cycle, there are excellent opportunities to expand the landscape of intelligence development. Forensic labs develop objective, data-based primary investigative intelligence which, when combined with existing data and other forensic lab information, often creates new information.<sup>76</sup>

The wide array of scientifically analyzed evidence, including digital evidence, can be effectively integrated in the intelligence process to provide an even more robust analysis. The research suggests that overall, crime laboratories can enhance their processes to provide a wider array of analysis with new streamlined processes to produce results

---

72 <https://www.atf.gov/firearms/national-integrated-ballistic-information-network-nibin>

73 *The "Crime Gun Intelligence Center" Model: Case Studies of the Denver, Milwaukee, and Chicago Approaches to Investigating Gun Crime.* (2017). Washington, DC: Police Executive Research Forum, p. 48. <https://www.policeforum.org/assets/crimegunintelligencecenter.pdf>

74 Dutton, G., et al. (2015). *The Impact of Forensic Science Research and Development.* Washington, DC: National Institute of Justice.

75 Accreditation is provided by the American Society of Crime Lab Directors (ASCLD) <https://www.asclcd.org/>.

76 *Promising Practices in Forensic Lab Intelligence.* (2019). Washington, DC: Global Advisory Committee, p. 1.

more quickly.<sup>77</sup> With continually enhanced forensic laboratory analysis and with systems in place to make forensic analysis a consistent part of the intelligence cycle, the quality and impact of intelligence will increase.

## GANG INTELLIGENCE

Gang intelligence provides challenges to fully understand the application of current law, regulation, policy, and practice for law enforcement intelligence. As noted previously, intelligence is the output of the analytic process. However, for those persons specializing in gang investigations, the term “intelligence” is commonly used more broadly. Typically, gang specialists include “indicators” under the rubric of intelligence; for example, information about gang behaviors, signs, and symbols of different gangs (i.e., colors and tagging), the modus operandi of different gangs and trends in the different gang activities. Frequently, much of this information is not analyzed or at least not in the same sophisticated manner of the intelligence process. As a practical element of the discussion in this section, the recognition of this fact is functional. Thus, in discussions of gang intelligence in this section, this common application of the term by gang investigators will be used.

Certainly, there is an important role for analysis when dealing with gangs; however, gang data and information is not subject to analysis as frequently as it should be. This should change not only with the expansion of analytic expertise in law enforcement agencies, notably through fusion centers, but also as a result of the approval of the *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces*<sup>78</sup> by the Global Intelligence Working Group.

According to the National Gang Center, there are in excess of 30,700 gangs in the United States, with more than 850,000 gang members.<sup>79</sup> These data alone illustrate the extent of the problem, with gangs—many operating like criminal enterprises—posing a disproportionate threat of violence and involvement in various types of crime. Certainly, with many criminal gangs taking on the characteristics of transjurisdictional criminal enterprises, the need for information sharing and analysis of threats is essential. The tools and resources of intelligence can be important factors in effectively dealing with gang problems.

**What is a gang?** The initial vision of someone hearing the word “gang” is of a group of young males, typically in the inner city, involved in turf battles in which they spray paint gang symbols on property and are involved in violent, often deadly, confrontations with other collectives of young people, most commonly males. Typically, a vision of the well-known Los Angeles-based Crips and Bloods gangs is part of that vision. While these types of gangs certainly exist, gangs encompass a much larger population.

The *National Gang Threat Assessment*<sup>80</sup> divided gangs into six broad categories:

- ◆ National and regional street gangs
- ◆ Gangs and organized crime
  - Asian organized crime
  - Russian organized crime
- ◆ Gangs and terrorist organizations
  - Domestic terrorist groups
  - International terrorist groups
- ◆ Prison gangs

---

77 McEwen, T. (2011). *The Role and Impact of Forensic Evidence in the Criminal Justice System*. Alexandria, VA: The Institute for Law and Justice.

78 Global Intelligence Working Group. (2008). *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces*. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice.

79 <https://www.nationalgangcenter.gov/survey-analysis/measuring-the-extent-of-gang-problems>

80 National Alliance of Gang Investigators Associations. (2005). *National Gang Threat Assessment*. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice.

- ◆ Hispanic gangs
- ◆ Outlaw motorcycle gangs

As can be seen from this categorization, in some cases the line between gangs and organized crime may be blurred. Similarly, the line between gangs and terrorist organizations can be difficult to discern because often, both use the tactics of intimidation and fear to accomplish their goals.

While each state has its own statutory definitions of a gang, most use a model similar to that of the Violent Gang and Terrorist Organization File (VGTOF) of the National Crime Information Center (NCIC). According to VGTOF guidelines, a gang member must be characterized as and have at least two of the following criteria:

- ◆ Has been identified as a gang member by an individual of proven reliability.
- ◆ Has been identified as a gang member by an individual of unknown reliability, and that information has been corroborated in significant respects.
- ◆ Has been observed by law enforcement members to frequent a known gang's area, associate with known gang members, and/or affect that gang's style of dress, tattoos, hand signals, or symbols.
- ◆ Has been arrested on more than one occasion with known gang members, consistent with gang activity.
- ◆ Has admitted membership in a gang at any time other than at the time of current arrest/incarceration.<sup>81</sup>

As a result of the geographic expansion of MS-13 and the 18th Street Gangs, both of which have shown extensive expansion, the FBI created the Transnational Anti-Gang (TAG) Task Forces, whose mission. . .

. . . is to investigate, disrupt, and dismantle transnational gangs in these three Central American countries, as well as to collect and disseminate intelligence to support related U.S.-based investigations. TAG Task Forces collaborate with host nation agencies to investigate gangs at the transnational level, including by identifying members and groups, or cliques, along with their areas of operation and their leadership structure.<sup>82</sup>

As can be seen, the value of intelligence and information sharing for both identifying and classifying a person as a gang member can be an important tool. This is particularly true since gangs are often transjurisdictional. Both tactical and strategic intelligence can provide important information to law enforcement agencies about gang threats and trends.

Two initiatives have been developed that serve to enhance the use of intelligence when dealing with the gang threat: the National Gang Intelligence Center (NGIC) and the *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces*.

**National Gang Intelligence Center.** The NGIC<sup>83</sup> integrates the gang intelligence assets of all U.S. Department of Justice agencies and has established partnerships with other federal, state, and local agencies that possess gang-related information—serving as a centralized intelligence resource for gang information and analytical support. This enables gang investigators and analysts to identify links between gangs and gang investigations, to further identify gangs and gang members, to learn the full scope of their criminal activities and enterprises, to determine which gangs pose the greatest threat to the United States, to identify trends in gang activity and migration, and to guide the appropriate officials in coordinating their investigations and prosecutions to disrupt and dismantle gangs. The NGIC's

81 National Gang Center. (Undated.) *Brief Review of Federal and State Definitions of the Terms "Gang," "Gang Crime," and "Gang Member"*. Unpublished Web document located at <https://www.hsd.org/?abstract&did=762864>.

82 <https://www.fbi.gov/investigate/violent-crime/gangs>

83 <https://www.fbi.gov/investigate/violent-crime/gangs/ngic> and <https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/National%20Gang%20Intelligence%20Center.pdf>

mission is to support law enforcement agencies through timely and accurate information sharing and strategic/tactical analysis of federal, state, and local law enforcement intelligence focusing on the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities throughout the United States.<sup>84</sup>

The NGIC focuses on gangs operating on a national level that demonstrate criminal connectivity between sets of common identifiers. In addition, because many violent gangs do not operate on a national level, the NGIC also focuses on selected regional-level gangs. To maximize effectiveness, the center produces intelligence assessments, intelligence bulletins, joint agency intelligence products, and other nonstandard intelligence products for its customers.<sup>85</sup>

***Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces.*** Developed by the Gang Intelligence Strategy Committee (GISC) of the Global Justice Information Sharing Initiative, the guidelines<sup>86</sup> seek to develop an integrated strategy to deal with gangs by cohesively linking both intelligence and operational responses to gang threats via task forces. On the issue of intelligence, the guidelines stress the importance of analysis and recommend the use of the intelligence process to manage and assess raw information. Similarly, the guidelines embrace the *National Criminal Intelligence Sharing Plan* as the intelligence model that should be used in all gang intelligence initiatives. Finally, the guidelines recognize the important role that intelligence can fulfill by more efficiently and effectively directing task forces responses to gang threats.

The gang guidelines are relatively new; however, with their endorsement by the Criminal Intelligence Coordinating Council, there will likely be widespread adoption of the guidelines by law enforcement agencies, fusion centers, and gang task forces.

## CRIME ANALYSIS AND INTELLIGENCE ANALYSIS: UNDERSTANDING THEIR DIFFERENCES AND INTERDEPENDENCE

Both intelligence analysis and crime analysis have been used in law enforcement for decades. Early applications were rudimentary: a recognition that a need existed to understand the character of crime; illicit commodity flows of criminal enterprises; behaviors of repeat offenders; and conditions within communities that contribute to crime. While the need was recognized—for example, it was often referred to by early policing leaders such as August Vollmer and O. W. Wilson<sup>87</sup>—the technological, analytical, and theoretical underpinnings to understand these phenomena were in their infancy.

As noted previously, early intelligence analysis was largely limited to collecting information about suspicious individuals and retaining that information in files (dossiers) just in case it was needed. It was much more a process of keeping records on people thought to be involved in criminality rather than a focus on analysis and understanding the threat environment. Information was being collected and retained on *individual* entities.

Early crime analysis focused largely on identifying crimes on maps with pins. “Pin mapping” provided a visually useful distribution of crime and crime types but tended to be almost exclusively descriptive—there was virtually no analysis. Temporal, methodological, demographic, and variance of crime characteristics were not known. Early crime analysis focused on *aggregate* data to understand crime trends.

---

84 *Attorney General’s Report to Congress on the Growth of Violent Street Gangs in Suburban Areas.* (2008). Washington, DC. U.S. Department of Justice, p. 14. <https://www.justice.gov/archive/ndic/pubs27/27612/index.htm>.

85 <https://www.fbi.gov/investigate/violent-crime/gangs/ngic>

86 <https://it.ojp.gov/documents/d/guidelines%20for%20establishing%20Gang%20Intelligence%20units.pdf>

87 An interesting review of the history of crime analysis can be found in Bruce, Christopher W. (2008). “Fundamentals of Crime Analysis.” In Samantha L. Gwinn, et al. *Exploring Crime Analysis: Readings on Essential Skills.* 2nd ed. Overland Park, KS: International Association of Crime Analysts.

With new knowledge from research, operational experimentation, and leaps in technology, both types of analysis have grown substantially more robust and sophisticated. While historically, intelligence analysis and crime analysis were viewed as being largely distinct from each other, serving uniquely different and defined roles, today they are viewed more interdependently, with both contributing to a unified crime control approach.

## UNDERSTANDING CRIME ANALYSIS

A number of factors have evolved in police research and practice which, collectively, have drawn intelligence analysis and crime analysis more closely together as critical tools in the scientific toolbox of law enforcement. Crime analysis is a type of analysis that *uses a set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and crime trend correlations*. Its goal is to assist operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, increasing apprehensions, and increasing the clearances of cases.<sup>88</sup>

The integration of crime and intelligence analysis is becoming more prevalent and was included in the latest version of the *National Criminal Intelligence Sharing Plan*, noting the roles of each:

Crime analysis focuses on analyzing a series of crimes—most notably homicide, assault, robbery, burglary, and auto theft—that have already occurred, with the intent of apprehending the offender(s) and deterring continued criminal acts. Conversely, intelligence analysis assesses diverse types of information that suggest potential criminality—such as suspicious activity reports, tips, and leads—for the purpose of identifying a criminal threat that is typically transjurisdictional in nature, with the purpose of intervening to stop the threat [including both the threat environment and individuals involved in the threat].<sup>89</sup>

Both use the scientific approach to problem solving, but each uses different analytic techniques because they have different goals. Crime analysis examines crimes that have already occurred. It seeks to find trends and consistencies to understand crime patterns. Temporal, geographic, crime type, crime characteristics and other forms of multidimensional analyses provide important information to policymakers about crime that has occurred throughout a jurisdiction. Identifying the types of crimes that were committed, noting the presence of repeat offenders, and describing victim characteristics are among the types of information that can aid in the deployment of personnel and the application of tactical police initiatives, provide direction to investigators, and help administrators define police priorities.

Intelligence analysis primarily focuses on the threat environment. Activities of criminal enterprises; the demand and distribution of unlawful commodities; the methods of operations of criminal enterprises and gangs; the character of transjurisdictional criminality; and threats to community members by criminal extremists are the types of threats that can be identified and understood through intelligence analysts. The goal, of course, is to provide intervention at both the strategic and tactical levels to stop the threats. Intelligence uses both macroanalysis (focusing on the behavior of criminal groups) and microanalysis (focusing on the behavior of individuals).

Historically, there was little overlap between the two for a variety of reasons, often dealing with organizational domains and different visions of their roles. However, both types of analysis, and their operating environments, have evolved, becoming more sophisticated in their application and more thoughtful with regard to the integration of the analysis in police policy.

---

88 Gottlieb, S., Singh, R., and Arenberg, S. *Crime Analysis: From First Report to Final Arrest*. Alpha Publishing, 1995.

89 Global Intelligence Working Group. (2013). *National Criminal Intelligence Sharing Plan, Version 2.0*. Washington, DC: Bureau of Justice Assistance, p. 25.

## THE FOUNDATION FOR CHANGE

BJA recognized that the problem of violence in the United States requires a multifaceted approach. In a coordinated initiative of projects, BJA has examined the manner in which trends in violence are identified by law enforcement for tactical purposes,<sup>90</sup> reviewed how cutting-edge analysis and the integration of resources can disrupt trends in violent crime,<sup>91</sup> and examined two decades of violence-reduction initiatives to determine what works.<sup>92</sup> Based on lessons learned, new initiatives were explored, such as the Law Enforcement Forecasting Group, which identified the importance of the analytic process for crime control (tactically) and resource allocation for crime reduction (strategically).<sup>93</sup>

Collectively, the lessons from these initiatives—and other promising practices largely supported by the various components of the Office of Justice Programs (OJP)—provide guidance on new avenues to explore the way that analysis is used to control violent crime. As a result, a renewed emphasis was placed on both crime analysis and intelligence analysis as integrated tools to aid in the development of strategic and tactical initiatives for crime control.

While the idea of crime analysis had been applied in a rudimentary manner since the early 1900s, in 1975 the former Law Enforcement Assistance Administration (LEAA) made a significant move forward by funding the Integrated Criminal Apprehension Program (ICAP). ICAP focused. . .

. . . on (1) the development of a system of operations management, (2) improved resource allocation, (3) expansion of uniformed patrol capabilities and responsibilities, and (4) the integration of police order maintenance functions with crime prevention, crime repression, and apprehension. ICAP is a process of police service delivery based on data collection, analysis, [and] planning. . .<sup>94</sup>

Technology had evolved, with most large law enforcement agencies having some type of computing capability—mostly through batch processing,<sup>95</sup> which was cutting-edge technology of the time—that pushed the concept forward. However, data collection, data entry, and data analysis were all labor-intensive, difficult, often technically challenging, and expensive because the only option for data analysis was using batch processing on mainframe computers. As personal computing evolved, there was both a greater capacity and greater flexibility for crime analysts to develop creative and useful means of analysis. The role of the analysts was expanding.

A BJA-funded project produced by the Vera Institute examined the role of crime analysts from the perspective of a cost-benefit analysis. Beyond that useful aspect of the project, the report provides a comprehensive breakdown of the crime analysts' role, noting their effectiveness is "highly dependent on the work of others."<sup>96</sup> This dependence is largely based on how decision makers and officers use the crime analysis products that are prepared. Clearly, the same can be said for intelligence analysts.

---

90 Police Executive Research Forum (2013), *CompStat: Its Origins, Evolution, and Future in Law Enforcement Agencies*, Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance, <https://www.bja.gov/Publications/PERF-Compstat.pdf>.

91 The Center for Community Safety (2013), *Winston-Salem Intelligence-Led Policing: A Blueprint for Implementing*, Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance, <https://www.bja.gov/Publications/WSSU-PB4-WinstonSalem-ILP.pdf>.

92 Michigan State University and University of Illinois at Chicago (2013), "Promising Strategies for Violence Reduction: Lessons From Two Decades of Innovation," *Project Safe Neighborhoods Case Study Report #13*, Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance, [https://www.bja.gov/Publications/MSU\\_PromisingViolenceReductionInitiatives.pdf](https://www.bja.gov/Publications/MSU_PromisingViolenceReductionInitiatives.pdf).

93 Law Enforcement Forecasting Group (2012), *Increasing Analytic Capacity of State and Local Law Enforcement Agencies: Moving Beyond Data Analysis to Create a Vision for Change*, Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance, <https://www.bja.gov/Publications/LEFGIncreasingAnalyticCapacity.pdf>.

94 Gaddis, R. K. (1982). *Integrated Criminal Apprehension Program—Final Report*. Washington, DC: National Institute of Justice. Quotation from the NCJRS abstract at <https://www.ojp.gov/ncjrs/virtual-library/abstracts/integrated-criminal-apprehension-program-final-report-0>.

95 <https://zos.conceptsolutionsbc.com/2014/04/types-of-mainframe-processing.html>

96 Matthies, C., & Chiu, T. (2014). *Putting a Value on Crime Analysts*. New York: Vera Institute, p. 11.

The crime analysts' ability to understand and describe crime trends has grown significantly with geographic information systems (GIS), stronger computer-based analytic tools,<sup>97</sup> and information sharing capacities<sup>98</sup> integrated with new data-driven theories of policing such as COMPSTAT<sup>99</sup>, evidence-based policing,<sup>100</sup> predictive policing,<sup>101</sup> and smart policing.<sup>102</sup> In this regard, it was noted on *Crimesolutions.gov* that:

Recent interest in hot spots policing is due in part to changes and innovations in policing that have occurred over the last three decades and the emergence of theoretical perspectives in criminology suggesting the importance of “place” in understanding crime. The observation that the distribution of crime varies within neighborhoods and is not spread evenly across areas has existed for some time. However, with the emergence of powerful computer hardware and software capable of carrying out sophisticated spatial analyses, crime analysts in police departments are now able to identify and track spatial concentrations of crime. Moreover, police reforms like CompStat revealed the strong linkages between spatial analyses of crime patterns and police operations meant to disrupt those patterns.<sup>103</sup>

Growth in professional development and the sharing of ideas and methodologies of crime analysis have also been important and significantly influenced by the activities of the International Association of Crime Analysts.<sup>104</sup> There is a clear complementary role for crime analysis and intelligence analysis in a police organization. Recognizing the role each plays and the value each brings to the organization is a core component of their success.

## AN EXAMPLE

Perhaps the best way to envision the application of an integrated crime analysis and intelligence analysis approach is through a real-world example that relied on both.

Homicide crime rates and homicide clearance rates are among the most accurate measures of crime occurrence/solution in a system of crime measurement generally recognized as flawed.<sup>105</sup> Hence, factors that influence these occurrences are of value to decision makers.

Because of an overall downward trend in homicide clearance rates, BJA wanted to learn what law enforcement agencies with high clearance rates were doing that made their investigations successful. As a result, BJA established the Homicide Process Mapping Project to identify best practices in homicide investigations that would result in an increase in homicide clearance rates.<sup>106</sup> To accomplish this goal, seven geographically representative law enforcement agencies were identified that had at least 24 homicides in 2011 and had a clearance rate of 80 percent or higher. In addition, because the first 48 hours of a homicide investigation are critical, the project identified critical tasks in the

---

97 These include robust statistical analysis programs; graphic depictions of analysis, mapping, commodity, and transaction flow analysis; and a variety of qualitative analytic tools.

98 Including both the increase of Internet protocols in information systems to enhance information sharing (as an example, see <https://www.niem.gov>) but also as growth-restricted law enforcement information sharing networks (as an example, see <https://www.riss.net/>).

99 [http://www.policeforum.org/assets/docs/Free\\_Online\\_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf](http://www.policeforum.org/assets/docs/Free_Online_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf)

100 <http://www.cebma.org/wp-content/uploads/Sherman-Evidence-Based-Policing.pdf>

101 <http://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx>

102 <https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/SmartPolicingFS.pdf>

103 “Practice Profile: Hot Spot Policing.” (undated). *CrimeSolutions.gov*. An online database of best practices in criminal justice, juvenile justice, and crime victim services. <https://www.crimesolutions.gov/PracticeDetails.aspx?ID=8>

104 <http://www.iaca.net/>

105 Carter, D. L., & Carter, J. G. (2015). “Effective Police Homicide Investigations: Evidence from Seven Cities with High Clearance Rates.” *Homicide Studies*. 20(2). Online first at <http://hsx.sagepub.com/content/early/2015/03/25/1088767915576996.abstract>.

106 Carter, D. L. (2013). *Homicide Process Mapping: Best Practices for Increasing Homicide Clearances*. Washington, DC: U.S. Bureau of Justice Assistance.

first 48 hours of the investigation that increase the probability of a clearance. The selected agencies, both municipal and county, were as follows:

- ◆ Baltimore County, Maryland, Police Department
- ◆ Denver, Colorado, Police Department
- ◆ Houston, Texas, Police Department
- ◆ Jacksonville, Florida, Sheriff's Office
- ◆ Richmond, Virginia, Police Department
- ◆ Sacramento County, California, Sheriff's Department
- ◆ San Diego, California, Police Department

Among the findings, the evidence clearly showed that the use of an intelligence analyst can significantly support a successful homicide investigation. All of the homicide units in this project had access to both crime and intelligence analysts (as an illustration of their value),<sup>107</sup> with most of the agencies having an analyst assigned directly to the homicide unit. Investigators in all agencies relied heavily on crime and hot-spot analysis to help target crime control efforts, most often associated with the department's CompStat program. In some cases, one analyst did both crime and intelligence analysis for investigators.

The homicide commander at the Jacksonville, Florida, Sheriff's Office (JSO) stated that usually, the first person he calls when notified of a homicide is the intelligence analyst. In Richmond, Virginia, an intelligence analyst typically responds to homicide scenes with investigators. Based on past analysis and knowledge obtained from the community, the analyst prepares a threat assessment on all homicides, and the information is disseminated to the field to reduce the likelihood of retaliation homicides or violence. This is referred to as the retaliation analysis tool (RAT).<sup>108</sup> Used predominantly for gang-related homicides, the assessment is performed for all violent crimes wherein a retaliation analysis defines the probability and nature of possible retaliation for the victim's injury or death. Gang members often attempt to injure or kill a member of the offending gang as payback. Police officers work closely with potential victims to prevent crime retaliation. Since there is a potential for retaliation in some neighborhoods based on historical information and information obtained from the community, retaliation is a significant issue that must be addressed to prevent future violence. A crime analyst can provide insight on violent crime and homicide key trends and indicators, while an intelligence analyst will identify individuals who pose potential threats.

Interestingly, in each of the agencies in this project, the traditional role of the lead homicide investigator on a case was evolving from being the stereotypical unrelenting sleuth to being an information manager. That is, homicide investigators relied on information they received from analysts as well as using information they received from specialized investigative units—such as gangs, a narcotics squad, or a fugitive squad—which would likely have information or informants that could aid in the homicide investigation. When new information was received, it not only went to the lead homicide investigator, but also to the analysts. To be an effective information manager, one needs effective analysis on an ongoing basis; every new piece of information that was developed by investigators fed the intelligence cycle for the case. All of the agencies in this project used analysts for investigative support, ongoing threat definition, and/or pattern analysis of homicide trends. The project empirically illustrated the value of integrating crime and intelligence analysis.

---

<sup>107</sup> In this context, crime analysis is typically a quantitative assessment of crime patterns and attributes. Intelligence analysis is typically a qualitative analysis of current threats (tactical) and changes in the threat picture (strategic).

<sup>108</sup> *Reducing Crime Through Intelligence-Led Policing*. (undated). Washington, DC: U.S. Bureau of Justice Assistance.

## CONCLUSIONS

The intent of this chapter was to provide the reader with insight into the meaning of intelligence, the diverse types of intelligence, its role, and some of the complications that emerge from using the term. It was noted that law enforcement intelligence, for example, is defined somewhat differently by the FBI and DEA than it is by SLTLE agencies. The reason for the difference is based on the sources of information used by the FBI and DEA as well as the responsibilities these federal law enforcement agencies hold for disseminating unique critical information in a timely fashion. The important point is that the consumer simply needs to know the different definitions and the different context. With this knowledge, information can be interpreted and used most effectively.

Also introduced in this chapter was the concept of homeland security intelligence and the unique role it fulfills for law enforcement agencies. While not a traditional activity for law enforcement, homeland security intelligence seeks to enhance public safety and order while protecting the community from nontraditional threats.

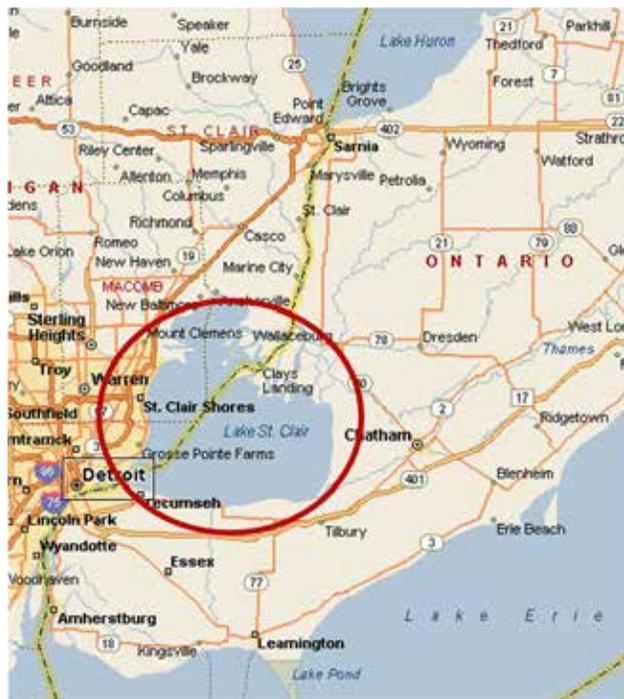
Chapter 1 addressed the meaning of national security intelligence and the complications it conceivably can pose for SLTLE agencies. Once again, it is important to understand the issues and parameters of each type of intelligence. Finally, some unique or specialized forms of intelligence—the Fire Service Intelligence Enterprise, public health intelligence, crime gun intelligence, and gang intelligence—were introduced to help the reader understand their specialized roles and the interaction and resources they provide to the law enforcement intelligence process.

Beyond examining the intelligence process, the history and development of crime analysis was discussed to illustrate how largely parallel avenues of development in crime and intelligence analysis began to merge to provide more robust, yet different, types of information to drive law enforcement operations.

The proverbial bottom line is that understanding the definitions, concepts, and applications of analysis is an essential foundation for the remaining topics discussed throughout this guide.

# CHAPTER ANNEX 1-1: LAW ENFORCEMENT INTELLIGENCE AND HOMELAND SECURITY INTELLIGENCE CASE STUDY

This illustration is based on an actual case. Its intent is to demonstrate the interrelationships between the two types of intelligence.



## LAW ENFORCEMENT AND HOMELAND SECURITY INTELLIGENCE CASE STUDY THREATS POSED BY ZEBRA MUSSELS

A congressman from a Midwestern state was a vocal supporter of legislation to ban Internet gaming in the United States. An individual who opposed this legislation made a threat to the congressman’s office that if the congressman voted for the legislation, the individual would introduce zebra mussels into some of his state’s lakes.

Zebra mussels (*Dreissena polymorpha*) are an invasive species native to the Black Sea and Caspian Sea regions of Eurasia. In 1988, they were introduced to U.S. fresh water in Lake St. Clair—between Lake Erie and Lake Huron on the Michigan, U.S.-Ontario, Canada, border—through ballast water discharges from transoceanic

vessels. The zebra mussel competes with native species of mussels and is particularly prone to clogging pipes, valves, and drains that affect drinking water, hydroelectric plants, and a wide variety of manufacturing firms. According to the Nonindigenous Aquatic Species Program of the U.S. Geological Survey, “Zebra mussels can have profound effects on the ecosystems they invade. . . and represent one of the most important biological invasions into North America.”<sup>109</sup> Zebra mussels are small and easily transported in a plastic bag, jar, or bucket. They can stay alive out of water for several days in cool, humid conditions by simply closing their shells tightly. Under the right environmental conditions, it would take as few as three zebra mussels to begin an invasion in a body of water.<sup>110</sup>

The congressman voted for the ban on Internet gaming. Recently, zebra mussels have been appearing in local lakes in the congressman’s state. The immediate issue: Is the presence of the newly discovered zebra mussels in the congressman’s state a product of the threat?

### CRIMINAL INTELLIGENCE

Zebra mussels are explicitly included in the United States Code (42 USC §42 and §43—the Lacey Act). Mere transportation of zebra mussels is a federal misdemeanor. If an individual intentionally causes damage or loss of property as a result of the introduction of zebra mussels or conspires to do so, this can be



<sup>109</sup> See <https://nas.er.usgs.gov/queries/FactSheet.aspx?speciesID=5>.

<sup>110</sup> Personal correspondence, *Nonindigenous Aquatic Species Program biologist, U.S. Geological Survey, Gainesville, Florida.*

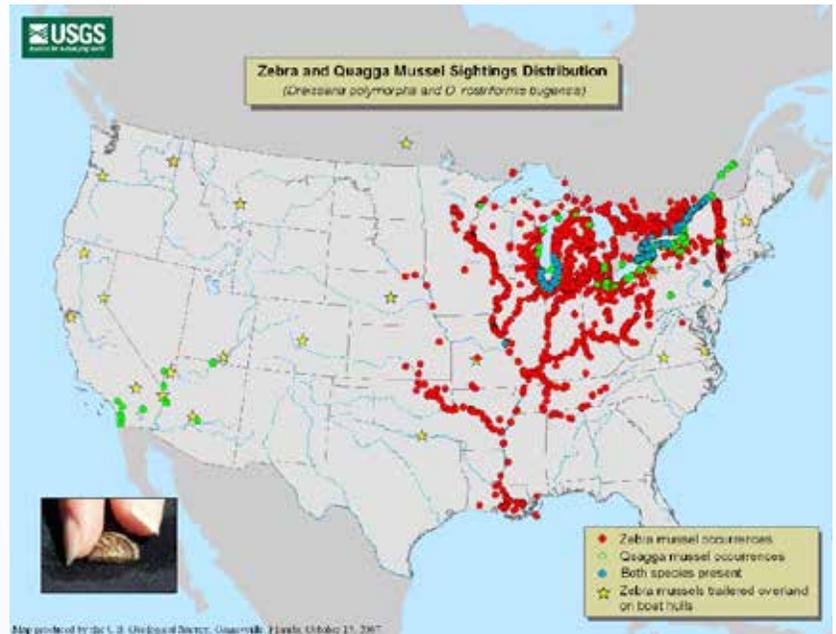
the federal crime known as “animal enterprise terrorism,” punishable as a felony, depending on the value of property loss.

Other possible federal and state crimes include extortion, terroristic threat, and criminal environmental law violations.

## HOMELAND SECURITY INTELLIGENCE

A determination should be made of hazards posed to the community and economy by this threat. Are threats posed to other bodies of water as a result of this act? What preventive/ protection measures should local

critical infrastructure or key resources vulnerable from this threat take? Intelligence requirements need to identify persons with zebra mussels in their possession and determine the reason. Businesses and government entities whose operations could be affected by the zebra mussels must be identified and notified.



## CASE INTELLIGENCE REQUIREMENTS

- ◆ What information is available about the individual who made the threat?
  - Has the congressman received threats in the past? If so, collect all related information.
  - Are there vocal activists against the ban on Internet gaming who could be reasonably tied to the congressman and /or the state?
- ◆ Are there any linkages between these individuals and environmental issues?
- ◆ How can zebra mussels be introduced into a new environment?
  - What do zebra mussels look like?
  - What are the different methods/ processes that might be used for introduction?
  - What are the indicators that zebra mussels have been introduced?
- ◆ What evidence is needed to prove:
  - That zebra mussels were intentionally introduced?
  - That there was intent to cause damage or a loss of property?
- ◆ What damage was caused by the zebra mussels?
  - What is the evidence that supports this?

## STANDING INTELLIGENCE REQUIREMENTS

- ◆ If someone is identified with zebra mussels in his or her possession:
  - Identify the individuals and the reasons for their possession of the zebra mussels.
  - Document precautions taken to avoid introduction of the zebra mussels to the local environment.
  - Document any evidence to support the elements of applicable state and/or federal laws.
    - What additional evidence may be needed?

## HOMELAND SECURITY INTELLIGENCE REQUIREMENTS

- ◆ Is there a need for the fusion center to forecast the zebra mussels' spread and impact, or can this be handled more effectively by another agency?
  - If so, which agency?
  - Is there an MOU in place to work with this agency?
- ◆ What are the characteristics of the new host environment that would help target the places the zebra mussels may be introduced and flourish?
- ◆ Do any of the identified host environments have characteristics that increase the seriousness of the invasion (e.g., public water supply, hydroelectric plant, manufacturing, commercial or recreational body of water)?
- ◆ Given the spread of zebra mussels, what is the probability their presence in the congressman's state is a product of natural transmission rather than an intentional act?
- ◆ What methods can be used to control zebra mussels?
- ◆ What resources are available to assist in handling possession and possible introduction of zebra mussels (e.g., NOAA, USGS, EPA, state natural resource agencies)?



# CHAPTER 2

## A BRIEF HISTORY OF LAW ENFORCEMENT INTELLIGENCE: PAST PRACTICE AND RECOMMENDATIONS FOR CHANGE



Distrust has surrounded law enforcement intelligence because of past instances in which police agencies maintained records of citizens' activities that law enforcement viewed as controversial, nontraditional, or suspicious, or perceived to be anti-American, even though no crimes were being committed. This, of course, violates fundamental constitutional guarantees and offends the American sense of fairness with respect to government intrusiveness. Unfortunately, the boundary is not precise regarding the types of information police agencies can collect and retain because of the subjective nature of determining whether information shows a criminal nexus to a person's behavior. Some legal guidelines lack precision in their application of law to factual situations. Beyond the legal ramifications, early intelligence initiatives by law enforcement often lacked explicit focus, were viewed as public surveillance, and typically maintained a shroud of secrecy. Important lessons can be learned from these historical experiences that provide context and guidance for law enforcement intelligence today.

Aggravating these factors was an unclear relationship between law enforcement intelligence and national security intelligence that has changed continuously since the mid-20th century. These changes have been both politically and legally controversial, since early initiatives sought to respond to changing sociopolitical events in American history—most recently, through post-September 11, 2001 (post-9/11), counterterrorism efforts. There is a tendency to judge past actions of policing in general using today's standards without historical context. Using historical context does not make past improper actions right, yet that context helps us understand why certain decisions were made. There is no evidence that improper information collection and retention was done with malice toward citizens' constitutional rights; rather, law enforcement was trying to protect its community. While that rationale does not

justify law enforcement actions, particularly under today’s standards, it provides context. As a result, there is value in understanding selected portions of history from both types of intelligence to gain perspective and understand the lessons learned.

## LAW ENFORCEMENT INTELLIGENCE: THE YEARS OF EVOLUTION

Early law enforcement intelligence initiatives, notably going back to the 1920s, used a records process known as the dossier system. Essentially, intelligence files were nothing more than dossiers—files with a collection of diverse raw information—about people who were thought to be criminals, to be involved with criminals, or to be a threat to the safety and order within a community. Bootleggers during Prohibition and many of the high-profile criminals of the early 20th century<sup>111</sup>—for example, Bonnie and Clyde, the Barker Gang, Machine Gun Kelly, and Al Capone—are obvious examples. However, local criminals, thugs, and ne’er-do-wells were the typical kinds of persons about whom police agencies most commonly kept dossiers.

During the Great Depression of the 1930s, little was done in the law enforcement intelligence arena. Other priorities were simply higher; the pervasive threat to the country was the economy, not criminality. Circumstances began to change in the latter part of the decade as communism—or the “Red Scare”—became predominant. The police relied on the only system they had “to keep an eye out for communists:” the dossier.

In 1937, U.S. Representative Martin Dies (D-Texas) became the first chairman of the House Un-American Activities Committee (HUAC).<sup>112</sup> Dies, a supporter of the Ku Klux Klan, fueled the fire of concern about communism in the United States, including labeling people as communists who appeared to be “un-American,” which often resulted in their loss of jobs and functional displacement from society. Concern about communism was pervasive but was of secondary interest in the 1940s because of World War II. After the war, when the Communist Soviet Union was formed and its nuclear arsenal built, the Red Scare reemerged with even greater vigor.

The fires were fanned significantly in 1950 by Senator Joseph McCarthy (R-Wisconsin), who was using this national concern as the foundation for his floundering reelection bid to the Senate. McCarthy railed against the American Communist Party and called for expulsion from government, education, and the entertainment industry of anyone who was an avowed—or even suspected—communist or communist sympathizer.<sup>113</sup> Because of the fear of the Soviet Union among the American public at this time, the war on communism resonated well.

Responding to expressions of public and governmental concern, local law enforcement agencies began creating intelligence dossiers on persons who were suspected communists and communist sympathizers. These dossiers often became known as the “Red Files.”<sup>114</sup> Thus, law enforcement agencies were keeping records about people who were expressing political beliefs and people who were known to sympathize with these individuals. The fact that these people were exercising their First Amendment constitutional rights and had not committed crimes was not considered an issue because it was felt that the presence of and support for communism within the nation was a threat to the national security of the United States.<sup>115</sup> Indeed, in the spirit of the times, keeping track of communists seemed like a duty law enforcement must fulfill. Moreover, there was support from the vast majority of the community that the government should keep track of communists and their activities. Finally, during this period the exercise of expression

---

111 <https://www.fbi.gov/history/famous-cases>

112 <https://www.trumanlibrary.gov/education/presidential-inquiries/house-un-american-activities-committee>

113 <https://millercenter.org/the-presidency/educational-resources/age-of-eisenhower/mcarthyism-red-scare>

114 Many major city police departments had “Red Squads,” intelligence units specializing in infiltrating, conducting countermeasures, and gathering information on political and social groups to include identifying people and documenting their activities and statements. Lawsuits shut down Red Squads in several cities, with other cities voluntarily shutting down the squads after seeing the proverbial writing on the wall.

115 It was rationalized that such activities were warranted on the grounds of a “compelling state interest.” This argument, however, did not meet constitutional scrutiny.

under the First Amendment was simply not as robust and government authorities were not challenged as they are today. Consequently, the constitutional freedom of speech did not have the resilience it now has.

The dossier system had become an accepted tool for law enforcement intelligence; hence, when new perceived threats emerged, it was natural for law enforcement to rely on this well-established mechanism for keeping information about people perceived to be a threat to community safety. In the 1960s, law enforcement met two challenges where intelligence dossiers appeared to be an important tool: the Civil Rights Movement and the anti-Vietnam War movement. In both cases, supporters of these movements appeared to be on the fringe of 1960s mainstream society. They were vocal in their views and both their exhortations and nontraditional actions (including public demonstrations) appeared to many as being un-American. This was aggravated by other social trends: World War II baby boomers were in their teens and twenties, exploring their own newly defined world of sex, drugs, and rock 'n' roll, contributing to the widely held stereotype of the long-haired, dope-smoking, commie-hippie spy—a sure target for a law enforcement traffic stop.

The overlap among these social movements was viewed by many as being conspiratorial. Moreover, rapidly changing values, stratified in large part along generational and racial lines, created a sense of instability that appeared threatening to the mainstream. Rather than being culturally unstable, as we have learned in hindsight, it was simply social evolution.<sup>116</sup> Because of the dissonance in the 1960s and the largely unsupported assumption that many of the activists and protestors might commit crimes or might be threats to our community security, law enforcement agencies began developing dossiers on these individuals just in case. The dossier information typically was not related to specific crimes; rather, it was kept as a contingency should the information be needed in some future investigation. Names, addresses, phone numbers, associates, relatives, organizations they belonged to, schools and colleges attended, and public statements and actions were among the types of information that were kept in the dossiers. There is little doubt that law enforcement was creating and keeping these dossiers with good faith to protect the community from activities that were viewed as threats; however, that good faith was not consistent with what we recognize today as constitutional practices.<sup>117</sup>

There was additional concern during this time because of the activist nature of the U.S. Supreme Court during the era of Chief Justice Earl Warren (1953–1969).<sup>118</sup> Many of the “liberal decisions” of the Warren Court were met with disfavor and the often-expressed belief that the court’s decisions<sup>119</sup> were “handcuffing the police.” With regard to the current discussion, perhaps most important was that the Warren Court led a generation of judicial activism and expanded interpretations of the Constitution. Moreover, it symbolically motivated activist attorneys from the 1960s to try new strategies for the protection of constitutional rights. Among the most successful was reliance on a little-used provision of the Civil Rights Act of 1871, codified as Title 42 U.S. Code, Section 1983—Civil Action for Deprivation of Civil Rights.

Commonly referred to as “1983 suits,” this provision essentially provides that anyone who, acting under color of state or local law, causes a person to be deprived of rights guaranteed by the U.S. Constitution or federal law may be civilly liable.<sup>120</sup> The initial lawsuits focused on whether a city, police department, or individual officers could be sued for depriving a person of his or her constitutional rights. The Supreme Court held that they could. A significant aspect

---

116 A wide range of research has been published on different aspects of this issue. As a resource, see Leicht, K. (2018). “Social Change.” *Oxford Bibliographies*. <https://www.oxfordbibliographies.com>

117 For perspective, most of these police practices had not yet been litigated; hence police actions were not in defiance of law per se.

118 <https://supremecourthistory.org/history-of-the-court-history-of-the-courts/history-of-the-courts-the-warren-court-1953-1969/>

119 Among the most often cited are *Miranda v. Arizona*—police officers must advise arrestees of their Fifth and Six Amendment rights prior to a custodial interrogation; *Mapp v. Ohio*—applying the Exclusionary Rule to the states; *Gideon v. Wainwright*—right to appointed counsel; and *Escobedo v. Illinois*—right to counsel when the process shifts from investigatory to accusatory.

120 <https://www.fjc.gov/sites/default/files/2014/Section-1983-Litigation-3D-FJC-Schwartz-2014.pdf>

of the case was that the police could be sued if there was “misuse of power possessed by virtue of state law and made possible only because the wrongdoer is clothed with the authority of state law.”<sup>121</sup> This opened the proverbial floodgates for lawsuits against law enforcement (and correctional institutions).

Initial lawsuits focused on various patterns of police misconduct; for example, excessive force and due process violations. The reach of lawsuits against law enforcement grew more broadly with decisions holding that the police chain of command could be held vicariously liable for the actions of those under their command, as well as their parent jurisdictions.<sup>122</sup> Moving into the late 1960s and early 1970s, this movement of lawsuits reached toward law enforcement intelligence units. It was increasingly discovered that law enforcement agencies were keeping intelligence files on people for whom there was no evidence of criminality. Even more egregious was that law enforcement was focusing on unpopular but constitutionally protected speech and expressive activity as the factor to create a dossier. The practice of law enforcement agencies keeping intelligence dossiers only for contingencies, and not for criminal prosecutions, was found to be improper, serving no compelling state interest and depriving those citizens of their constitutional rights. As a result, the courts repeatedly ordered intelligence files to be purged from police records and in many cases police agencies had to pay damage awards to plaintiffs. The decisions also permitted citizens to gain access to their own records. Many activists publicized their intelligence files as a badge of honor, often to the embarrassment of the police.<sup>123</sup> Law enforcement intelligence operations were cut back significantly or eliminated as a result of the embarrassment and costs associated with these lost lawsuits. The lessons learned from this era suggest caution in the development of intelligence records—information must be collected, retained, reviewed, purged, and disseminated in a manner that is consistent with legal and ethical standards.

This lesson is reinforced by the findings of the United States Senate Select Committee to Study Government Operations<sup>124</sup>—the Church Committee, named after its chairman, Frank Church (D-Idaho)<sup>125</sup>—which held extensive hearings on domestic intelligence, most notably the Federal Bureau of Investigation’s (FBI) Counter Intelligence Program (COINTELPRO),<sup>126</sup> which spanned the years from 1959 to 1971. The committee concluded that:

Domestic intelligence activity has threatened and undermined the Constitutional rights of Americans to free speech, association and privacy. It has done so primarily because the Constitutional system for checking abuse of power has not been applied.

Concern was widespread about all aspects of intelligence. The combined effect of these diverse factors prompted the U.S. Department of Justice (DOJ) to develop guidelines for the management of criminal intelligence records that were maintained by state and local law enforcement agencies.

Codified as 28 CFR<sup>127</sup> Part 23—Criminal Intelligence Records Systems Operating Policies<sup>128</sup>—the regulation governs interjurisdictional and multijurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies and that are funded with federal funds. The regulation, created in 1979, stemmed from an amendment to the Omnibus Crime Control and Safe Streets Act of 1968.

---

121 *Monroe v. Pape* 365 U.S. 167 (1961).

122 <https://fedsoc.org/commentary/publications/municipal-liability-under-section-1983-the-importance-of-state-law>

123 For example, it was not uncommon to find notations and even photographs of an “intelligence target” having dinner or attending a public event such as a movie or the theater. The citizen would then pose a rhetorical question: “Is this how you want your tax dollars spent?”

124 United States Senate Select Committee to Study Government Operations. (1976). *Intelligence Activities: Final Report*. Washington, DC: Library of Congress.

125 Also known as the Church Commission.

126 <https://vault.fbi.gov/cointel-pro>

127 Code of Federal Regulations.

128 <http://www.iir.com/28cfr/>

The Justice Systems Improvement Act of 1979 created significant changes in DOJ organizations and stimulated regulatory changes, including creation of this regulation by the DOJ Office of Legal Policy. The regulation arose out of concern for aggressive information collection and intelligence activities by state and local law enforcement agencies frequently involving the collection and retention of information about citizens who were expressing unpopular beliefs but whose actions were not criminal.

Since the federal government cannot mandate policy to state and local governments, the only method that such policy could leverage was to make the policy implementation a condition for the acceptance of federal funds. The regulation provides guidelines on the collection, retention, review, dissemination, and purging of criminal intelligence records. Essentially, the regulation requires that before information that identifies an individual or an organization may be retained in the criminal intelligence records system of a state or local law enforcement agency, there must be sufficient evidence to establish a reasonable suspicion that the individual is involved in criminal behavior. When the regulation was created, many in law enforcement viewed this as a significant barrier to effective intelligence operations. However, hindsight has proven the regulation to be an important tool for the maintenance of citizens' civil rights without placing an undue burden on intelligence activities. Indeed, despite the fact that the required application of the regulation applies to only a small portion of U.S. law enforcement agencies, the *National Criminal Intelligence Sharing Plan*<sup>129</sup> recommends that all agencies that have a criminal intelligence records system follow the 28 CFR Part 23 guidelines as a matter of good practice.

## CONGRESSIONAL INQUIRIES OF INTELLIGENCE ACTIVITIES

During this era, inquiries into the Intelligence Community moved away from assessing the efficiency of intelligence operations and toward assessing the legality and propriety of the actual operations conducted. As will be seen, the recommendations made by three congressional committees would result in major changes in both the jurisdiction and the roles of IC members with respect to law enforcement and national security intelligence. This would lead to the separation of the two types of intelligence activities—the so-called “wall between domestic and international intelligence.”<sup>130</sup>

In 1975, the Rockefeller Commission recommended limiting the CIA's authority to conduct domestic intelligence operations. Furthermore, the commission recommended that the director of Central Intelligence (DCI) and the director of the FBI set jurisdictional guidelines for their respective agencies. In 1976, the House Select Committee on Intelligence (the Pike Committee, chaired by Representative Otis Pike, D-New York) also made recommendations to further limit the jurisdictional overlap between agencies responsible for national security intelligence and agencies primarily responsible for law enforcement intelligence. It was the recommendations of the Church Committee, however, that were the most profound in developing the wall of separation.

The Church Committee, in an inquiry formed by the U.S. Senate in 1976, examined the conduct of the IC in a broader fashion than did the Rockefeller Commission.<sup>131</sup> The recommendations made by this inquiry led to jurisdictional reformations of the IC. Most of the recommendations were directed at developing new operational boundaries for the FBI and the CIA. Of the committee's 183 recommendations, the following illustrate how law enforcement intelligence was separated from national security intelligence:<sup>132</sup>

- ◆ The committee recommended that agencies such as the NSA, the CIA, and military branches not have the power to conduct domestic intelligence operations (i.e., law enforcement intelligence functions). Specific

---

129 <https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>

130 <https://fas.org/irp/eprint/wall.pdf>

131 Johnson, L. (1985). *A Season of inquiry: The Senate intelligence investigation*. Lexington, KY: The University Press of Kentucky.

132 For a complete review of the recommendations made by the Church Committee, visit <https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm>, or, for a more complete review of the formation of the Church Committee, see note 14.

attention was given to the role of the CIA, noting that “the CIA should be prohibited from conducting domestic security activities within the United States.”

- ◆ The committee recommended that the FBI have “sole responsibility” in conducting domestic intelligence investigations of Americans.
- ◆ The FBI should “look to the CIA as the overseas operational arm of the intelligence community.”<sup>133</sup>
- ◆ All agencies should ensure against improper intelligence activities.

The recommendations of the Church Committee have been widely recognized as a primary reason for the separation of law enforcement intelligence from national security intelligence. The call for this separation, however, did not mean that the agencies should stop working with each other. In fact, the Church Committee also recommended that the FBI and the CIA continue sharing information and make a better effort to coordinate their initiatives. This was operationally complicated: How do the two agencies work together and coordinate initiatives when there are substantial limitations on the kinds of information that can be collected and shared? Moreover, what, if any, impact did this stovepiping of information have on state, local, and tribal law enforcement (SLTLE) intelligence? (It essentially eliminated information sharing on threats.) The result was increased compartmentalization both between the agencies and within each agency.<sup>134</sup> As would be seen in the *9/11 Commission Final Report*, this rigid compartmentalization was blamed in part as the intelligence failure that preceded the 9/11 attacks.

## NATIONAL CRIME COMMISSIONS AND NEW INITIATIVES INFLUENCING THE EVOLUTION OF SLTLE INTELLIGENCE

Since 1931, there have been 16 national initiatives in the United States examining a wide array of crime and justice issues, ranging from street crime and drug trafficking to organized crime, terrorism, and police use of force. Many of these have included assessments and recommendations related to some aspect of law enforcement intelligence. Understanding the broad intent of the commissions followed by those with specific intelligence recommendations demonstrates a well-established legacy for establishing law enforcement intelligence operations that are objective, analytic, and respectful of privacy and civil rights. While the recommendations reflect forward thinking, not all recommendations were immediately embraced—largely because they represented a change in the police occupational culture of the era. Nonetheless, important concepts were established that served as the foundation for today’s law enforcement intelligence practices.

### THE COMMISSIONS AND THEIR PURPOSE

The National Commission on Law Observance and Enforcement<sup>135</sup> (known as the Wickersham Commission) issued a series of reports and memoranda from 1928 to 1931 examining all aspects of serious crime in the United States. The intent was to address the growth of organized crime (particularly that arising from Prohibition) and increases in violent crime that appeared to be correlated with growing industrialization and urbanization. The commission also sought to understand the failure of law enforcement, the courts, and corrections to effectively manage America’s crime problem. For the next three decades, there were no major national commissions examining crime—due in

---

133 Ibid.

134 For example, because of the regulations—or at least the interpretation of the regulations—FBI agents working within the former Foreign Counter Intelligence Division (FCI) were often barred from sharing information with agents working on criminal investigations.

135 <https://www.ncjrs.gov/pdffiles1/Digitization/44540NCJRS.pdf>

large part, no doubt, to America's preoccupation with the Great Depression, followed by World War II, and post-World War II concerns about the growing nuclear threat from the Soviet Union. Indeed, these global events were largely responsible for the lack of implementation of virtually all of the Wickersham Commission's recommendations.

In November 1963, the assassination of President John F. Kennedy prompted President Lyndon Johnson to create what came to be known as the Warren Commission.<sup>136</sup> While the commission's goal was to determine the circumstances leading to the assassination, the less controversial results of the commission examined the relationships among federal, state, and local law enforcement, their communications, and generally their ability to work together for a common purpose: protecting the President of the United States. Unknown to anyone at the time, the assassination was a harbinger of a violent and paradigm-changing decade to come.

As the 1960s progressed, increased concern about crime was emerging because of the growth of violence, the increase in illegal drug use, the greater awareness of organized crime, and concerns about inequities in the administration of justice, particularly as related to minorities. To address these concerns, in 1965 President Johnson created the President's Commission on Law Enforcement and Administration of Justice—an inquiry that complemented his domestic social agenda, known as The Great Society.<sup>137</sup> The President's Commission investigated all aspects of the criminal justice system, summarized in its title volume, *The Challenge of Crime in a Free Society*.<sup>138</sup> As part of the commission's work, specific inquiries were made into a number of explicit issues and reported in a series of task force reports addressing such issues as the courts, correction, victims, narcotics, and organized crime that were released in 1967, including a specific *Task Force Report: Police*.<sup>139</sup>

Because the 1960s were seen as the "decade of social revolution" on many fronts, there were concerns ranging from violence and riots in our cities to increases in the use of narcotics, the growth of illegal dangerous drugs, and concerns about moral decay, often illustrated by the increasing presence of pornographic materials. In 1967, resulting from a series of violent demonstrations in cities throughout the United States spurred by the Civil Rights Movement, the National Advisory Commission on Civil Disorders<sup>140</sup> (known as the Kerner Commission) was created in an attempt to understand the dynamics of civil disobedience and civil disorders, as well as to evaluate the government's response. The following year saw two additional commissions created. The first was the National Commission on the Causes and Prevention of Violence, its final report titled *To Establish Justice, To Ensure Domestic Tranquility*,<sup>141</sup> with a number of specially focused subsidiary reports.<sup>142</sup> Also created in 1968 was the U.S. Commission on Obscenity and Pornography, which issued nine volumes<sup>143</sup> of reports and its primary *Technical Report*.<sup>144</sup>

The social upheaval of the 1960s was characterized by many factors, including a significant rise in the abuse of illegal drugs, as learned in earlier commission reports. As a result, a new inquiry was created specifically to examine this issue more closely in a series of reports published in subsequent years: the U.S. Commission on Marihuana and Drug Abuse<sup>145</sup> (1970).

One of the signature components of the 1967 President's Commission was the attempt to professionalize all aspects of the criminal justice system. Following this lead was the U.S. Justice Department's National Advisory Commission

---

136 <https://www.archives.gov/research/jfk/warren-commission-report>

137 <https://www.history.com/topics/1960s/great-society>

138 <https://www.ncjrs.gov/pdffiles1/nij/42.pdf>

139 <https://www.ncjrs.gov/pdffiles1/Digitization/147374NCJRS.pdf>

140 <https://www.ncjrs.gov/pdffiles1/Digitization/8073NCJRS.pdf>

141 <https://ia800700.us.archive.org/30/items/toestablishjusti00unit/toestablishjusti00unit.pdf>

142 <https://onlinebooks.library.upenn.edu/webbin/book/lookupname?key=United%20States%2E%20National%20Commission%20on%20the%20Causes%20and%20Prevention%20of%20Violence>

143 <https://catalog.hathitrust.org/Record/001108277>

144 <https://babel.hathitrust.org/cgi/pt?id=mdp.39076006957786&view=1up&seq=7>

145 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1749335/>

on Criminal Justice Standards and Goals, which produced multiple volumes of work<sup>146</sup> (1973), as well as a series of reports from the successor to the commission, the National Advisory Committee on Criminal Justice Standards and Goals<sup>147</sup> (1976).

National inquiries, seeking to identify causes of various crimes as well as providing blue-ribbon advice on the best tactics, recommended strategies and programs to deal with crime. These included the Attorney General's Task Force on Violent Crime<sup>148</sup> (1981); the President's Commission on Organized Crime<sup>149</sup> (1983); and the Attorney General's Commission on Pornography<sup>150</sup> (1986), which included an investigation into the link between pornography and organized crime.

Throughout the 1990s, there were no national commissions on crime issues, as had been so prevalent in the previous three decades. However, there was a significant increase in government sponsored research and program development on a wide array of crime-related issues from the National Institute of Justice<sup>151</sup> (NIJ), the Bureau of Justice Assistance<sup>152</sup> (BJA), the Bureau of Justice Statistics<sup>153</sup> (BJS), the Office of Juvenile Justice and Delinquency Prevention<sup>154</sup> (OJJDP), and the newest U.S. Justice Department agency, the Office of Community Oriented Policing Services<sup>155</sup> (COPS), created in 1994. In many ways, the research and products developed by these agencies served as surrogates for those created by the national commissions.

In the late 1990s, there was a growing concern over terrorism, particularly after attacks on the U.S. military and the U.S. Embassy bombings in Africa, as well as a general increase in terrorist attacks throughout the Middle East. As a result, the U.S. Congress mandated a five-year annual inquiry into the susceptibility of the United States to attacks using weapons of mass destruction (WMDs). The body spearheading this inquiry, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Commission), issued its first report in 1999.

In 2004, as a follow-up to the 2001 terrorist attacks using airplane hijackings in New York, Washington, and Pennsylvania, the Gilmore Commission issued its report, which had significant implications for law enforcement at all levels of government but addressed much wider issues: the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). As will be seen, the 9/11 Commission's recommendations had a significant impact on both legislation and policy with respect to both law enforcement intelligence and national security intelligence.

In 2015, following a number of high-profile officer-involved shootings, mostly involving persons of color, and subsequent public demonstrations against the police use of force and law enforcement's perceived lack of responsive to community concerns, President Obama created the President's Task Force on 21st Century Policing.<sup>156</sup> While some critics argued that the task force members and their approach were intended to give a vision of objectivity to what was viewed as a political agenda, professional law enforcement largely embraced the task force recommendations, particularly de-escalation of force. While virtually all previous national commissions on crime and justice were viewed as professional and objective, the latest task force fell victim in some ways to the highly politicized environment of the decade.

---

146 <http://worldcat.org/identities/lccn-n50067996/>

147 <http://id.loc.gov/authorities/names/n77000055.html>

148 <https://catalog.hathitrust.org/Record/002194587>

149 <https://www.ncjrs.gov/pdffiles1/Digitization/96374NCJRS.pdf>

150 <https://catalog.hathitrust.org/Record/000824987>

151 <https://nij.ojp.gov/>

152 <https://www.bja.gov/default.aspx>

153 <https://www.bjs.gov/>

154 <https://www.ojjdp.gov/>

155 <https://cops.usdoj.gov/>

156 [https://cops.usdoj.gov/pdf/taskforce/taskforce\\_finalreport.pdf](https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf)

In 2019, the President issued an executive order creating the *President's Commission on Law Enforcement and Administration of Justice*.<sup>157</sup> This is the first comprehensive, systemwide criminal justice endeavor to examine crime in over 50 years. Like previous commissions, this effort is examining the current status of crime and the criminal justice system's responses. Unlike previous commissions, there is a solid body of empirical research that provides evidence-based solutions to many crime problems. Moreover, some of the research offers important insights about policies that work and those that do not. Since 1967, the character of crime and responses to crime have significantly changed as a result of technology. Global organized crime has expanded significantly, with the Latin American drug cartels far overtaking the Italian-Sicilian Mafia organizations as the most pervasive criminal enterprises in the world.

At its core, the commission examined:

- ◆ How do certain social ills such as mental illness, substance abuse, and homelessness affect the ability of law enforcement to police?
- ◆ How can we improve officer recruitment, training, and retention?
- ◆ What are the major issues confronting rural and tribal law enforcement?
- ◆ What are the major issues affecting the physical safety and mental health of police officers?
- ◆ How can federal grant programs aid SLTLE?
- ◆ What novel issues and criminal threats have arisen from new technologies?
- ◆ What is the cause of diminished respect for law enforcement and the laws they enforce, and how does it affect both police and public safety?
- ◆ What role can commercial business and community development organizations play in cultivating safe communities?
- ◆ What methodologies, techniques, and targeted deterrence can be employed to reduce crime?
- ◆ How can we integrate education, employment, social services, and public health services to reduce crime and ease the burden on law enforcement?

In studying these issues, the commission was assisted by working groups consisting of subject-matter experts across federal, state, and local government. The working groups assisted and facilitated the commission's study of these issues and provided advice and counsel on their specific subjects. As will be seen in a later discussion, a number of the issues directly or collaterally addressed law enforcement intelligence.

#### TABLE 2-1: SUMMARY OF NATIONAL CRIME COMMISSIONS

- ◆ National Commission on Law Observance and Enforcement (Wickersham Commission), 1931
- ◆ President's Commission on the Assassination of President Kennedy (Warren Commission), 1964
- ◆ President's Commission on Law Enforcement and Administration of Justice, 1967
- ◆ National Advisory Commission on Civil Disorders (Kerner Commission), 1967
- ◆ National Commission on the Causes and Prevention of Violence, 1968
- ◆ Commission on Obscenity and Pornography, 1968
- ◆ Commission on Marihuana and Drug Abuse, 1970
- ◆ National Advisory Commission on Criminal Justice Standards and Goals, 1973
- ◆ National Advisory Committee on Criminal Justice Standards and Goals, 1976

157 *The President's Commission on Law Enforcement and Administration of Justice*. (2020). Washington, DC: U.S. Department of Justice. <https://www.justice.gov/file/1347866/download>

- ◆ National Advisory Committee for Juvenile Justice and Delinquency Prevention, 1980
- ◆ Attorney General’s Task Force on Violent Crime, 1981
- ◆ President’s Commission on Organized Crime, 1983
- ◆ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), 1999
- ◆ National Commission on Terrorist Attacks Upon the United States (9/11 Commission), 2004
- ◆ The President’s Commission in 21st Century Policing (2015)
- ◆ President’s Commission on Law Enforcement and Administration of Justice (2020)

## THE NATIONAL CRIME COMMISSIONS AND LAW ENFORCEMENT INTELLIGENCE

Not all of these commissions directly addressed the issue of intelligence; however, they all called for increased use of diverse analytic techniques, not only to understand crime and criminal justice but also to aid in forecasting crime for purposes of prevention—a fundamental construct of the intelligence process.

The Wickersham Commission observed that there was a need to study and understand the crime environment (i.e., analysis) as an important tool to capture criminal offenders. Thirty-three years later, one of the earliest explicit recommendations for intelligence and information sharing between federal agencies and state and local law enforcement came from the 1964 President’s Commission on the Assassination of President Kennedy (the Warren Commission). While the majority of the commission’s recommendations were directed at federal agencies, notably the Secret Service and the FBI, it also recommended that these agencies work more closely with local law enforcement. Specifically, the commission called for increased information sharing and stronger liaison between local and federal agencies.<sup>158</sup>

The 1967 President’s Commission reports emphasized many of the same factors; however, they provided significantly more research, more detail, and explicit recommendations. Moreover, in the year following the release of the President’s Commission reports, Congress passed landmark legislation—the Omnibus Crime Control and Safe Streets Act of 1968—which, among other things, provided funding for many of the commission recommendations to be implemented. Within the intelligence arena, the commission recommended the following:

Police departments in every major city should have a special intelligence unit solely to ferret out organized criminal activity and to collect information regarding the possible entry of criminal cartels into the area’s criminal operations.<sup>159</sup>

Interestingly, the commission noted that “criteria for evaluating the effectiveness of the [intelligence] units, other than mere numbers of arrests, must be developed.”<sup>160</sup> That debate remains. The President’s Commission went on to recommend that the “. . . Department of Justice should give financial assistance to encourage the development of efficient systems for regional intelligence gathering, collection and dissemination.”<sup>161</sup> This would become a reality roughly a decade later, when the Regional Information Sharing System (RISS) Program and its six geographic centers were established.<sup>162</sup>

---

158 The Warren Commission Report. (2003). *Report of the President’s Commission on the Assassination of President John F. Kennedy*. New York: Barnes and Noble, Inc. [Originally published in 1964].

159 President’s Commission on Law Enforcement and Administration of Justice. (1967). *Task Force Report: Organized Crime*. Washington, DC: U.S. Government Printing Office, p. 20.

160 Ibid.

161 Ibid., p. 22.

162 See <http://www.riss.net/>.

While the intelligence focus of the President’s Commission was largely on organized crime and, to a lesser extent, on narcotics control, the Kerner Commission’s focus was on civil disobedience and violent civil disorders. With respect to the riots and civil disorders experienced by America’s cities, the commission observed that:

No particular control tactic was successful in every situation. The varied effectiveness of control techniques emphasizes the need for advance training, planning, adequate intelligence systems, and knowledge of the [inner-city].<sup>163</sup>

Further, the commission recommended that law enforcement agencies should:

Establish an intelligence system to provide police and other public officials with reliable information that may help to prevent the outbreak of a disorder and to institute effective control measures in the event a riot erupts.<sup>164</sup>

The National Commission on the Causes and Prevention of Violence made similar observations. It noted that:

A major weakness of many police departments is the absence of a reliable intelligence system. The absence has gravely handicapped police and public officials in anticipating and preventing trouble, and in minimizing and controlling a disorder that has broken out. In large part, this happens because of a failure to learn about and to understand neighborhood problems and grievances and to develop reliable information concerning community organizations and leaders. Related to this problem is the need for a reliable mechanism to monitor, to collect and to evaluate rumors and also the need for an effective program to counter false and provocative rumors which can aggravate tension and incite violence.<sup>165</sup>

The recognition that intelligence could be a valuable tool for forecasting threats and dealing with complex criminality was slowly growing as a wide range of systemic crime-related social problems were examined by these national inquiries. Intelligence was being viewed more broadly, as evidenced by the most comprehensive recommendation yet from the National Advisory Commission on Criminal Justice Standards and Goals (NAC). The NAC developed a standard expressly for intelligence operations—ironically, it is Standard 9.11—that states, in part:

Every police agency and every state immediately should establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner which protects every individual’s right to privacy while it curtails organized crime and public disorder.<sup>166</sup>

The standard is remarkably similar to a recommendation from the *National Criminal Intelligence Sharing Plan*, released 31 years later. Interestingly, the standard notes that information is collected, and intelligence is disseminated. This reference to analysis had not been clearly articulated previously in the commission reports. Moreover, the attention to individual privacy that was included in the standard is also an important ingredient that is critical to all law enforcement intelligence activities today.

Furthermore, included in the commission’s report were recommendations directed at the structure and operations of the intelligence functions for state and local law enforcement agencies. These recommendations included the following:

---

163 National Advisory Commission on Civil Disorders. (1968). *Summary Report*. Washington, DC: U.S. Government Printing Office, p. 6.

164 *Ibid.*, p. 16.

165 National Commission on the Causes and Prevention of Violence. (1968). *Law and Order Reconsidered*. Washington, DC: U.S. Government Printing Office, p. 312.

166 National Advisory Commission on Criminal Justice Standards and Goals. (1973). *Police*. Washington, DC: U.S. Government Printing Office, p. 250.

## Establishing Intelligence Functions

- ◆ Each state should develop a centralized law enforcement intelligence function with the participation of each police agency within the state.<sup>167</sup>
- ◆ States should consider establishing regional intelligence networks across contiguous states to enhance criminal information sharing processes.<sup>168</sup>
- ◆ Every local law enforcement agency should establish its own intelligence function in accordance with its respective state's intelligence function.<sup>169</sup>

## Intelligence Function Operations

- ◆ Each state and local intelligence function should provide support to federal agencies.
- ◆ Operational policies and procedures should be developed for each local, state, and regional intelligence function to ensure efficiency and effectiveness.<sup>170</sup> Each agency should have a designated official who reports directly to the chief and oversees all intelligence operations.
- ◆ Each agency should develop procedures to ensure the proper screening, securing, and disseminating of intelligence-related information.<sup>171</sup>

In 1976, the concept and operating policies for intelligence were expanded even further by the National Advisory Committee for Criminal Justice Standards and Goals. The committee's publication, *Task Force Report on Organized Crime*, has a complete chapter on intelligence and provides more detail than any previous commission or inquiry. Beyond recommendations for the creation of an intelligence unit, the standards include recommendations for maintaining privacy, the use of the need-to-know and right-to-know standards for dissemination, intelligence records purging standards, and the need to maintain individual and organizational accountability in the intelligence function.<sup>172</sup> While the recommendations focus on organized crime, including drug trafficking, compared with the all-crimes, all-hazards approach used by law enforcement in the post-9/11 environment, many of the 1976 standards and discussions of intelligence are consistent with today's vision of good practice in law enforcement intelligence.

Created in 1983, the President's Commission on Organized Crime was a comprehensive examination of all aspects of organized crime ranging from traditional organized crime (e.g., the Mafia, La Cosa Nostra) to drug-trafficking cartels,<sup>173</sup> sophisticated money-laundering operations, and entrepreneurial crime of all types and commodities. The intent was to provide a comprehensive insight about organized crime, its structure, its effects, and how best to control it. It was recognized that a critical tool for law enforcement to successfully deal with multijurisdictional complex criminality was effective intelligence analysis.<sup>174</sup>

By the mid-1980s, criminal enterprises had grown dramatically and encompassed a diverse array of illegal activities, from drug trafficking to counterfeiting consumer goods. Investigators and intelligence units had neither the expertise

---

167 Ibid.

168 National Advisory Commission on Criminal Justice Standards and Goals. (1976). *Report of the Task Force on Organized Crime*. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration.

169 Ibid.

170 Ibid.

171 National Advisory Commission on Criminal Justice Standards and Goals. (1976). *Report of the Task Force on Disorder and Terrorism*. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration.

172 National Advisory Committee for Criminal Justice Standards and Goals. (1976). *Task Force Report on Organized Crime*. Washington, DC: U.S. Government Printing Office, pp. 121–135.

173 At this time, the Colombian drug cartels were significantly growing and were a harbinger for decades-long violent and aggressive drug production and trafficking from Colombia and Mexico.

174 President's Commission on Organized Crime. (1984). *Organized Crime and Money Laundering*. Washington, DC: U.S. Government Printing Office, 1984.

nor the personnel to contain the problem effectively. This was aggravated by a failure of law enforcement to generally understand the nature of organized crime and by poor information sharing between law enforcement agencies at all strata of government.<sup>175</sup> Organized crime was characterized as a “rapidly changing subculture” that was outpacing the capability of law enforcement to control it. Increasingly, organized crime was viewed largely as a federal responsibility that would be supported by state and local law enforcement through information sharing and participation on task forces.

Similar to the issues of organized crime, the Attorney General’s Commission on Pornography (1986) recognized that intelligence operations would be a useful tool for stopping interstate traffic in obscene and pornographic materials. However, state and local law enforcement tended to view this as a low priority and not a good investment of time and resources.

In the 1990s, following an increased number of terrorist attacks in the Middle East, and particularly after the bombings of U.S. embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, questions began to emerge about the U.S. mainland as a terrorist target and the ability of the United States to effectively forecast, manage, and respond to an attack at home—particularly an attack involving weapons of mass destruction (WMDs). As a result, in 1999, Congress mandated the creation of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission). The annual reports issued from 1999 to 2003 went beyond WMDs and explored terrorism more broadly—particularly after 9/11—and what the U.S. government needed to do to effectively protect the homeland. In addition to recommending more robust intelligence and information sharing, the commission urged policymakers to move beyond simply reacting to the September 11, 2001, terrorist attacks and to develop forward-thinking efforts by government at the federal, state, and local levels, as well as by the private sector. In its 2002 report, the Gilmore Commission stated:

Intelligence—its timely collection, thoughtful analysis, and appropriate dissemination—is the key to effective prevention of terrorist attacks. From the inception of our deliberations, we have said that “more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats.” While improvements have been made, that statement is still true today.<sup>176</sup>

That message was reinforced, particularly with regard to information sharing, in a staff report from the 9/11 Commission. One issue of concern was the effectiveness of information sharing by the FBI with state and local law enforcement. The commission’s staff report stated, in part:

We heard complaints that the FBI still needs to share much more operational, case-related information. The NYPD’s Deputy Commissioner for Counterterrorism, Michael Sheehan, speculated that one of the reasons for deficiencies in this information sharing may be that the FBI does not always recognize what information might be important to others. . . . Los Angeles Police Department officials complained to us that they receive watered-down reports from the FBI. . . . We have been told that the FBI plans to move toward a “write to release” approach that would allow for more immediate and broader dissemination of intelligence on an unclassified basis.<sup>177</sup>

These issues are being addressed through the *National Criminal Intelligence Sharing Plan* (NCISP), specifically through the development of law enforcement intelligence requirements by the FBI. Moreover, former FBI Executive

175 President’s Commission on Organized Crime. (1987). *Final Report*. Washington, DC: U.S. Government Printing Office.

176 Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (2002). *Implementing the National Strategy*. Washington, DC: The Rand Corporation, p. 30.

177 National Commission on Terrorist Attacks Upon the United States (2004). *Staff Statement No. 12: Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States*, p. 8. [https://govinfo.library.unt.edu/911/staff\\_statements/staff\\_statement\\_12.pdf](https://govinfo.library.unt.edu/911/staff_statements/staff_statement_12.pdf).

Assistant Director for Intelligence Maureen Baginski stated in remarks at the 2004 COPS National Community Policing Conference that included in the initiatives of the FBI Office of Intelligence was a revised report-writing style that would facilitate information sharing immediately, including with those intelligence customers who did not have security clearances.<sup>178</sup>

Interestingly, the 9/11 Commission's staff report on reformation of the intelligence function included many of the issues and observations identified in previous national commission reports over the previous 40 years. The difference, however, is that substantive change was actually occurring, largely spawned by the tragedy of September 11, 2001.

*The 9/11 Commission Final Report* issued a wide range of recommendations related to intelligence. Cooperative relationships, the integration of intelligence functions, and a general reengineering of the intelligence community were at the heart of their recommendations. In commentary, the commission noted the role of SLTLE agencies, stating:

There is a growing role for state and local law enforcement agencies. They need more training and work with federal agencies so that they can cooperate more effectively with those authorities in identifying terrorist suspects.<sup>179</sup>

The commission went on to recognize that:

The FBI is just a small fraction of the national law enforcement community in the United States, a community comprised mainly of state and local agencies. The network designed for sharing information, and the work of the FBI through local Joint Terrorism Task Forces, should build a reciprocal relationship in which state and local agents understand what information they are looking for and, in return, receive some of the information being developed about what is happening, or may happen, in their communities.<sup>180</sup>

The commission also recommended creation of a new domestic intelligence entity that would need to establish “. . .relationships with state and local law enforcement. . . .”<sup>181</sup> In proposing a new National Counterterrorism Center (NCTC), the commission stated that the center should “. . . [reach] out to knowledgeable officials in state and local agencies throughout the United States.”<sup>182</sup> Implicit in the commission's recommendations is that terrorism is a local event that requires critical involvement of state and local government in prevention and response.<sup>183</sup>

Moving into the second decade of the 21st century, counterterrorism was giving way to a broadening focus domestically by other issues: the increasing levels of violence in America, the opioid crisis, and a growing concern about police-community relationships, including a number of controversial officer-involved shootings. Spurred by a growing public outcry, as well as self-examination in the use of force by policing leaders, President Obama commissioned The President's Task Force on 21st Century Policing. While intelligence issues were not a focus of the report, there were two issues of note.

Part of the task force's work was examining communications between the police and community, including the use of social media. This was the first national criminal justice commission initiative convened since the rapid growth of

178 Maureen Baginski, former FBI Executive Assistant Director for Intelligence. Remarks in a keynote address to Community Policing for America's Future: National Community Policing Conference, Office of Community Oriented Policing Services, Washington, DC (June 22, 2004).

179 National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Final Report*. Washington, DC: U.S. Government Printing Office, p. 390. Also available in full online at <http://www.9-11commission.gov/report/911Report.pdf>.

180 Ibid., p. 427.

181 Ibid., p. 424.

182 Ibid., p. 404.

183 Ibid.

social media. The task force reported in a survey of 500 police departments that 100 percent of the agencies had websites and nearly all had or planned to have Facebook and Twitter accounts within the next five years.<sup>184</sup> The report expressly noted that one of the roles of social media is for information gathering in the intelligence process. Another role is to share threat and crime information with the public.

Changes that emerged in policing following this report—with significant leadership from prominent police executives—was growing trust between the police and community and more open communications. Among the ramifications has been a greater willingness for community members to report suspicious activities to police agencies, particularly as related to potential school shootings, mass violence, and domestic terrorism. That information has significant value for intelligence analysis.

Recognizing the growth in firearms violence, the 2020 President’s Commission provided strong support Crime Gun Intelligence Centers, stating. . .

Law enforcement should develop, gather, and leverage all available data and intelligence to identify leaders of gangs or criminal organizations and the principal violent actors within such gangs. In doing so, they should work with correctional facility intelligence teams and share data across jurisdictions and agencies. In addition to coordinating information regarding gangs and violent organizations, law enforcement should develop and amass the intelligence necessary for law enforcement to discern the best use of resources to dismantle violent gangs. This cultivation of data is an important aspect of crime reduction generally, but it is especially important for gang investigations. Crime analysts can provide accurate data (e.g., affiliations, current charges, or social media) to law enforcement officers whose areas are most likely affected by these individuals or groups. Even after an investigation commences, crime analysts can perform the vital role of digesting and assessing investigative data (e.g., wiretaps and other forms of electronic surveillance) to gather evidence against these organizations and organizational leaders. Technology companies should provide access to such information when law enforcement has lawful authority to obtain it, including using court orders. Crime gun intelligence (CGI) tools—such as the Bureau of Alcohol, Tobacco, Firearms and Explosives’ (ATF) National Integrated Ballistics Information Network (NIBIN), firearm tracing, and acoustic gunshot detection technology—are also essential analytical assets for the identification of the most violent criminal organizations and associates.<sup>185</sup>

The commission went on to recommend:

**Recommendation 8.1.3:** Local law enforcement, in collaboration with federal law enforcement, should implement targeted enforcement and patrols in designated and confined geographical areas to gather, collect, and share intelligence on known gang members for arrest and prosecution.<sup>186</sup>

**Recommendation 8.2.3:** Congress should provide additional funding to the Department of Justice to increase the number of National Integrated Ballistic Information Network (NIBIN) sites, and the Department of Justice should provide additional grant funding to the Local Law Enforcement Crime Gun Intelligence Centers Integration Initiative.<sup>187</sup>

---

184 *The President’s Task Force on 21st Century Policing*. (2015). Washington, DC: Office of Community Oriented Policing Services, p. 37.

185 *The President’s Commission on Law Enforcement and Administration of Justice*. (2020). Washington, DC: U.S. Department of Justice, p. 113.

186 *Ibid.*, p. 114.

187 *Ibid.*, p. 119.

**Recommendation 9.2.3:** The Department of Homeland Security and the Federal Bureau of Investigation should provide intelligence training to state and local authorities that focuses on integrating criminal intelligence with national intelligence to better protect the nation.<sup>188</sup>

**Recommendation 11.2.3:** The Department of Justice should provide funding to expand real time crime centers (RTCCs) throughout the nation and develop technology tools that provide RTCCs with the ability to identify and disseminate crime intelligence, analyze crime patterns, and develop strategies for reducing crime.<sup>189</sup> (p. 164)

The inquiries into crime and justice from these various national initiatives have similar themes: Attack the root causes of crime, understand all aspects of the crime dynamic, attack crime from a holistic approach, work with and share information between agencies and the community, move beyond traditional approaches, and protect the privacy and civil rights of individuals. Whether the crime is strong-armed robberies or terrorism, these principles run true. Certainly, the practice of law enforcement intelligence has listened to and learned from these lessons in a frenzy of change during the post-9/11 era.

## THE IMPACT OF PROFESSIONAL ASSOCIATIONS

Professional associations provide important roles for working professionals. They develop accepted standards of practice; provide networking to share ideas and information; aid members in their professional development; provide a common voice of leadership on important issues; provide members with awareness of new techniques and issues during annual meetings; and provide professional camaraderie. While there are many professional police organizations, the current discussion will focus on three that have influenced the current development of law enforcement intelligence.

## LAW ENFORCEMENT INTELLIGENCE UNITS<sup>190</sup> (LEIU)

In the 1950s, the vast majority of American law enforcement agencies did not have an intelligence unit. Those that did had few resources committed to this function, little guidance on how the unit should perform, and, frankly, differing perspectives on the role of the unit, with virtually no best practices on how the unit should accomplish its mission. Fundamentally, intelligence unit members relied on investigative experience and intuition. In general, they focused on complex criminality, mostly transjurisdictional organized crime. When it came to sharing information with other agencies, some departments jealously guarded the information they possessed, while others that wanted to share information were limited by the lack of a central clearinghouse and a virtual absence of technology beyond mail, telephones, and hand-carried intelligence reports.

In 1956, a voluntary sharing system was created by 26 police departments from seven states. The organization, composed of state and local law enforcement agencies, was called the Association of Law Enforcement Intelligence Units (LEIU). Aside from the LEIU, there were still few formalized methods of intelligence information exchange.

As described previously, increasing calls for better intelligence and information sharing from the various national commissions resulted in more agencies developing an intelligence function, often resulting in widely publicized civil liberties complaints, lawsuits, and consent decrees. At the federal and state levels, new policies, laws, and regulations were developed to establish controls on information collection and sharing, but many were unclear on how these would be operationally implemented, particularly to permit information sharing across state lines.

To address this issue, in 1976, the LEIU formulated an early set of file guidelines for criminal intelligence units, followed by the creation of 28 CFR Part 23 by the Justice Department. The LEIU refined its file guidelines to ensure

<sup>188</sup> Ibid., p. 138.

<sup>189</sup> Ibid., p. 164.

<sup>190</sup> <http://www.leiu.org/>

that they were consistent with 28 CFR Part 23 but were also structured to be implementable as policy. These have become the national standard.

The LEIU's membership expanded, and so did its activities. The organization maintains a criminal intelligence clearinghouse that facilitates the timely exchange of confidential information among its 240 local, state, and federal member agencies. Its annual conference provides for certificate training and the opportunity for intelligence professionals to network with other members and their associates. The LEIU also provides its members with evaluation and technical assistance in the formation and organization of their agencies' intelligence function. In addition, the LEIU provides timely publications and appropriate advocacy for professional criminal intelligence standards on the national level as well as annual training events to ensure that the membership has contemporary awareness of relevant issues and trends.

The general chairperson of the LEIU is also a member of the Criminal Intelligence Coordinating Council.

## **INTERNATIONAL ASSOCIATION OF LAW ENFORCEMENT INTELLIGENCE ANALYSTS<sup>191</sup> (IALEIA)**

Before 1980, no organization dedicated to represent analytic personnel in law enforcement existed. To fill this need, a small group of professional intelligence analysts and managers held their inaugural meeting in New Orleans, Louisiana, in October 1981. They created the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA).

These first members represented local, state/provincial, and federal law enforcement agencies in Canada and the United States. Today, IALEIA's membership includes more than 2,500 members representing more than 40 countries. These members are united to promote standards of excellence in law enforcement analysis by enhancing the mutual exchange of ideas, supporting analytical standards, and providing training.

IALEIA has evolved as the role of the law enforcement analyst has matured. The organization strives to capture the intelligence analysis experience of individuals and agencies and to convert and share that knowledge through law enforcement educational products. IALEIA devotes its organizational resources as a leader in training through its international conferences and the Foundations of Intelligence Analysis Training (FIAT) program, which is viewed as the foundational standard for new analysts. To enhance the analyst profession, IALEIA provides a certification program with a designation of criminal intelligence certified analyst (CICA).

Continuing its emphasis on facilitating networking among analysts, IALEIA fosters regional chapters and forged partnerships with the Australian Institute of Professional Intelligence Officers (AIPIO), the LEIU, and the Canadian Association for Security and Intelligence Studies (CASIS). Among its products, IALEIA shares knowledge through the *Journal of Intelligence Analysis*, the *IntelScope* professional newsletter, and the *Law Enforcement Analytic Standards (2011)* and *Criminal Intelligence for the 21st Century (2011)*. The IALEIA president is also a member of the Criminal Intelligence Coordinating Council (CICC) and provides input on all CICC publications, particularly from the perspective of the practicing analyst.

The purpose of IALEIA is to advance high standards of professionalism in law enforcement intelligence analysis at the local, state/provincial, national, and international levels. The intent is to enhance understanding of the role of intelligence analysis, encourage the recognition of intelligence analysis as a professional endeavor, develop international qualification and competency standards, reinforce professional concepts, devise training standards and curricula, furnish advisory and related services on intelligence analysis matters, conduct analytic-related research studies, and provide the ability to disseminate information regarding analytical techniques and methods.

---

<sup>191</sup> <https://ialeia.org/>

In the mid-2000s, IALEIA and the LEIU agreed to hold their annual meetings and training sessions jointly—a decision that has proven to be highly successful.

## INTERNATIONAL ASSOCIATION OF CRIME ANALYSTS<sup>192</sup> (IACA)

While historically, crime analysis and intelligence analysis were viewed independently, over the past decade it has become clear that the two different forms of analysis not only overlap but are also synergistic. IACA was formed in 1990 to help crime analysts around the world improve their skills and make valuable contacts, to help law enforcement agencies make the best use of crime analysis, and to advocate for standards of performance and technique within the profession itself. These goals are accomplished through training, networking, and publications.

The organization currently has more than 4,000 active members from more than 60 nations and includes crime analysts, intelligence analysts, police officers of all ranks, educators, and students. In the past few years, IACA has aggressively pursued membership in non-English-speaking nations with improved products and services, including a dedicated Latin American Subcommittee.

IACA's Professional Training Series provides low-cost, multiday classes in fundamentals of crime analysis, crime mapping, computer applications, tactical analysis, problem analysis, and special topics at different locations around the world. The IACA's certified law enforcement analyst (CLEA) credential, offered since 2005, is an intermediate-level certification that requires experience, education, professional contributions, and a high score on a difficult test. Police chiefs and agencies can be confident that an IACA-certified law enforcement analyst possesses a demonstrated proficiency in crime analysis skills. The organization has had a significant impact on increasing crime analysis skills and applications globally over a comparatively short period of time.

## LAW ENFORCEMENT INTELLIGENCE INITIATIVES IN THE FIRST DECADE OF THE POST-9/11 ENVIRONMENT

Several important initiatives spurred by the terrorist attacks of September 11, 2001, have had a significant—and rapid—effect on the evolution of law enforcement intelligence. The more significant developments occurring during this time are listed in Table 2-2.

In October 2001, about six weeks after the 9/11 attacks, the International Association of Chiefs of Police (IACP) held its annual meeting in Toronto, Ontario, Canada. At that meeting, the Police Investigative Operations Committee discussed the need for SLTLE agencies to reengineer their intelligence function as well as the need for national leadership to establish standards and direction for SLTLE agencies. From this meeting, the IACP, with funding support from the Office of Community Oriented Policing Services (COPS), held the IACP Intelligence Summit in March 2002. The summit developed a series of recommendations including creation of a criminal intelligence sharing plan and adoption of intelligence-led policing.<sup>193</sup>

The Global Justice Information Sharing Initiative (Global), a group funded by the U.S. Office of Justice Programs, was already in existence with the charge of developing processes and standards to efficaciously share information across the criminal justice system. In response to the IACP Intelligence Summit of 2002, Global created a new subgroup, the Global Intelligence Working Group (GIWG). The purpose of the GIWG was to move forward with the recommendations from the summit. The first GIWG product was the NCISP.

Formally announced at a national signing event in the Great Hall of the U.S. Department of Justice on May 14, 2004, the NCISP signified an element of intelligence management that is important for all law enforcement officials.

---

<sup>192</sup> <https://iaca.net/>

<sup>193</sup> IACP Intelligence Summit. (2002). *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA: International Association of Chiefs of Police.

With formal endorsements from the DOJ, the U.S. Department of Homeland Security (DHS), and the FBI, the NCISP provided an important foundation on which SLTLE agencies could create their intelligence initiatives. The intent of the plan was to provide SLTLE agencies (particularly those that do not have established intelligence functions) with the necessary tools and resources to develop, gather, access, receive, and share criminal intelligence.

The NCISP<sup>194</sup> established a series of national standards that have been formally recognized by the professional law enforcement community as the role and processes for law enforcement intelligence today. The plan is having a significant effect on organizational realignment, information sharing philosophy, and training in America's law enforcement agencies.

TABLE 2-2: SIGNIFICANT POST-9/11 LAW ENFORCEMENT INTELLIGENCE INITIATIVES

- ◆ COPS/IACP Intelligence Summit
- ◆ Global Intelligence Working Group (GIWG)
- ◆ Counterterrorism Training Coordination Working Group (CTTWG)
- ◆ *National Criminal Intelligence Sharing Plan (NCISP)*
- ◆ Criminal Intelligence Coordinating Council (CICC)
- ◆ *Minimum Criminal Intelligence Training Standards*
- ◆ *Fusion Center Guidelines*
- ◆ U.S. Department of Homeland Security (DHS) *Target Capabilities List (TCL)*
- ◆ Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
  - Creation of the Office of the Director of National Intelligence (ODNI) and appointment of the Assistant Deputy Director of National Intelligence (ADDNI) for Homeland Security and Law Enforcement
  - Creation of the Directorate of Intelligence (DI) at the FBI
  - Creation of the National Counterterrorism Center (NCTC)
  - Creation of the Information Sharing Environment (ISE)
- ◆ Creation of the Interagency Threat Assessment and Coordination Group (ITACG)
- ◆ National Strategy for Information Sharing (NSIS)
- ◆ Second COPS/IACP Intelligence Summit

The NCISP also recognized the importance of local, state, and tribal law enforcement agencies as a key ingredient in the nation's intelligence process and called for the creation of the CICC to establish the linkage needed to improve intelligence and information sharing among all levels of government. Composed of members from law enforcement agencies at all levels of government, the CICC was formally established in May 2004 to provide advice in connection with the implementation and refinement of the NCISP. Members of the CICC serve as advocates for local law enforcement and support its efforts to develop and share criminal intelligence to promote public safety and secure our nation. Because of the critical role that SLTLE agencies play in homeland security, they must also have a voice in the development of policies and systems that facilitate information and intelligence sharing. The CICC serves as the voice for all levels of law enforcement agencies by advising the U.S. Attorney General and the Secretary of Homeland

194 [https://govinfo.library.unt.edu/911/staff\\_statements/staff\\_statement\\_12.pdf](https://govinfo.library.unt.edu/911/staff_statements/staff_statement_12.pdf)

Security on the best use of *criminal* intelligence as well as the capabilities and limitations of SLTLE agencies related to information sharing.<sup>195</sup>

During the same period that these initiatives were occurring, somewhat independently many states and regions were developing multijurisdictional intelligence capabilities intended to maximize the diverse raw information input for analysis and examine potential acts of terrorism that may occur within regions. The units, originally called regional intelligence centers and later referred to as fusion centers, were not only embraced but actively encouraged by DHS, which began providing funding for some of the centers to support operations related to homeland security responsibilities. The concept of intelligence fusion caught on rapidly as an efficient and effective mechanism to develop and disseminate intelligence products. With recognition that other crimes, such as financial crime and weapons offenses, may have a nexus with terrorism, the centers' foci broadened to all crimes. Moreover, with the broad mission of DHS, which was increasingly providing substantial amounts of funding, the fusion centers' focus broadened further to encompass "all crimes, all hazards, all threats."

Recognizing the benefits of standardization to enhance the quality of work being done by the fusion centers, the GIWG once again moved forward to create the *Fusion Center Guidelines*.<sup>196</sup> The guidelines developed a series of recommendations and promising practices for law enforcement agencies that are participating in the intelligence fusion process. While primarily focusing on criminal intelligence, the guidelines also spotlight the law enforcement information sharing relationship with the private sector as well as public safety issues related to homeland security intelligence. The fusion process seeks to have as many law enforcement agency information sharing partners as possible. Analytic outputs will be more robust as law enforcement participation increases because a wider array of diverse information will be entered into the analytic process. Hence, the recommendation from the NCISP and the second COPS/IACP Intelligence Summit that all agencies, regardless of size, should develop an intelligence capacity is clearly an important ingredient for increased agency participation with fusion centers.

At virtually the same time, DHS was developing plans to meet its mission, mandated in Homeland Security Presidential Directive-8 ". . .to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies. . . ." <sup>197</sup> A critical part of this initiative was to define the critical knowledge, skills, abilities, and processes—i.e., "capabilities"—that were necessary for law enforcement and emergency services personnel to perform these tasks. These capabilities were articulated in detail in the *Target Capabilities List*<sup>198</sup> (TCL). Intended to protect the nation from all hazards, ". . .the TCL is a national-level, generic model of operationally ready capabilities defining all-hazards preparedness."<sup>199</sup> The list is broken down into different areas associated with prevention and response. In the Prevent Mission Area, there are two specific intelligence-related target capabilities: information gathering and recognition of indicators and warnings and intelligence analysis and production. The information gathering capability is focused on ". . .the continual gathering of only pure, unexamined data. . ." that can be used in the intelligence process to identify threats and indicators of threats. This type of information is essential for effective analysis and is the currency that fusion centers rely on law enforcement agencies to submit to the fusion process, typically through tips, leads, suspicious activity reports, and observation of terrorism or criminal indicators.

The intelligence analysis target capability involves:

. . .the merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture.

---

195 <https://bja.ojp.gov/program/it/global/groups/cicc>

196 [https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf)

197 Homeland Security Presidential Directive/HSPD-8, National Preparedness, December 17, 2003 at (5), <https://www.govinfo.gov/content/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1745.pdf>. For more information on HSPD-8 and the Targeted Capabilities List, see the Fact Sheet at <https://www.hsdl.org/?abstract&did=776292>.

198 Available online at <https://www.hsdl.org/?abstract&did=776292>.

199 U.S. Department of Homeland Security. (2007). *Target Capabilities List*. Washington, DC: US DHS, p. 1.

This process focuses on the consolidation of analytical products among the intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings.<sup>200</sup>

The discussion of both of these target capabilities in the *Target Capabilities List* refers to both the NCISP and the *Fusion Center Guidelines* as standards and process to accomplish the capabilities. Hence, the integration of these initiatives strives to create a culture of information sharing that inextricably includes SLTLE.

Building on these initiatives and other new programs and activities in the Intelligence Community, as well as recommendations from the 9/11 Commission, was legislation passed by Congress: the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). While there were many important aspects of this legislation, four important factors are significant for the current discussion: creating the Office of the Director of National Intelligence (ODNI), creating a Directorate of Intelligence (DI) in the FBI, creating the National Counterterrorism Center (NCTC), and mandating the creation of the Information Sharing Environment.

The first factor of the IRTPA provisions related to SLTLE was creation of the ODNI. The Director of National Intelligence (DNI) serves as the head of the Intelligence Community and as a principal advisor to the President on issues related to national security. One of the unprecedented aspects of this office is the formal recognition that SLTLE has a role in national security as well as homeland security. The staff of the ODNI includes an Assistant Deputy Director of National Intelligence (ADDNI) for Homeland Security and Law Enforcement. While the role and functions of this position are still evolving, essentially the ADDNI is responsible for policy issues related to information sharing between the intelligence community and SLTLE. Moreover, the ADDNI has a seat at the table to advise the Intelligence Community on law enforcement capabilities, operations, and restrictions as related to national security issues.

The second factor was creation of the FBI Directorate of Intelligence (DI) (currently called the Intelligence Branch<sup>201</sup>) to manage all FBI intelligence activities.<sup>202</sup> The DI is organized as part of the FBI's National Security Branch<sup>203</sup> (NSB) and was embedded in all investigative domains—counterterrorism, counterintelligence, weapons of mass destruction, cyber, and criminal inquiries.<sup>204</sup> A key responsibility of the DI was identifying threats and sharing threat information with SLTLE agencies and the intelligence community. The DI's goal was to be a “full and trusted partner who can be relied on to proactively bring FBI resources to the table to help resolve threats.”<sup>205</sup> The IRTPA mandate firmly established and expanded the DI's authority over the management of the FBI's intelligence functions, including oversight of field intelligence operations and coordination of human source development and management.

The third factor was the creation of the National Counterterrorism Center<sup>206</sup> (NCTC). The NCTC serves as the primary organization for integrating and analyzing all intelligence pertaining to terrorism with the exception of purely domestic terrorism. The center also serves as the central knowledge bank on terrorism information and provides all-source intelligence support to governmentwide counterterrorism activities. The center's mission is essentially to “get the right counterterrorism information into the right hands of the right people” at DHS and the FBI, in the intelligence community, and, indirectly, at SLTLE agencies. The NCTC seeks to bring intelligence from across the

---

200 Ibid., p. 91.

201 <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch>

202 Rather than create a new domestic intelligence agency, as recommended by the 9/11 Commission, the legislation increased the intelligence authority and responsibilities of the FBI.

203 <https://www.fbi.gov/about/leadership-and-structure/national-security-branch>

204 <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch>

205 Statement by FBI Assistant Director Wayne Murphy, Directorate of Intelligence at the 2007 IACP Intelligence Summit, Washington, DC, November 27, 2007.

206 <https://www.dni.gov/index.php/nctc-home>

federal government into one place to integrate and analyze it and then disseminate the integrated intelligence to customers.

The final IRTPA factor of concern to SLTLE agencies is creation of the ISE. IRTPA required the President to establish an Information Sharing Environment “for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties.” It also required designation of a program manager for the Information Sharing Environment (PM-ISE), who was charged with planning and overseeing the ISE’s implementation and management. The *Information Sharing Environment Implementation Plan*<sup>207</sup> was designed to increase the sharing of terrorism information among and between the 16-member intelligence community, law enforcement agencies at all levels of government, and the private sector, as well as foreign partners. The ISE seeks to “. . . implement an effective, widespread culture of information sharing, balanced with a need for security and the protection of privacy and civil liberties. . . .”<sup>208</sup> The *Implementation Plan* provides a detailed process and action steps that indicate significant expectations for SLTLE agencies that wish to be participants in the ISE. The *Implementation Plan* further stipulates that each state must identify a primary state fusion center as the information sharing nexus between the federal ISE and SLTLE agencies.<sup>209</sup>

As is evident from the above initiatives, information sharing has become the fundamental principle for intelligence processes to protect America. Despite new programs, legislation, and regulations, information sharing across governmental levels was still problematic. An attempt to remedy this was to have key decision makers and representatives of all levels of the ISE to meet on a consistent basis and resolve information sharing problems. Across the government, federal partners initiated “fellows programs” to provide unique opportunities for state and local partners to collaborate directly with DHS and the IC to ensure that threat information is most effectively shared among and across all levels of government.<sup>210</sup> One specific approach to address this concern was the creation of the Interagency Threat Assessment and Coordination Group<sup>211</sup> (ITACG) within the NCTC.<sup>212</sup> ITACG members include DHS, FBI, members of the Intelligence Community, and state and local law enforcement and homeland security representatives. A key role of the group is to support the efforts of NCTC to produce federally coordinated terrorism-related information products intended for dissemination to state, local, and tribal officials and private sector partners.

ITACG members—particularly at the state and local levels—help define the intelligence products needed by each type of consumer. Because each level of government has different priorities, ITACG members provide advice, counsel, and subject-matter expertise to the Intelligence Community regarding the operations of SLTLE agencies, including how such entities use terrorism-related information to fulfill their counterterrorism responsibilities as well as their core mission of protecting their communities.

---

207 [https://www.dni.gov/files/ISE/documents/DocumentLibrary/ise-impplan-200611\\_0.pdf](https://www.dni.gov/files/ISE/documents/DocumentLibrary/ise-impplan-200611_0.pdf)

208 Ibid. Program Manager’s Office, p. 83.

209 In November 2007, a letter jointly signed by the U.S. Attorney General and the Secretary of Homeland Security was sent to each state governor with respect to the designation of a primary fusion center. The letter stated, in part, “. . . Guideline 2 states that DOJ and DHS will work with governors or other senior state and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism, law enforcement, and homeland security information in an all-crimes approach. . . it is imperative for your office to designate one fusion center to serve as the statewide hub. . . . In designating a single fusion center, please give consideration to developing an inclusive strategy that is consistent with the federal efforts to constitute the ISE.”

210 Saupp, K., Engelhardt, D., Collins, M., & Hale, B. (August 2017). “Integrating State and Local Expertise into the Intelligence Community.” *Police Chief Magazine*. <https://www.policchiefmagazine.org/integrating-state-local-expertise-intelligence-community/>

211 <https://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionIV.html>

212 As programming evolved, this became known as the Joint Counterterrorism Assessment Team (JCAT) <https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team>

Beyond these responsibilities, a key role of the ITACG is to coordinate the production and timely dissemination of specific intelligence products to SLTLE officials. The intelligence products include the following:

- ◆ Alerts, warnings, and notifications of time-sensitive terrorism threats to locations within the United States
- ◆ Situational awareness reporting regarding significant events or activities occurring at the international, national, state, or local levels
- ◆ Strategic assessments of terrorist risks and threats to the United States<sup>213</sup>

The ISE was evolving beyond a plan and moving into actual policy and processes. Taking the next step, in October 2007 the White House released the National Strategy for Information Sharing (NSIS):

This Strategy will assist the Administration in ensuring that Federal, State, local and tribal government employees responsible for protecting our Nation from future attacks or responding should an attack occur understand the Administration's expectations and plans for achieving improvements in the gathering and sharing of information related to terrorism.<sup>214</sup>

The strategy goes on to note:

The President's guidelines recognized that State, local, and tribal authorities are critical to our Nation's efforts to prevent future terrorist attacks. . . .The informational needs of State, local, and tribal entities continue to grow as they incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they require access to timely, credible, and actionable information and intelligence about individuals and groups intending to carry out attacks within the United States, their organizations and their financing, potential targets, pre-attack indicators, and major events or circumstances that might influence State, local, and tribal preventive and protective postures.<sup>215</sup>

The role of SLTLE intelligence is undeniable.

In many ways, post-9/11 intelligence developments came full circle with the second IACP/COPS Intelligence Summit. While many important—and substantive—changes have been made in law enforcement intelligence, this 2008 Summit Report observed that:

The participants in the follow-up IACP Criminal Intelligence Sharing Summit nevertheless made it clear that many of the nation's law enforcement agencies do not participate in the criminal intelligence sharing plan. Too many state, local, and tribal agencies, it would seem, underestimate their importance to the criminal intelligence sharing process, overestimate the burdens of full participation, and/or remain unaware of how to contribute to the vital work of the plan.<sup>216</sup>

Clearly, challenges remain.

---

213 Ibid.

214 *National Strategy for Information Sharing*. (2007). Washington, DC: Executive Office of the President, p. 1.

215 Ibid., p. 17.

216 International Association of Chiefs of Police. (2008). *National Summit of Intelligence*. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice, p. 2.

## COLLATERAL DEVELOPMENTS

A number of other activities were either already in place or in development concurrently with the above initiatives. The distinction of these activities is that they have helped facilitate the goals and processes of the strategies described above.

**Counterterrorism Training Coordination Working Group (CTTWG).** The Counterterrorism Training Coordination Working Group (CTTWG) was formed in 2002 to facilitate interagency coordination, information exchange, and sharing of innovative training initiatives between federal agencies involved in terrorism and antiterrorism training. The group was later expanded to include representation from the major law enforcement and law enforcement training organizations. Further expansion of the CTTWG included policy-level agency representatives from a broad range of federal agencies and law enforcement organizations involved in federal, state, local, and tribal law enforcement training and academe. The CTTWG recognized that increasingly, training issues and programs being brought before them were focusing on the discipline of intelligence. As a result, greater attention was focused on intelligence training and how to maximize the use of limited resources by ensuring that the intelligence training conveys a consistent, quality message; is not duplicative; is consistent with national standards; and meets the needs of law enforcement. Among the new intelligence initiatives was the creation of an online Law Enforcement Intelligence Master Training Calendar.<sup>217</sup> The group also assumed responsibility for preparing Version 2.0 of the *Minimum Criminal Intelligence Training Standards*.

**Minimum Criminal Intelligence Training Standards.**<sup>218</sup> Recognizing that the intelligence capacity of America's law enforcement community could not be realized without effective training, the CTTWG developed the *Minimum Criminal Intelligence Training Standards*. The standards identify six law enforcement focal areas—chief executive, intelligence commander/manager, intelligence analyst, criminal intelligence officer, general law enforcement officer, and train-the-trainer—critical to successful intelligence activities. For each area, a group of experienced law enforcement intelligence professionals articulated learning objectives and identified key knowledge, skills, and abilities needed to execute intelligence responsibilities. With position-specific knowledge of the intelligence process increased within the law enforcement community, the willingness and ability to proactively contribute to the Information Sharing Environment increases significantly. Version 2.0 of the standards was approved in October 2007. These standards evolved into the *Common Competencies for State, Local and Tribal Intelligence Analysts*<sup>219</sup> and the *Analyst Professional Development Road Map*.<sup>220</sup>

**Global Justice Extensible Markup Language Data Model (GJXDM).** Because of the administrative independence among and between each component of the criminal justice system, many criminal justice information systems evolved in a manner that would not easily permit electronic information sharing. Frequently relying on proprietary data models from vendors, agencies often had to exchange information in hard copy or reenter it. The Global Justice Information Sharing Initiative took on the task of developing a common data model that could serve as a standard to be used by all system components. The Global Justice Extensible Markup Language Data Model (GJXDM) is an Extensible Markup Language (XML) standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner.<sup>221</sup> There are three primary parts to the GJXDM: the Data Dictionary (identifying content and meaning), the Data Model (defining structure and organization), and the Component Reuse Repository (a database). While the intent of the data model was to enhance criminal justice

217 The Intelligence Master Training Calendar is available on the public side of the National Criminal Intelligence Resource Center website: <http://mastercalendar.ncirc.gov/>.

218 The standards are available at: <https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other>.

219 [https://www.ncirc.gov/documents/public/common\\_competencies\\_state\\_local\\_and\\_Tribal\\_intelligence\\_analysts.pdf](https://www.ncirc.gov/documents/public/common_competencies_state_local_and_Tribal_intelligence_analysts.pdf)

220 <http://www.it.ojp.gov/GIST/179/Analyst-Professional-Development-Road-Map>

221 <https://bja.ojp.gov/program/it/national-initiatives/gjxdm>

information sharing, the model has been embraced as a means to enhance electronic sharing of criminal intelligence data. As a result, the GJXCM serves as an important technological component to support the ISE.

**National Information Exchange Model<sup>222</sup> (NIEM).** A joint initiative of DOJ and DHS, NIEM embraced the GJXDM data model and built an information sharing policy framework that met the mandates of the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and Homeland Security Presidential Directive 5 (HSPD-5).

Rather than nationwide integration of all local, state, tribal, and federal databases, NIEM focuses on cross-domain information exchanges between key domains and communities of interest (COIs), across all levels of government—whether between individual local law enforcement agencies, law enforcement and emergency-service agencies, and other domains, or between local, state, tribal, regional, and federal agencies.<sup>223</sup>

The development of a common data standard and data sharing model is clearly an important thread that permeates the culture of information sharing.

**Grants for Training, Technical Assistance and Technology.** Various agencies and bureaus within both DOJ and DHS have been committed to providing grant support to further the intelligence mission. The wide variety of intelligence training programs supported, special activities providing technical assistance, and assistance given in purchasing technology and information systems—consistent with GJXDM and NIEM—have all been critical to the development of the information sharing culture. It is particularly important to note that many intelligence-related initiatives have been collaborative partnerships between DOJ and DHS. Beyond the support these initiatives have provided, this collaboration demonstrates information sharing in practice.

While these collateral initiatives have since evolved or been eliminated, they all contributed significantly to the development of law enforcement intelligence.

## IMPLICATIONS

The *ISE Implementation Plan* states that there is a need to “promote a culture of information sharing across the Information Sharing Environment.” While a great deal of work—and resocialization—remains, a review of the initiatives discussed above demonstrates that significant strides have been made. The ISE will have challenges to meet its ultimate goal; however, the changes that have been made in a comparatively short period represent important milestones and are a significant leap forward.

Collectively, these initiatives have changed the philosophy of law enforcement intelligence that reflects:

- ◆ A commitment to information sharing both within and between law enforcement agencies.
- ◆ The need to establish an objective, thoughtful intelligence function that has consistent national professional standards.
- ◆ The recognition that SLTLE agencies have an important role in both homeland security and national security.
- ◆ A process committed to preventing terrorism and multijurisdictional criminality.
- ◆ A commitment to pursuing the intelligence function in a manner that is consistent with privacy and civil rights protection.

---

<sup>222</sup> See <http://www.niem.gov>.

<sup>223</sup> Introduction to the National Information Exchange Model. (February 12, 2007). Washington, DC: NIEM Program Management Office, p. 3.

## THE INTELLIGENCE EVOLUTION REFINED

As noted previously, the renaissance of law enforcement intelligence was significantly influenced by the terrorist attacks of September 11, 2001. Going into the second decade of the 21st century, three factors were further expanding the application of the intelligence process.

- ◆ **The rapid evolution of technology.** Not only did we experience new technologies; they were faster, had more memory, had increased wireless capabilities, integrated new devices to include livestream audio and video, and featured new software driven by artificial intelligence to drive capabilities such as facial recognition and analytic integration of diverse types of unstructured data. In this regard, we saw enhanced analytic capabilities such as forecasting algorithms; a more robust ability for pattern analysis with large volumes of data; and the ability to collectively analyze, link, and compare statistical data, written files, audio, and video. Hence, information collection and analysis were moving forward rapidly, requiring new skills, new policies, new training, and additional analysts.
- ◆ **Increases in violent crime.** Across the country, violent crime and homicides had increased significantly. Indeed, the violence became so pervasive that the DOJ created the National Public Safety Partnership<sup>224</sup> to provide resources and expertise from various federal agencies and contemporary research to help suppress violent crime. At the same time, there was a growing frequency of school shootings, mass-violence attacks, targeted violence, and domestic terrorism attacks (notably by white nationalists) that were further aggravating violence in America. As a result, new initiatives were being developed, including those embracing intelligence analysis. For example, BJA sponsored a homicide clearance project that found agencies that were most successful in clearing homicides used intelligence analysis and other creative initiatives to more successfully identify perpetrators.<sup>225</sup> In Florida, the Florida Department of Law Enforcement, in collaboration with other agencies, was mandated to do statewide threat assessments at schools to prevent school shootings. And increasingly, gang investigation units were employing intelligence analysis to help stem shootings, particularly by repeat offenders. The need to suppress violence became a factor that needed more effective analysis.
- ◆ **Growth/expansion of criminal enterprises.** Unique, and sometimes complicated, criminal enterprises were not only growing; they were also increasingly transnational and employing new technology to further their crimes. Gangs began to operate as criminal enterprises, often with drug-trafficking organizations; criminal organizations fueled the opioid crisis, often working from overseas; and human trafficking expanded in the sex, domestic service, and agriculture industries in virtually every state. With the legalization of marijuana by many states, new black-market marijuana cartels emerged, capitalizing on the growing demand for the substance with the intent to increase profits by avoiding regulation and taxes. Especially challenging has been the growth of Darknet marketplaces selling contraband in all forms, such as illicit drugs, firearms, stolen identities, stolen arts and antiquities, and more. All of these represent complex criminality, many with international components that are most effectively attacked using the intelligence process.

One result of these factors was the need for more analysts—professionals trained in the scientific method and capable of doing not only research but also using sophisticated software for both qualitative and quantitative analysis. Parallel to this growth was the need for professional standards<sup>226</sup> that were developed and recently revised in a coordinated effort between DOJ and IALEIA.<sup>227</sup> Furthermore, BJA, Global, and DHS collaborated to prepare the

---

224 <https://www.nationalpublicsafetypartnership.org/>

225 <https://www.nationalpublicsafetypartnership.org/clearinghouse/Resource/175>

226 [https://it.ojp.gov/documents/d/Law%20Enforcement%20Analytic%20Standards%2004202\\_combined\\_compliant.pdf](https://it.ojp.gov/documents/d/Law%20Enforcement%20Analytic%20Standards%2004202_combined_compliant.pdf)

227 <https://www.ialeia.org/>

*Analyst Professional Development Road Map, Version 2.0*<sup>228</sup> intended to create “. . . a sustainable, professional career path for analysts operating within federal, state, local, tribal, and territorial organizations.” Law enforcement agencies that had never used analysts before were increasingly recognizing their value in helping officers and investigators work smarter, not harder.

During this era, we also saw a greater integration of intelligence analysis and crime analysis work products. While these work products have different goals and methods, they complement each other. As a result, strategic intelligence and crime analysis products were helping decision makers focus resources and efforts to make the greatest impact on crime control within their communities. A good operational example of this is the development of real-time crime centers,<sup>229</sup> wherein an array of new technologies collect data to which analysts give meaning—such as crime patterns, crime trends, hot spots, suspicious behaviors, and potential suspects—to prevent crime and apprehend offenders.

Concurrently, the role of fusion centers also broadened. While initially developed essentially as counterterrorism intelligence centers after the 9/11 attacks, the centers did not really embrace their all-crimes, all-hazards mission until a few years later. As entities of state and local governments, many of the centers experienced pressing crime needs and truly began to expand their operations, focusing on significant crime issues as well as new and emerging crime.<sup>230</sup>

As fusion centers developed and expanded, with more major urban area fusion centers being developed, there was great concern by many that the centers would actively perform surveillance of people in communities—a fear that was heightened by technologies that could be both stealthy and intrusive. While this concern remains, it is not nearly as pronounced as it once was because of proactive measures on guidelines, model policy, training, and technical assistance—largely under the guidance of the Criminal Intelligence Coordinating Council—to protect citizens’ privacy, civil rights, and civil liberties (P/CRCL).

During this period of evolution, there were also both challenges and failures. While many factors played a role, the intelligence process was one of the most important. For example, despite the amount of attention and resources and the number of task forces and intelligence initiatives devoted to illicit drug trafficking, the rapid and expansive growth of the opioid crisis was unforeseen, and law enforcement’s response was slow and somewhat off-target. While the opioid crisis was a social and public health problem, it was also a law enforcement problem as a result of the illegal trafficking and sale of drugs. Yet strategic analysis did not detect the rapidity of the crisis development or its devastating effect on America’s communities.

Another major issue left unseen was the mounting social unrest largely directed toward police officers for what was perceived to be the targeting of minorities for police action, including several high-profile, officer-involved shootings of minorities. Place-based analysis of crime located high-probability crime areas. Most notably in New York, but also in other cities, law enforcement used proactive stop-and-frisk activities in an effort to suppress crime in these hot spots. While the tactic worked to suppress crime, it created a new controversy wherein African-American males believed they were being racially profiled for targeted stops; this perception was evolving into widespread social discontent. There were certainly indicators of unrest, but they largely went unnoticed. On August 9, 2014, this changed with the shooting of Michael Brown in Ferguson, Missouri.<sup>231</sup> This incident set off weeks of demonstrations across the country focusing on police officers’ relationships with minority communities. While these demonstrations have many components, for the current discussion, the sentiment and the movement should have been identified by strategic analysis but were missed.

228 <https://it.ojp.gov/GIST/1210/Analyst-Professional-Development-Road-Map--Version-2-0>

229 <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/RealTimeCrimeCenterInformation.pdf>

230 <https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-in-a-fusion-center>

231 Institute for Intergovernmental Research. (2015). *After-Action Assessment of the Police Response to the August 2014 Demonstrations in Ferguson, Missouri*. Washington, DC: COPS Office. <https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-P317>

A notable challenge for law enforcement intelligence has been the meteoric expansion of social media and Darknet for use by criminal offenders and criminal extremists. Law enforcement has responded to this expansion and developed initiatives to identify both offenders and threats. Yet the international character of the Internet and its vast size has posed significant limitations to identify crimes and threats, even with software designed to aid in identifying this information. Moreover, care has to be taken to protect P/CRCL, particularly balancing extremist rhetoric with the First Amendment protection of free speech.

The remedy to these challenges: We must be creative in our perspective of crime and social problems and not fall into what the 9/11 Commission called the “failure of imagination.” The first step toward preventing a crisis is believing it could happen.

An important mechanism for guiding law enforcement intelligence has been the CICC. The CICC has been active in monitoring issues and change, providing guidance in a wide array of publications on promising practices and recommendations.<sup>232</sup>

## REFORMING LAW ENFORCEMENT INTELLIGENCE AT THE STATE, LOCAL, AND TRIBAL LEVELS

Although the recommendations provided by various national crime commissions were designed to strengthen law enforcement’s capabilities to fight organized crime, by the mid-1980s, criminal enterprises had grown dramatically and encompassed such a diverse array of illegal activities that the ability of SLTLE agencies to deal with these problems was limited. Investigators and intelligence units had neither the expertise nor the personnel to contain the problem effectively. This was aggravated by a failure of law enforcement to generally understand the nature of the problem and by poor information sharing between law enforcement agencies at all strata of government.<sup>233</sup> Organized crime was characterized as a “rapidly changing subculture” that was outpacing the capability of law enforcement to control it. As a result, law enforcement intelligence units were often relegated to being little more than information clearinghouses or, in some cases, viewed as failed initiatives.<sup>234</sup>

Despite the lack of success, many within the law enforcement community still viewed the intelligence function as important to law enforcement agencies. However, a primary limitation of state and local intelligence units was their inability to move beyond the collection of information to a systematic method of analyzing the collected data. The solution, then, was to have “the analytical function. . . [guide] the data collection [procedure]” rather than vice versa.<sup>235</sup>

Another limitation of law enforcement intelligence was that many law enforcement executives either did not recognize the value of intelligence, did not have the skills necessary to use intelligence products effectively, or both. Furthermore, intelligence personnel did not have the skills for sophisticated analysis and report writing needed to produce meaningful intelligence products. Training was considered an important solution to this problem and still is.

A historical issue was that intelligence units tended to be reactive in nature, often viewed as repositories of sensitive information rather than proactive resources that could produce information critical for preventing crime and apprehending offenders. Similarly, intelligence units tended not to produce consistent, specifically defined products. Instead, intelligence reports tended to be written on an ad hoc basis to address critical matters.

---

232 <https://it.ojp.gov/global/working-groups/cicc/resources>

233 President’s Commission on Organized Crime. (1987). Washington, DC: U.S. Government Printing Office.

234 Martens, F. (1987). “The Intelligence Function.” In Herbert Edelhertz (ed.), *Major Issues in Organized Crime Control*. Washington, DC: U.S. Government Printing Office.

235 Ibid.

A final limitation was that intelligence products were not disseminated in a timely or comprehensive manner. This, perhaps, was the greatest setback because the character of organized crime was constantly changing: Different commodities were being trafficked, methods of operations tended to evolve, and participants in the operation of the enterprise changed. The need for timely and relevant information was seen as a necessary component for improving law enforcement intelligence operations.

While the majority of past recommendations focused on the development and operations of intelligence units, recommendations have also been made regarding the ethical issues associated with state and local intelligence operations. Similar to the concerns that led to the formation of the Church Committee at the federal level, potential abuses of power were a concern at the state and local levels. Accordingly, recommendations were made to ensure that citizens' civil rights remain intact.

For example, the *LEIU File Guidelines*<sup>236</sup> were created to provide a practical policy and procedures intended to facilitate an effective intelligence process that was compliant with 28 CFR Part 23 and protected citizens' rights. Similarly, the Commission on the Accreditation of Law Enforcement Agencies (CALEA) has recommended that every agency with an intelligence function establish procedures to ensure that data collection on intelligence information is "limited to criminal conduct that relates to activities that present a threat to the community" and to develop methods "for purging out-of-date or incorrect information."<sup>237</sup> In other words, the CALEA standard identified the need for law enforcement agencies to be held accountable for abuses of power associated with their intelligence activities. The latest revision of the CALEA intelligence standard embraces the *National Criminal Intelligence Sharing Plan* and its recommendations.

As will be seen later, the development of the intelligence-led policing concept and the creation of the *National Criminal Intelligence Sharing Plan* have been important milestones in the evolution of law enforcement intelligence. By creating both an overarching intelligence philosophy and a standard for operations, SLTLE intelligence is becoming more professional. It is embracing more sophisticated tools, developing greater collaboration for one voice from the law enforcement intelligence community, and moving with a greater sense of urgency because of 9/11.

## CONCLUSIONS

While we have evolved in our expertise and professionalism, many of the same issues remain. What are the lessons learned from history?

- ◆ Building dossiers full of raw, diverse information provides little insight—analysis is needed to give meaning to the information.
  - The improper collection of information can have a negative impact on our communities, including a chilling effect on the constitutional right of freedom of speech.
- ◆ To be effective, intelligence units must be proactive, developing unique products and disseminating the products to appropriate personnel on a consistent and comprehensive basis.
- ◆ A clear distinction is needed between law enforcement intelligence and national security intelligence. While there is information that can support the goals of both forms of intelligence, the competing methodologies and types of information that may be maintained in records mandate that the distinction remain clear and that overlap occur only for clear purposes of public safety, including the apprehension of offenders and prevention of criminal and/or terrorist acts.

---

236 [https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/leiu\\_crim\\_intell\\_file\\_guidelines.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/leiu_crim_intell_file_guidelines.pdf)

237 Commission on Accreditation for Law Enforcement Agencies. (1998). *Standards for law enforcement agencies*. 4th ed. <https://www.calea.org/node/11406>.

- ◆ Targeting people is unlawful without some evidence of a criminal predicate. Targeting is unlawful:
  - If the reason for the targeting is a person’s support of an unpopular cause.
  - If people are being targeted because of their political beliefs, religion, race, ethnicity, or other attributes or characteristics that are inherently lawful (e.g., racial profiling, people who are perceived to be Muslim, persons with extensive tattoos assumed to be gang members).
- ◆ Targeting without lawful justification can result in civil rights suits and vicarious liability lawsuits, which can be both costly and embarrassing to the police department.
- ◆ The need to institute a privacy policy and civil rights protections is an essential professional objective.
- ◆ Monitoring an individual’s behavior is proper if reasons can be articulated that reasonably support the notion that:
  - The person may be involved in criminality now or in the future.
  - There is a reasonable threat to public safety.
- ◆ Retaining information in intelligence files about an individual or an organization is improper if there is no reasonable suspicion of his or her criminal involvement unless that information is used only as noncriminal identifying information and is labeled as such.
- ◆ A full-time law enforcement intelligence function should be organized professionally and staffed with personnel who are specifically trained in analysis and intelligence product preparation.
- ◆ There must clear lines of communication between the intelligence unit and decision makers.
- ◆ Law enforcement intelligence units must be evaluated regularly to ensure functional utility and operational propriety.
- ◆ Law enforcement intelligence must fully embrace the latest technologies, including social media, both as tools for collection, analysis, and dissemination and for identifying technology-enhanced crimes and emerging threats.
- ◆ Information sharing remains an important priority.

While past abuses of the intelligence function were no doubt good-faith efforts to protect the community, they were nonetheless abuses. The changes that have occurred, particularly in the post-9/11 environment, and the professional development of the law enforcement intelligence function have demonstrated a respect for civil rights, a reliance on the scientific approach to problem solving, and a commitment to keeping America’s communities safe.

# CHAPTER 3

## THE INTELLIGENCE PROCESS (CYCLE) FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT



In the first chapter, the differences between law enforcement intelligence and national security intelligence were discussed. Despite these differences, they share one core aspect: the *intelligence process* (also known as the *intelligence cycle*). The process employs the scientific approach to problem solving to provide objective and reliable data collection and analysis. While very similar to research methods, as will be seen, the intelligence process has broader applications. The importance of this process is that it provides mechanisms to ensure the consistent management of information that is used by analysts to create intelligence. This chapter is intended to be an overview of the intelligence process. Many of the issues introduced here will have expanded discussion later in the guide.

A basic premise should be remembered (and will be repeated): Law enforcement does not collect intelligence—information is collected. Intelligence is the product of the analytic process.

The intelligence cycle has been depicted in a variety of ways throughout the intelligence literature. The number of phases in the process may differ based on the model used and the application;<sup>238</sup> however, the intent of each model of the cycle is the same: *to have a systemic, scientific, and logical methodology to comprehensively process information to ensure that the most accurate actionable intelligence is produced and disseminated to the people who provide an operational response to prevent a criminal threat from reaching fruition.*

---

238 “Application” refers not only to the difference between law enforcement and national security intelligence, but also to how the intelligence cycle is used in the private sector.



## NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN: RECOMMENDATION ON TRAINING AS RELATED TO THE INTELLIGENCE PROCESS

**Recommendation:** To fully implement the tenets of the NCISP, law enforcement agency leadership should ensure that personnel receive training on the intelligence process and privacy issues associated with the intelligence process.

*National Criminal Intelligence Sharing Plan, Version 2.0, p. 29.*

The process applies to all crimes, whether terrorism, drug trafficking, human trafficking, gangs, or any other criminal enterprise. Indeed, the process also helps identify circumstances in which there is a nexus among these different types of crimes. For example, intelligence analysis discovered that the Mexican drug cartels are also involved in human trafficking.<sup>239</sup> From an analytic perspective, the nexus between the two crimes was smuggling—a key component of both types of trafficking.

To be consistent with established national standards, the model used in this discussion is the one prescribed in the *National Criminal Intelligence Sharing Plan (NCISP)*, Version 2.0.<sup>240</sup> While components of the intelligence cycle are often depicted as “steps,” in practice, the different components of the cycle are phases—there is a constant ebb and flow of information between phases as information is processed and shared. Hence, the intelligence process is not a series of independent steps that are mechanically processed in an unbending sequential order; rather, they represent a recipe for intelligence development and information sharing that frequently changes based on the availability of “ingredients” (i.e., raw information) and the “nutritional needs” of the consumer, ranging from situational awareness to actionable intelligence.

The NCISP model of the intelligence cycle (Figure 3-1) has six phases:

1. Planning and Direction
2. Collection
3. Processing/Collation
4. Analysis
5. Dissemination
6. Reevaluation

Each phase may be broken down into subprocesses (illustrated in Figure 3-2) that collectively contribute to an effective information management and analysis system.



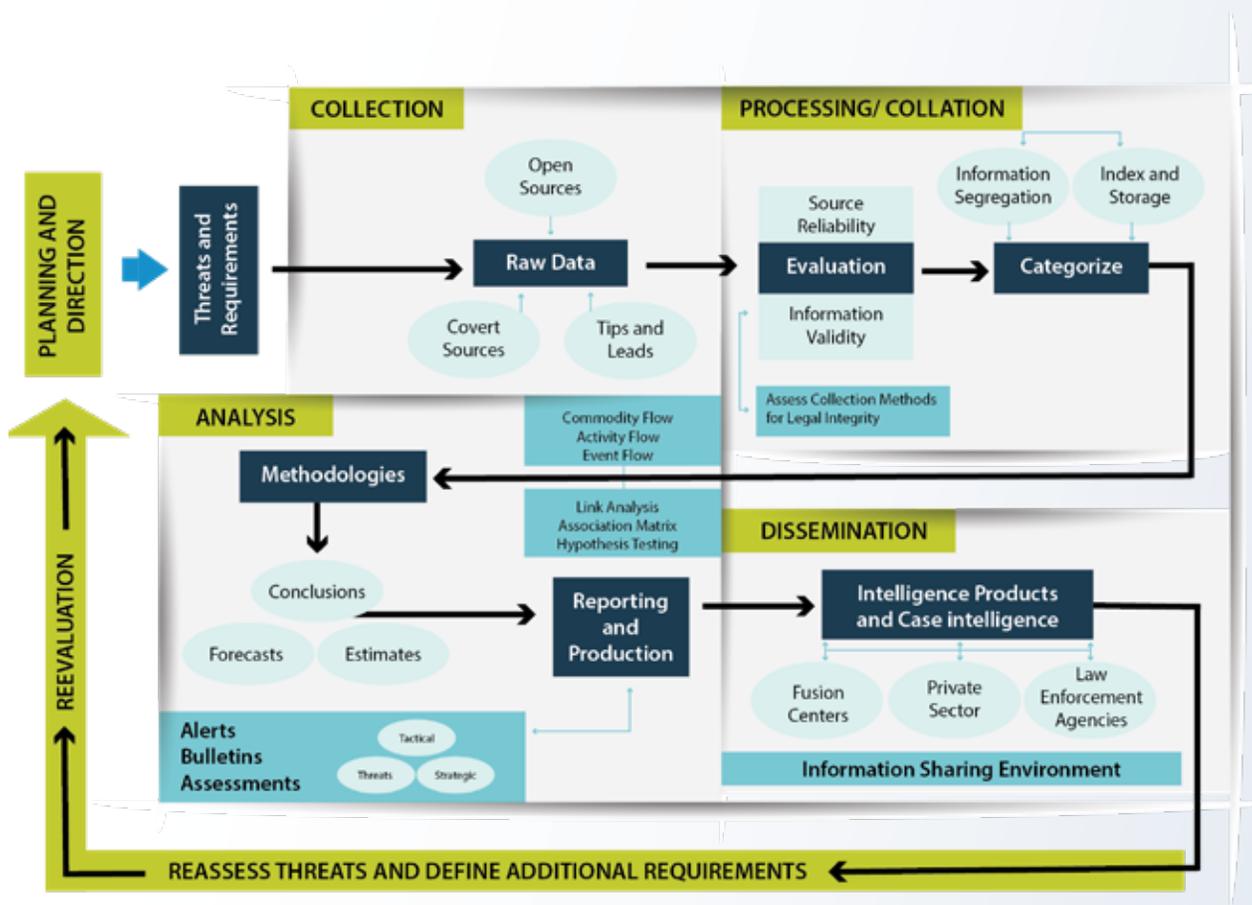
<sup>239</sup> <https://www.insightcrime.org/news/brief/human-trafficking-drug-cartels-mexico/>

<sup>240</sup> <https://it.ojp.gov/gist/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>, p. 23.

In many ways, the intelligence cycle acts like a radar sweep across a community. The process seeks to identify potential threats, determine whether suspicious activity has a criminal nexus, and provide indicators of criminality for operational units to develop responses. For example, an intelligence bulletin may describe certain indicators. An officer observes behaviors that are consistent with these indicators and collects further information that is processed through the cycle, which provides an analyst with more raw data to help refine the analysis. With a more refined analysis that is again disseminated to operational units, the likelihood increases of providing more explicit intelligence that operational units may use to prevent a crime or a threat. This illustrates the ebb and flow of the intelligence process.

For example, assume that an intelligence bulletin describes an emerging threat of Eastern European organized crime that is involved in extortion and protection rackets in a city. A police officer working neighborhoods with large populations of Russian immigrants has noticed an increase in thefts and property damage to small businesses largely operated by immigrants. Moreover, the victims are reluctant to talk to police officers about the crimes. In light of the intelligence bulletin, the officer provides information to the intelligence unit that the crimes that were reported as simple thefts and property destruction within this area of the city may, in reality, be indicators of enforcer activities of the Eastern European organized crime protection schemes. The analyst takes this information, corroborates it by documenting protection enforcement practices of the organized crime group in other cities, and provides this additional information to officers in a revised bulletin. This will support operational investigations of the criminal enterprise with the intent to prosecute the leaders, thereby preventing future victimization of both the extortion and the penalty crimes. The intelligence process requires this ongoing, two-way information flow to be most effective.

FIGURE 3-2: INTELLIGENCE PROCESS AND SUBPROCESSES



## PLANNING AND DIRECTION

The intelligence function involves many coordinated activities. Similar to intermeshed gears, there must be a plan for how each moving part will operate in concert with other elements and how the gears will collectively manage a change in the environment. The gears of the intelligence process are prioritized and synchronized in the first phase of the cycle, Planning and Direction.

Former FBI Executive Assistant Director for Intelligence Maureen Baginski often stated, “The absence of evidence is not the absence of a threat.” That is, a criminal threat is likely present in most communities, but law enforcement agencies may simply be unaware of the threats because they have no evidence. As part of the Planning and Direction process, it is important to recognize not only the threats that have been identified, but also dynamic threats where evidence indicating their presence may serendipitously appear.

For example, a patrol officer notices that in her patrol area over a comparatively short period of time, there has been an increase in young Latina women, all of whom appear to be living in a low-income housing unit with several women in each room. When the officer has contacted them, they have been reluctant to speak with her, and few speak English. The officer observes that they all leave in vans in the early morning. The activity seems suspicious, and the officer’s first assumption is they are undocumented immigrants. She submits a suspicious activity report on her observations. The analyst examines the information further and integrates it with information gathered from other sources. Based on the collective analyzed information, the analyst concludes that the women are most likely human-trafficking victims employed as domestic workers in a newly formed business in the city that has housekeeping contracts with several hotels. In this illustration, the officer’s observations discovered evidence of a previously unknown criminal enterprise operating in the city.

While a common perspective is that the intelligence process should take an all crimes/all threats approach, pragmatically, all crimes and threats are

## INFORMATION COLLECTION DISCIPLINES USED BY THE INTELLIGENCE COMMUNITY

In light of the Information Sharing Environment (ISE), there is a benefit to understanding some of the terminology used in the Intelligence Community (IC), even though it is generally not used by law enforcement intelligence. With regard to information collection, there are five general collection platforms or collection disciplines that are used by the IC:

1. **Human Intelligence (HUMINT)** is the use of human beings to collect or confirm information via overt, covert, or clandestine methodologies.
2. **Signals Intelligence (SIGINT)** is an umbrella term for different methods of intercepting and exploiting electronic signals, whether intercepted on the ground, via aircraft, or via satellite. There are three forms of SIGINT:
  - a. **Communications Intelligence (COMINT)** is the collection and exploitation of communications signals including any form of electronic voice communications, fax, wireless devices, and voice over Internet protocol (VOIP).
  - b. **Electronic Intelligence (ELINT)** is the interception of noncommunications transmissions such as via radar, transponder, motion detectors, and so forth.
  - c. **Foreign Instrumentation Signals (FISINT)** is the interception and exploitation of performance and tracking data (usually telemetry) during tests of weapons systems and space vehicles.
3. **Imagery Intelligence (IMINT)** is derived from visual photography, infrared image capture, lasers, electro-optics, visual radar, and satellite imagery.
4. **Measurement and Signatures Intelligence (MASINT)** is the analysis of electronic emanations from equipment and seeks to detect information patterns in a different part of the electronic spectrum not previously captured by other methods.
5. **Open Source Intelligence (OSINT)** is the analysis of information available to the public without legal process, covert methods, or consent.

not equal and must be prioritized considering the probability of their presence and the nature of the harm they pose to the community. For example, a local street gang that is generally nonviolent but involved in selling marijuana is a far less serious threat to the community than MS-13. Threat prioritization is part of the Direction component of the cycle's first phase. This is done through ongoing threat evaluation and assessments.

A threat evaluation is a comparatively quick fundamental review of information to make a determination as to whether there is a criminal nexus with certain reported suspicious behaviors, the probability of its being an ongoing crime problem within a community, and the type of threat it poses to community safety. For example, a small group of men are identified in a community going from house to house selling a driveway-sealing service to homeowners. They have two pick-up trucks with signs about their business and equipment that appear legitimate. They take deposits from homeowners for the work and schedule appointments to do the work later but never show up. This type of fraud, which is surprisingly common and effective, is largely transient. The threat to victimization exists but is likely to be short-lived and is not violent. Public education may become the primary police response. This threat evaluation was a relatively simple but effective way to understand the suspicious behavior and associated crime.

Threat assessment is more comprehensive and can be quite detailed depending on the nature of the threat (described in detail in the next chapter). The importance of the threat assessment in Planning and Direction lies within the ability to maximize resources and operational initiatives to those crimes and circumstances which pose the greatest risk to public safety. In many ways, the intelligence process looks for images through a lens that is out of focus. The two-way exchange of information and ongoing analysis helps focus the lens to understand whether a threat is present and the degree of risk it poses to the community.

Threat assessments are not the only way to identify threats, however. Ongoing crime analysis can monitor changing and emerging threats based on crime patterns. This is at the heart of the work in real-time crime centers. For example, crime analysis shows an increase in strong-armed robberies. Place-based analysis shows that the robberies are occurring at different locations, but in each location the robbery is near an ATM. Descriptions by victims and available video surveillance indicate that the likelihood is high that the same two suspects are committing all the robberies and that the suspects are working together—one serves as the lookout and the other the robber, and then they change roles between robberies. The suspects escape in a vehicle whose description is consistently provided by the victims. With this information, law enforcement officers may place surveillance cameras at ATMs—particularly after analyzing the geographic pattern trend of the robbers—and deploy license plate readers. Patrol officers may be deployed with directed patrol in a pattern that passes several ATMs, and plainclothes officers may be deployed near ATMs that the analysis indicates are likely target areas. Hence, analysis helps identify a new crime trend, identify potential crime target areas, and provide key foundation information to deploy operational responses.

The Planning and Direction process constantly monitors changes in the environment and helps define changing priorities as well as new information sharing needs. For example, analysis related to the opioid crisis has shown that law enforcement officers had to establish new relationships with the public health community to assist users who overdosed. It was also learned that police officers have a health and safety threat if they do not properly handle fentanyl. Investigators working on illicit opioid trafficking not only have to investigate traditional drug trafficking tradecraft but must also understand the sale and distribution of illicit drugs through Darknet marketplaces. Understanding these factors helps in planning and directing both ongoing analytic and investigative needs, as well as operational plans; it also helps identify the necessary resources to execute those plans.

Moreover, Planning and Direction helps identify resource needs and threat priorities and helps focus awareness training for officers, and often the public, on how to recognize identified threats. Further, to be most effective, policy, procedural, and resource allocation mechanisms must be sufficiently nimble to effectively respond to the changing threat environment. For example, homicides committed by members of MS-13; ransomware attacks to computer networks; and newly discovered, highly refined heroin in the local drug market are all threats that require

different types of expertise and responses. Just like the intelligence process itself, the Planning and Direction phase is characterized by an ebb and flow of information that provides insight so that the evolving threat environment can be managed efficaciously.

## COLLECTION

Collection is the gathering of raw information that will be used by analysts to prepare intelligence reports and products. To better envision the Collection phase of the process, analysts typically gather information from several sources:

1. Specifically sought-out information that is in response to **intelligence requirements**
2. A response to reported terrorism or criminal **indicators**
3. **Suspicious activity reports** (SARs) of activities observed by or reported to officers
4. **Open source research** by analysts, including social media
5. **Access to law enforcement and intelligence information systems** with databases of information that can be used for research and comparison
6. **Information sharing** with analysts and investigators from other jurisdictions
7. **Leads** that officers develop during the investigation of unrelated cases
8. **Tips** that may come from citizens, informants, and/or the private sector

The response to *intelligence requirements* is information that is intentionally and specifically sought to answer certain questions. That information may be sought from open sources or may be a product of law enforcement methods, such as interviews, surveillance, undercover operations, technological information collection, and/or other law enforcement processes. A response to **indicators** would be the collection of information by law enforcement officers based on their observations of circumstances or behaviors they recognize as a result of information gained from training and/or intelligence bulletins that describe such indicators. Typically, indicators include the signs and symbols of criminal activity such as graffiti; the symbol of an extremist group on a car; or unusual activity at a location that is consistent with threat activity described in an intelligence report.

Information collected from **suspicious activity reports** is based on behavior observed by law enforcement officers who, relying on their training and experience, believe that an individual may have been involved in criminal activity in the past or may be in the future; however, a specific criminal nexus is not identified.

**Open source information**, which will be discussed in greater detail in a later chapter, refers to information that can be obtained without the necessity of gaining permission or using legal processes. In the era of networking and social media, open source information can be among the most insightful for an analyst. There is a wide array of *law enforcement and intelligence information* systems an analyst may query. Many agencies have their own systems and databases; there are also state and regional systems of all types.<sup>241</sup>

**Information sharing between analysts and investigators** often takes the form of building on professional social networks. Beyond exchanging information, individuals often solicit input and advice on an analytic problem. The term “leads” refers to information officers develop about a probable emerging threat that is largely unrelated to a current

---

241. There are too many systems to list for the current discussion. For perspective, see the paper at <http://www.cfp2000.org/papers/dempsey.pdf>. Even this is somewhat dated in that more systems have been developed since the paper was written. Yet the paper provides a comprehensive list. The Regional Information Sharing Systems Secure Cloud (RISSNET) is among the most widely used. Go to <https://www.riss.net/> and hover over the RISSNET Resource menu item to see the array of systems available from this one system.

investigation but comes to light during the inquiry. “Tips” reflect information that has been observed by citizens and submitted to a law enforcement agency for further inquiry.

The collection process must seek to establish a criminal nexus with any person or organization that is identified in criminal intelligence records. This nexus is referred to as a *criminal predicate*. The standard of proof for the criminal predicate is to have facts and evidence that establish *reasonable suspicion*<sup>242</sup> (more than mere suspicion) that a particularly identified person has committed, is committing, or is about to commit a crime.

In practice, law enforcement agencies collect information on individuals where no criminal predicate exists. Examples are *suspicious activity reports* (SARs), tips, and leads. This may appear to be a contradiction; however, it is an inherent part of the intelligence process that has a remedy. A law enforcement agency has an obligation to determine whether there is veracity to the criminal allegations found in SARs, leads, or tips. This is the purpose of the two-tiered temporary file and permanent file records system used for intelligence records (a remedy developed in the *LEIU File Guidelines*<sup>243</sup> that is a practical application of 28 CFR Part 23). As the name implies, the temporary file is simply a place (including a specifically designated computer record) to file information while a determination if a criminal predicate exists. If *reasonable suspicion* is not established, then the information is purged. If the criminal predicate is established, then the information is placed in a permanent file in the criminal intelligence records system.<sup>244</sup> Thus, in practice, *retention* of collected information becomes the critical issue where the criminal predicate must be demonstrated.

Care was taken to specify that a criminal predicate must be established when collecting and retaining information that **identifies people or organizations**. The critical point to note is that constitutional protections attach when identity is established.

The intelligence process also seeks to collect information about crime trends, methods of criminal operations (sometimes referred to as the modus operandi or criminal tradecraft), ideologies of criminal extremists, and other nonidentifying information that helps describe and understand criminal phenomena. For example, understanding the rationale used by eco-fascists<sup>245</sup>—people who adhere to a belief system mixing white nationalism and environmentalism that was the basis of deadly terror attacks in Christchurch, New Zealand, and El Paso, Texas—helps understand motivations and potential targets of future attacks. The criminal predicate rule does not apply to these types of information when individuals and organizations are not identified.

A final issue of collection—and the entire intelligence process—is information security<sup>246</sup> (INFOSEC). INFOSEC focuses on identifying and protecting information that might provide an intelligence target with clues to an inquiry, thereby enabling the target to thwart the inquiry. To protect the integrity of the intelligence inquiry, it is essential to maintain security of collection sources, methods, and content.

## PROCESSING/COLLATION

This phase of the intelligence process has four distinct activities, as illustrated in Figure 3-3. The first is to evaluate raw data from the collection phase to determine its value for analysis. An assessment should first examine

---

242 Standards of proof, from lowest to highest are reasonable suspicion, probable cause, preponderance of the evidence, and proof beyond a reasonable doubt.

243 [https://it.ojp.gov/documents/LEIU\\_Crim\\_Intell\\_File\\_Guidelines.pdf](https://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf)

244 By policy, information in the temporary file should have a time deadline for its review, resulting in action to purge or move the information to a permanent file.

245 <https://www.newstatesman.com/science-tech/social-media/2018/09/eco-fascism-ideology-marrying-environmentalism-and-white-supremacy>

246 <https://www.cdse.edu/catalog/information-security.html>

the *reliability of the source* of the information. Ideally, an assessment of reliability was recorded by the individual who was the primary collector. The importance of this assessment relates to the confidence level an analyst will give the information when making judgments during the analysis. As a simple illustration, the conclusion drawn by an analyst when using information derived from a completely reliable source will be different than a source deemed to be unreliable. (In both cases, corroborating information should be sought.)

The next assessment during the evaluation phase examines the *validity* of the raw information. Validity is epitomized by the question, “Does the information actually portray what it seems to portray?” Validity assessment may be done by the collector and/or the analyst. The collector may believe that if information comes from a reliable source and it is logical, then validity is high. Conversely, the analyst may have competing information from a different reliable

source that questions the validity of the information. For example, an officer may report that a professor (considered a reliable source) saw a college student who is known to have anger management issues away from campus with a semiautomatic handgun. However, the analyst has information that the student, who has been reported before, is a replica gun collector. In cases such as this, the analyst should define intelligence requirements to collect additional information so as to gain the most accurate raw information to determine whether the handgun is real and, if so, whether the student poses a threat. Thus, the intelligence cycle starts over, even though this is only the third phase.

Source reliability and information validity are often initially assessed using ordinal scales similar to those depicted in Figure 3-4. These are rudimentary scales but nonetheless provide important fundamental guidelines for intelligence assessments. As such, law enforcement personnel should be trained to provide these assessments when collecting information for the intelligence cycle.

A next step of evaluation is to assess the *method* by which the information was collected to ensure that it meets constitutional standards. The NCISP states:

**Recommendation:** Law enforcement and homeland security agencies should maintain a strong emphasis on the protection of privacy, civil rights, and civil liberties (P/CRCL) in all law enforcement and homeland security actions and operations.

#### Action Items

- ◆ All law enforcement and homeland security agencies should develop a privacy policy and ensure that the tenets of the policy are implemented.
- ◆ Law enforcement and homeland security agencies should develop and/or enhance existing agency policies that may have P/CRCL implications (such as social media use, First Amendment-protected demonstrations).
- ◆ Agencies should consider, as a best practice, performing a Privacy Impact Assessment in order to uncover the privacy risks and vulnerabilities within their information sharing systems.<sup>247</sup>

247 Criminal Intelligence Coordinating Council. (2013). *National Criminal Intelligence Sharing Plan, Version 2.0*. Washington, DC: GIWG, p. 20.

FIGURE 3-3: PROCESSING AND COLLATION ACTIVITIES



FIGURE 3-4: EXAMPLE OF RELIABILITY AND VALIDITY RATING SCALES

## Source Reliability

<b>A</b>	<b>COMPLETELY RELIABLE</b>	<ul style="list-style-type: none"><li>• No Doubt of Trustworthiness, Authenticity</li><li>• The Source Is Competent</li><li>• History of the Source Is Completely Reliable</li></ul>
<b>B</b>	<b>USUALLY RELIABLE</b>	<ul style="list-style-type: none"><li>• Some Doubt of Trustworthiness, Authenticity</li><li>• Some Doubt About Competence</li><li>• Majority of Time a Reliable Source</li></ul>
<b>C</b>	<b>FAIRLY RELIABLE</b>	<ul style="list-style-type: none"><li>• Usually Some Doubt of Authenticity, Trust</li><li>• Usually Some Doubt About Competence</li><li>• Reliable Source Some of the Time</li></ul>
<b>D</b>	<b>NOT USUALLY RELIABLE</b>	<ul style="list-style-type: none"><li>• Definite Doubt About Authenticity, Trust</li><li>• Definite Doubt About Competence</li><li>• History of Occasional Reliability</li></ul>
<b>E</b>	<b>UNRELIABLE</b>	<ul style="list-style-type: none"><li>• Great Doubt About Authenticity, Trust</li><li>• Great Doubt About Competence</li><li>• History of Unreliable Information</li></ul>
<b>F</b>	<b>NO JUDGMENT</b>	<ul style="list-style-type: none"><li>• Cannot Be Judged</li><li>• No Information to Base Decision</li></ul>

## Information Validity

<b>1</b>	<b>CONFIRMED</b>	<ul style="list-style-type: none"><li>• Confirmed by Other Independent Sources</li><li>• Logical in Itself</li><li>• Agrees With Other Information on Subject</li></ul>
<b>2</b>	<b>PROBABLY TRUE</b>	<ul style="list-style-type: none"><li>• Not Confirmed</li><li>• Logical in Itself</li><li>• Agrees With Other Information on Subject</li></ul>
<b>3</b>	<b>POSSIBLY TRUE</b>	<ul style="list-style-type: none"><li>• Not Confirmed</li><li>• Reasonably Logical in Itself</li><li>• Agrees Somewhat With Other Information</li></ul>
<b>4</b>	<b>DOUBTFULLY TRUE</b>	<ul style="list-style-type: none"><li>• Not Confirmed</li><li>• Not Illogical in Itself</li><li>• Not Believed When Received, But Possible</li></ul>
<b>5</b>	<b>IMPROBABLE REPORT</b>	<ul style="list-style-type: none"><li>• The Contrary is Confirmed</li><li>• Is Illogical in Itself</li><li>• Contradicted by Other Information</li></ul>
<b>6</b>	<b>NO JUDGMENT</b>	<ul style="list-style-type: none"><li>• Cannot Be Judged</li><li>• No Information to Base Decision</li></ul>

A critical issue for information collection by law enforcement is the assessment of the *method* used to collect the data. When a law enforcement agency is collecting information, it must follow lawful processes. For example, information collected about a person should be consistent with constitutional standards. Two constitutional issues of most common concern are privacy related to the method of collection and freedom of expression when dealing with ideological extremists. Beyond these, of course, is assessing the Fourth Amendment constitutional integrity of physical evidence collected as well as Fifth and Sixth Amendment protections of statements made during interrogations.<sup>248</sup>

The issue of lawful collection methods is important for three reasons. First, it is a constitutional guarantee that law enforcement officers have sworn to uphold. Second, if there is a criminal prosecution of the intelligence target, critical evidence could be excluded from trial if the evidence were not collected in a lawful manner.<sup>249</sup> Third, if a pattern emerges that information about individuals was collected on a consistent basis that does not meet constitutional standards, this may open the agency to civil liability for civil rights violations.<sup>250</sup>

Thus, not only is this assessment a professional obligation, but it is also important for prosecutions and for protecting the agency. Once again, both training and a review process should seek to ensure that the information was lawfully collected and that the facts of the collection are carefully documented.

The third activity in the collation/processing phase is to integrate the new information with existing data. During this process, in consideration of all other information that has been collected, the following questions may be asked:

- ◆ Does the information meet the criminal predicate test?
- ◆ Is the information relevant and material (as opposed to being just “interesting”)?
- ◆ Does the information answer questions from the analysis?
- ◆ Does the information add new questions to the analysis?
- ◆ Does the information need corroboration?
- ◆ Does the information support the working hypotheses of the inquiry, or does it suggest a new or alternate hypothesis?
- ◆ What additional information is needed for validity, if any, as a result of the new information?

The answers to these questions will help define requirements and directions for the inquiry. This process also includes organizing and indexing the data to standardize<sup>251</sup> the data fields and enhance the ability to make accurate data comparisons.

A final activity during this phase is *deconfliction*. This is the process or system used to determine whether multiple law enforcement agencies are conducting inquiries or operations involving the same person, crime, or target.

Event deconfliction is the process of determining when law enforcement personnel are conducting an event in close proximity to one another at the same time. Events include such law enforcement actions as undercover operations,

---

248 The right to be protected against self-incrimination and the right to counsel during a custodial interrogation, based on *Miranda v. Arizona* 384 U.S. 436 (1966).

249 According to the Exclusionary Rule and the Fruit of the Poisonous Tree Doctrine. [https://www.law.cornell.edu/wex/fruit\\_of\\_the\\_poisonous\\_tree](https://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree)

250 As an example, see <https://www.lohud.com/story/news/local/rockland/clarkstown/2019/02/05/clarkstown-black-lives-matter/2781051002/>.

251 A common problem of standardization is in the spelling of names, particularly names that can have different spellings. As an example, alternate spellings of a name exist for the same person, such as *Osama bin Laden* and *Usama bin Laden*. Lack of standardization can cause critical information to be missed, particularly during a standard computer search, in the analytic process.

surveillance, or executing search warrants. When certain elements (e.g., time, date, or location) are matched between two or more events, a hit (or conflict) results. Immediate notification is then made to the affected agencies or personnel regarding the identified conflict.<sup>252</sup>

The deconfliction process not only identifies whether multiple inquiries or activities exist, but also provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of the inquiry. Deconfliction helps maintain the integrity of cases, saves resources, and can significantly enhance the safety for operational personnel. Moreover, if it is learned that multiple agencies are investigating the same target, this can enhance information sharing. The information systems used for deconfliction are often referred to as “pointer systems” for the reason that they can point inquiries about cases to the different agencies that are investigating the same individuals.

As noted by the Commission on Accreditation of Law Enforcement Agencies (CALEA),

Event Deconfliction Systems are used by public safety to identify law enforcement events occurring in close proximity, thereby promoting safety and effectiveness. This is particularly important for agencies in concurrent or contiguous jurisdictions that are involved in high-risk activities, such as undercover operations, surveillance, execution of search warrants, or fugitive apprehension. The Event Deconfliction System receives information from agencies and then provides notifications when qualifying activities are occurring in close proximity.<sup>253</sup>

There are several deconfliction systems available to law enforcement:

- ◆ National Drug Pointer Index<sup>254</sup> (NDPIX) managed by the Drug Enforcement Administration
- ◆ National Virtual Pointer System<sup>255</sup>
- ◆ Nationwide Officer Safety Event Deconfliction<sup>256</sup>
- ◆ Nationwide Deconfliction Pointer Solution<sup>257</sup>
- ◆ Deconfliction and Information Coordination Endeavor (DICE)<sup>258</sup>
- ◆ RISS Officer Safety Event Deconfliction System (RISSafe)<sup>259</sup>

In sum, the Processing/Collation phase of the intelligence cycle is important for two reasons: (1) it seeks to provide quality control of information through the process; and (2) it provides important insights in defining intelligence requirements.

## ANALYSIS

Analysis is at the heart of the intelligence process. Entire books have been written on analytic methodologies and the critical thinking process. The intent of the current discussion is not to repeat this information but to provide some insights about analytic responsibilities in the context of the intelligence cycle that will be of benefit to the intelligence consumer.

252 Carr, T. (2017.) “Event Deconfliction Avoids Operational Conflicts, Saves Lives, and Solves Cases.” *The Police Chief*. (February). <https://www.policechiefmagazine.org/event-deconfliction-avoids-operational-conflicts/>

253 [https://www.ncirc.gov/Deconfliction/Documents/CALEA\\_Standard\\_Event\\_Deconfliction\\_Aug15.pdf](https://www.ncirc.gov/Deconfliction/Documents/CALEA_Standard_Event_Deconfliction_Aug15.pdf)

254 [https://www.dea.gov/sites/default/files/2018-06/ndpix\\_signed\\_pia\\_032907.pdf](https://www.dea.gov/sites/default/files/2018-06/ndpix_signed_pia_032907.pdf)

255 [https://www.ncirc.gov/Deconfliction/Documents/National\\_Virtual\\_Pointer\\_System.pdf](https://www.ncirc.gov/Deconfliction/Documents/National_Virtual_Pointer_System.pdf)

256 <https://www.ncirc.gov/deconfliction/>

257 <https://www.ncirc.gov/deconfliction/Resources.aspx>

258 <https://dice.usdoj.gov/dice/login/>

259 <https://www.riss.net/rissafe/>

The analytic process is essentially the scientific approach to problem solving. It is the use of established research methodologies—both quantitative and qualitative—that seek to objectively integrate correlated variables from a body of raw data to derive an understanding of the phenomena under study. It is synergistic in nature, in that the completed analysis provides knowledge rather than a simple recitation of facts. However, the outcome is only as good as (1) the quality of the raw information submitted for analysis; and (2) the quality of the analysis. Hence effective training, policy direction, supervision, and an operational plan for the intelligence function are all essential for the analytic process to produce robust and actionable intelligence.

The term “actionable intelligence” has two fundamental applications for law enforcement. The first is tactical, wherein the output of analysis must provide sufficient explicit information that operational units can develop some type of response or action. In some cases, that response is minimal, such as providing indicators of terrorism or criminal activity for patrol officers to observe. In other cases, it may involve a complex operational activity to make arrests. The second application of actionable intelligence is strategic, describing changes in the threat picture of a jurisdiction or region. That is, the intelligence may describe changes in crime types and/or crime methodologies. Based on this information, law enforcement leaders can take steps to protect community safety to prevent or mitigate a threat. Both types of actionable intelligence rely on effective analysis.

The outputs of the analytic process are reports referred to as *intelligence products* (described in more detail both in the following section on dissemination and in a later chapter). During the analysis, an intelligence analyst prepares explicit inferences about the criminal enterprise to understand its effects. These are typically expressed as *conclusions*, *forecasts*, and *estimates* that are explained in the products.

**A conclusion**, as the term infers, is a definitive statement about how a criminal enterprise operates, its key participants, its characteristics, and the criminal liability of each. A *forecast*<sup>260</sup> describes the expected implications of the criminal enterprise, the future of the enterprise, changes in the enterprise, or participants and threats that are likely to emerge from the enterprise. An *estimate* focuses on physical, social, and/or monetary effects, changes in commodity transactions, and/or likely future effects of the criminal enterprise. For example, it can identify probable victims of a crime threat, profits from a new criminal enterprise, economic losses associated with a terrorist attack, or the increase of contraband in a community from a criminal enterprise.

There are different consumers of intelligence, each of whom has somewhat different analytic needs. For example, line officers need to have information that concisely identifies criminal indicators, suspects, addresses, crime methodologies, vehicles, and other observable factors thought to be associated with a criminal enterprise. Administrators and managers need information on the changing threat environment that has implications for the deployment of personnel and the allocation and expenditure of resources. Analysts need to develop a comprehensive package of information that includes raw data sources, methods, and intelligence requirements. Intelligence reports that contain little more than suppositions, assumptions, rumors, or alternate criminal scenarios are not actionable.

## DISSEMINATION

Regardless of the type of intelligence product, it has virtually no value unless the system is able to get the right information to the right people in a time frame that will permit users to act on the intelligence. Dissemination—or information sharing—seeks to accomplish this goal. There are many related issues that could be discussed, including various intelligence and information records systems, privacy issues, information system security issues, operations security of shared information, the means of dissemination, interoperability issues, and the Global Justice

---

<sup>260</sup> Sometimes the word “prediction” is used rather than “forecast.” Prediction is a definitive statement of the future which, in reality, is virtually impossible to determine. Intelligence analysis is probabilistic in nature; hence the term “forecast” is used to describe what is likely to occur, given the currently known facts and evidence.

Data Standards.<sup>261</sup> However, the intent of the current discussion is to describe the general philosophy and rules of intelligence dissemination as a step in the intelligence cycle.

Pre-9/11, the general philosophy of intelligence dissemination tended to focus on information security. That is, intelligence records were not widely disseminated out of a concern that critical information would fall into the wrong hands, thereby jeopardizing the inquiry as well as possibly endangering undercover officers, informants, and collection methods. (Tongue-in-cheek, this was sometimes referred to as SPS or “secret police stuff.”) While these issues remain important, the post-9/11 philosophy is radically different. Indeed, law enforcement seeks to place as much information in the hands of as many authorized people who need it to prevent threats from reaching fruition. Basically, the idea is that the more authorized people who receive the information, the greater the probability of identifying and interrupting a threat. Perhaps the critical question is, “Who is considered an authorized person?”

**Right to know and need to know.** Even with this changed philosophy, there are rules of dissemination that seek (1) to protect individuals’ civil rights and (2) maintain information security as needed. To accomplish these goals, the first rules of dissemination provide criteria to determine who should receive the intelligence. The accepted standard has a two-pronged test:

1. Does the individual to which the information is to be disseminated have the right to know the information? This is determined by the recipient’s official capacity and/or statutory authority to receive the information being sought.
2. Does the recipient have a bona fide need to know the information? The information to be disseminated is pertinent and necessary to the recipient to prevent or mitigate a threat or assist and support a criminal investigation.<sup>262</sup>

Intelligence products that provide information on criminal indicators and methodologies are intended for wide distribution so that officers can be aware of these factors during the course of their daily activities. As a general rule, it can be assumed that anyone working in law enforcement meets the right-to-know and need-to-know tests for these types of intelligence. However, intelligence reports related to a specific criminal inquiry that identifies individuals or organizations should have more limited dissemination. As a general rule, while all law enforcement officers would have the right to know this information, only those officers working on some aspect of the inquiry have the need to know the information.

With the changing intelligence philosophy and the recognized need to involve the private sector and non-law-enforcement government personnel in the Information Sharing Environment (ISE), the application of right to know and need to know has changed somewhat from the pre-9/11 era.<sup>263</sup> For example, anyone in law enforcement has the right to know intelligence (by virtue of his or her employment). Similarly, a member of the National Guard or a Department of Homeland Security (DHS) intelligence analyst working in a fusion center would have the right to know intelligence by virtue of his or her assignment, even though he or she is not a law enforcement employee. In yet a different application, the corporate security director of a nuclear power plant would have the right to know intelligence related specifically to the security director’s responsibilities of protecting the plant.

Once again, because of the new intelligence philosophy, a significantly broader range of people have the need to know intelligence. The rationale, as stated previously, is that all officers need to be aware of threats to increase the probability of stopping the threat. The need to know intelligence by non-law-enforcement personnel should

<sup>261</sup> As a comprehensive resource, see <http://it.ojp.gov>.

<sup>262</sup> Adapted from: Association of Law Enforcement Intelligence Units. (Revised 2002). *Criminal Intelligence File Guidelines*, Section IX: File Dissemination. Sacramento, CA: LEIU.

<sup>263</sup> A review of the goals and action steps in the *Information Sharing Environment Implementation Plan* clearly demonstrates the mandate for these additional intelligence consumers. See [https://www.dni.gov/files/ISE/documents/DocumentLibrary/ise-impplan-200611\\_0.pdf](https://www.dni.gov/files/ISE/documents/DocumentLibrary/ise-impplan-200611_0.pdf).

be determined on a case-by-case basis. For example, in all likelihood there is no need for a DHS analyst to know intelligence related to an auto-theft ring. However, the analyst would need to know information related to a criminal enterprise smuggling cocaine from Colombia because of the value of communications between the DHS analyst and other federal agencies, such as the Drug Enforcement Administration (DEA) or Immigration and Customs Enforcement (ICE).

**Third Agency Rule.** Another information sharing guideline is found in what is commonly called the Third Agency Rule. Essentially, the rule is that if an officer receives intelligence from an intelligence source (such as a fusion center), that officer cannot further disseminate the intelligence to a third party without permission of the original source.<sup>264</sup> Thus, for example, Officer Adam receives intelligence from the Central Fusion Center. Officer Adam should not give the intelligence directly to Officer Baker without first gaining permission from the Central Fusion Center. This is a general rule—with some exceptions that will be discussed later—and it will be stated or applied differently between agencies. Consumers of intelligence should be aware of the local applications of the Third Agency Rule.

In law enforcement, two kinds of intelligence may be produced: case or investigative intelligence and intelligence products. Case intelligence identifies people. Intelligence products provide more general information about threats and indicators. For investigative intelligence, it should be assumed that the Third Agency Rule is intact. For intelligence products, it is generally assumed that the Third Agency Rule is waived. Fundamentally, the reason is that when individuals or organizations are *not* identified in intelligence products, civil rights do not attach. Again, a review of agency policy must be made to understand the exact applications of the rule locally.

It should be reinforced that in law enforcement intelligence, both the right-to-know and need-to-know provisions as well as the Third Agency Rule serve two purposes: to protect individuals' civil rights and to maintain operations security of intelligence inquiries. This being said, such dissemination practices do not carry the force of law and typically have minimal or no sanctions if a person does not comply with the guidelines. In a few cases, there are regulatory obligations for following the guidelines—such as an agreement to abide by the rules as a user of a criminal intelligence information system—but in most cases, it is a professional agreement.

**Classified information.**<sup>265</sup> A great deal has been written about classified information. For the most part, these regulations apply to the Intelligence Community and federal law enforcement. As a rule, unless working in a fusion center or assigned to a Joint Terrorism Task Force (JTTF), most SLTLE officers do not have security clearances or access to classified information; however, having a basic understanding of information classification provides perspective for the following discussion. Essentially, classified information is a designation of information that is critical to the security of the United States. There are explicit processes and procedures for classifying, storing, providing access to, and generally handling this information which have sanctions, including federal criminal violations, if the processes are violated.

There has been a great deal of debate about the need for security clearances for SLTLE personnel. Law enforcement executives and managers argue that they need a security clearance to have access to information about threats within their jurisdictions. On this same theme, a report from the Congressional Research Service (CRS) stated:

... these officials might need some access to classified information, for example, “real time” intelligence information concerning terrorism threats, to adequately plan, coordinate, and execute homeland security activities.<sup>266</sup>

---

264 Often, an intelligence product has a notification about sharing, such as “This bulletin may be widely disseminated to law enforcement personnel.” Such a notification meets the requirement of consent to share with respect to the Third Agency Rule.

265 For detailed information on classified information, see the Information Security Oversight Office (ISOO) at <https://www.archives.gov/isoo>.

266 Reese, S. (2005). *State and Local Homeland Security: Unresolved Issues for the 109th Congress*. Washington, DC: Congressional Research Service, Library of Congress, p. 11.

Federal authorities respond that they will provide all information needed to SLTLE personnel about threats within a community—a response met with some skepticism.<sup>267</sup>

Another issue to be aware of is that federal security clearances are not universal. For example, if a law enforcement executive has a security clearance from the U.S. Department of Defense as a result of his/her military reserve status or an officer has a DEA clearance that was investigated by the U.S. Office of Personnel Management (OPM) as part of an Organized Crime Drug Enforcement Task Force (OCDETF), those clearances may not be recognized by the FBI as granting access to classified information for which the FBI is the custodian. These are issues of which the reader should be aware—they remain to be resolved.

A range of issues related to classified information and security clearances are discussed in a later chapter. Suffice it to note at this point that classified information may be disseminated only to an individual who has the appropriate type of security clearance,<sup>268</sup> which establishes the right to know. The need to know must still be determined before dissemination, even if the individual has the appropriate level of clearance.

**Sensitive But Unclassified information (SBU)/Controlled Unclassified Information<sup>269</sup> (CUI).** Sensitive But Unclassified (SBU) information—including but not limited to “tear line”<sup>270</sup> intelligence reports—does not have any statutory restrictions, clearances, or sanctions as are found with classified information. Rather, the SBU designation is more akin to a professional responsibility that is expected to be honored in light of one’s professional obligations. While most SLTLE officers do not have security clearances, virtually all have access to Sensitive But Unclassified (SBU) information. SBU information may have been previously classified, but in these cases typically sources and methods of collection have been removed, thereby declassifying the information and rendering it SBU. In other cases, the inherent sensitivity of the information based on its character—such as an analysis of terrorist tactics that produces indicators of terrorist activity—may warrant the SBU label.

There are many forms of SBU labels, particularly at the federal level; however, the two most commonly used in law enforcement are Law Enforcement Sensitive (LES) and For Official Use Only (FOUO). As a general rule, LES information may be shared with anyone in the law enforcement community (sworn or nonsworn) who has the right to know and the need to know the information. FOUO means the information may be shared with anyone who has the right to know and need to know. For example, if there was information about a threat by white nationalists to a synagogue, this information would need to be shared with the leadership and security personnel of the synagogue. These are

---

267 In a joint publication by the Major Cities Chiefs Association (MCCA) and the Major County Sheriffs of America (MCSA), a resolution to handle the backlog of security clearances applications for SLTLE personnel was offered as follows:

Chiefs and sheriffs will join with DHS to implement a comprehensive plan to eliminate the backlog of pending applications and expedite the security clearance process. Features of the plan include:

1. Reduction in requests for TOP SECRET/Sensitive Compartmented Information (TS/SCI) clearances and accesses.
2. Focus primarily on faster and more useful SECRET level clearances.
3. Law enforcement agencies propose to conduct background investigations and expedite adjudication of SECRET level clearances.
4. DHS agrees to provide training on clearance process.
5. DHS agrees to assist major law enforcement agencies in expediting priority security clearances.
6. Per federal statutes/regulations, DHS commits to accept clearance granted by other agencies.

Source: *Intelligence and Information Sharing: DHS and Law Enforcement*. (2007). Major Cities Chiefs Association and Major County Sheriffs of America, p. 3. (Unpublished report.)

268 For a description of the types/levels of federal security clearances and their meanings, see <https://federalemployeelawblog.com/2015/06/02/114/>.

269 <https://www.archives.gov/cui>

270 The tear line refers to a classified report that includes a summary of the report at the bottom, excluding information about the sources of information and/or methods of information collection. This summary may be torn off the report; hence it is referred to as tear-line information and is SBU.

general rules which, in practice, have no enforceable sanctions should they be violated. Rather, they provide guidance on disseminating sensitive information and rely on the professional decisions of those who receive the information to maintain security.

Particularly for sensitive information that may need to be shared with the private sector or government personnel outside a specific intelligence group, some agencies have adopted the Traffic Light Protocol to guide the dissemination of information.

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). . . .TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration.<sup>271</sup>

Because of the lack of explicit guidance and the wide range of SBU dissemination labels, there is both uncertainty and inconsistency in dissemination processes. As a result, one of the mandates from the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) was to develop the Information Sharing Environment (ISE), which included, as one of the ISE Program Manager’s responsibilities, the creation of a labeling protocol for SBU information that had a consistent meaning and application across the entire ISE. This is particularly true given the important role of sharing unclassified terrorist information with state, local, and tribal law enforcement. There is a need to disseminate information—that is, to share important information with others. However, that information sharing must be *controlled*—protecting information and ensuring that it is not disseminated inadvertently.

As a result, the federal government is in the process of changing SBU label markings with a new information control model called Controlled Unclassified Information (CUI). There are a number of new factors with CUI that provide more specific, and universal, direction than has existed with SBU labels. Since a discussion of these details is provided in in a later chapter, it should be noted, for purposes of *dissemination* in the current discussion, that there are controls for establishing the right to know for unclassified information that needs to be safeguarded.

Whereas pre-9/11 intelligence products were rarely disseminated to most police officers, in the post-9/11 environment, with its strong emphasis on information sharing, officers tend to get so much information they cannot consume it all. Hence, a balance needs to be achieved. Information dissemination needs to be selectively shared so that officers are not overwhelmed. That is, efforts need to be made to give information to those officers who actually need the intelligence. For example, a threat determined by the Missouri Information Analysis Center at a community event in Kansas City would likely not need to be disseminated across the state to officers in St. Louis. Similarly, the information needs to be easily and readily consumable—just the core information that officers need.<sup>272</sup>

## REEVALUATION

The classic definition of a system is a series of interconnected component processes that have an interrelated purpose, such that a change in one component will affect the other components. The intelligence process is indeed a system. As each component—or phase—processes information, it affects the body of knowledge in the other components as related to the intelligence inquiry. Just as in any other system, homeostasis—that is, a steady state of the system—must be maintained. This is the purpose of reevaluation: To ensure that all information is being processed in a comprehensive manner, the intelligence process must be ongoing, with each new piece of information in the process being added to the full body of new knowledge to aid in developing the most precise intelligence

---

271 <https://www.us-cert.gov/tlp>

272 One intelligence commander stated that his unit produced “red-light reports” for uniformed officers. The commander wanted brief reports that would enable an officer to read the key information on the in-car computer during the time that he or she was stopped at a traffic signal.

possible. Reevaluation also serves as a measurement to determine whether the intelligence products created by this process have value. Are threats accurately identified? Are intelligence products actionable? Are all components of the intelligence process functioning as intended? Are effective operational interventions able to be employed based on the intelligence? When problems or discrepancies are identified, they need to be corrected and reevaluated.

## CONCLUSIONS

The intent of this chapter was to describe the intelligence process (or cycle) as depicted in the *National Criminal Intelligence Sharing Plan*. As can be seen, many critical terms and concepts are essential for the intelligence process to work. The core purpose of the discussion was to introduce key terminology and concepts to provide a perspective on how these relate to the production of actionable intelligence and, as will be seen, the role of the process in other intelligence initiatives, notably intelligence-led policing (ILP).





# CHAPTER 4

## TECHNOLOGY AND INTELLIGENCE

Law enforcement intelligence has used technology of various forms for decades. Technologies to collect information include such tools as pen registers,<sup>273</sup> wiretaps,<sup>274</sup> body recorders, infrared video and imagery, enhanced listening devices (such as parabolic antennas), video surveillance, and Global Positioning Satellite (GPS) tracking devices, among others. Similarly, law enforcement began adopting mainframe computers in the late 1960s and personal computers (PCs) in the early 1970s; today, law enforcement professionals also use tablets and smartphones to store, analyze, and share information.<sup>275</sup>

As law enforcement intelligence received new vigor in the post-September 11, 2001 (post-9/11), environment, technology played an increasingly important role. There was increased use of online open sources to learn about extremist ideologies and search for leads. New intelligence resources were more readily available and easy to access as a result of technological applications, many of which were products of the Global Justice Information Sharing Initiative<sup>276</sup> and its various working groups. Information sharing between law enforcement agencies became easier and faster, and there was growing use of digital video, not only from surveillance cameras but from a wide range of

---

273 <https://cyber.harvard.edu/privacy/Introduction%20to%20Government%20Investigations.htm>

274 A pen register records telephone numbers, dates, and times and length of calls from a particular phone. A wiretap intercepts and records content (conversations and other transmitted data) from the target phone.

275 For a history of police adoption of technology, see *The Evolution and Development of Police Technology*. (1998). Washington, DC: Seaskate, Inc. and the National Institute of Justice. <https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf>

276 <https://it.ojp.gov/>

## FACIAL RECOGNITION CICC RECOMMENDATION

- ◆ Any possible connection or involvement of an individual to a criminal investigation must be determined through further analysis and investigation.
- ◆ If, after completing the analytic process, face recognition information is downloaded into a criminal intelligence or investigative file, the information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information govern its use.
- ◆ Face recognition information—probe photographs, image repositories, lists of most likely candidates, etc.—is not considered criminal intelligence, criminal history, or SAR information. As such, the laws, regulations, and policies that specifically apply to those types of situations may not apply to face recognition information until such time as it is downloaded and incorporated into a criminal intelligence or investigative case file. It is the further analytic and investigative processes by trained examiners that associate face recognition results with an identifiable individual.

*Face Recognition Policy Development Template for Use in Criminal Intelligence and Investigative Activities.* (2017). Washington, DC: Criminal Intelligence Coordinating Council, p. 4. <https://it.ojp.gov/GIST/1204/Face-Recognition-Policy-Development-Template-For-Use-In-Criminal-Intelligence-and-Investigative-Activities>

sources, increasingly from smartphones.<sup>277</sup> Technology was giving analysts access to raw information quickly, easily, and safely. Also, with each iteration of new technology, analytic tools were getting more robust, with growing capabilities. Virtually all of these collection, storage, and analytic technologies are still used in versions that have been upgraded and refined over the decades.

Overall, law enforcement’s use of technology, per se, has not driven new policing philosophies for crime prevention, criminal investigation, delivery of police service, or public safety. Indeed, policing philosophies—such as community policing or intelligence led policing—are largely independent of technology. However, technology helps operationalize those philosophies more efficiently and effectively. Whereas in the past, for example, public education might have required attending public meetings and providing public service announcements on television and radio, today officers can post many public education initiatives to a police department’s Web page, Facebook page, or Instagram account or send out a tweet. Virtually everything an intelligence analyst does is made faster, easier, and more comprehensive using technology.

As another example, building on the lessons learned from the Integrated Criminal Apprehension Program<sup>278</sup> of the 1970s, CompStat<sup>279</sup> (computerized statistics) was developed. CompStat provided detailed crime analysis on a timely basis so that operational responses could be developed to disrupt crime trends. Technology enabled crime analysis to be more detailed, more precise, and more quickly produced, which, in turn, fostered the implementation of CompStat.

This chapter does not discount the continued value of technologies that law enforcement has relied on for decades to support the intelligence process. However, greater focus in this chapter will be given to emerging, and largely more personally invasive, technologies used for the intelligence process. Moreover, the discussion will focus on a five-point model to apply emerging technologies to the intelligence function.

## EMERGING TECHNOLOGIES AND LAW ENFORCEMENT INTELLIGENCE: A PERSPECTIVE

Our society is experiencing an explosion of technology—faster networking speeds, high-volume storage at low cost, fast processing speeds, alternate means of communications such as social media, and the integration of audio and video digital images that can easily be shared among devices as well as manipulated in almost undetectable fashion (such as “deep

277 <https://www.textrequest.com/blog/history-evolution-smartphone/>  
278 <https://www.ncjrs.gov/pdffiles1/Digitization/43901NCJRS.pdf>  
279 [https://www.policeforum.org/assets/docs/Free\\_Online\\_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf](https://www.policeforum.org/assets/docs/Free_Online_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf)

fakes”<sup>280</sup>). Encrypted communications, communications, and messaging applications that permit messages to disappear; cell phone tracking with geographical and temporal data; and biometric access to smartphones, which in themselves store a treasure trove of data, are commonplace. A significant amount of that data is related to social media platforms<sup>281</sup> and e-commerce.<sup>282</sup> Even motor vehicles, appliances, and household items—such as refrigerators, garage door openers, televisions, and ovens—can be connected to communicate and store information as part of the Internet of things (IoT). For example, there is a growing application of digital vehicle forensics that seeks evidence used in a criminal investigation or traffic accident, which may include a vehicle’s onboard GPS data, media console data, Wi-Fi connectivity, and vehicle black-box data. The field also includes examination of smartphone apps that are either directly interactive with the vehicle systems or downloaded in the media console. Collectively, these data sources can provide a great deal of insight about the vehicle’s movement and even identify the driver, given smartphone connectivity, that could be valuable information for investigations and intelligence. Connectivity among diverse technologies has become an important focal point.

Artificial intelligence (AI), machine learning (ML), and predictive algorithms are changing the face of data analysis. Increasingly, all of these technologies are being coalesced into information streams that are being shared on social media and used in everything from marketing to e-commerce to service delivery. Even the economy has taken on new dimensions through the use of cryptocurrency. Collectively, these and other technologies are changing the social, economic, and political character of global societies. They provide great promise for human evolution but can also serve as an avenue to new forms of criminality, many of which are transnational in nature.

The discussion of all aspects of technology as they relate to the intelligence process—both as tools and as targets—is a discipline about which volumes could be written. Moving beyond the operational applications of these technologies is an additional discipline of how to apply law and policy to technological use—an area of study that has proven challenging because the criminal justice system must apply doctrine created for the physical world to the digital world. The current discussion is not meant to be a comprehensive essay on technology as an intelligence tool or as an intelligence target; rather, it is a primer. That is, the goal is to provide perspective on technological issues, applications, and processes as they relate to the intelligence process. Part informative, part food for thought, the discussion should be viewed as a starting point for examining the interaction of technology and the intelligence process.

## TECHNOLOGY USES FOR THE INTELLIGENCE PROCESS

While the topic could be approached in several ways, the current discussion takes a somewhat broad perspective in examining technology and the intelligence process in five areas:

1. Information collection, surveillance, and identification
2. Social media
3. Analysis of quantitative and qualitative raw information, particularly with Artificial intelligence (AI) applications
4. Information and intelligence sharing/dissemination
5. Accountability for the intelligence process

## INFORMATION COLLECTION, SURVEILLANCE, AND IDENTIFICATION

Of course, the lifeblood of the intelligence process is raw information. New technologies provide a variety of methods to collect information that is accurate, comprehensive, and current into the intelligence cycle. Drones that can record

<sup>280</sup> <https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html>

<sup>281</sup> In 2009, 21 percent of Americans had a social media profile; ten years later, 79 percent of Americans had a social media profile online. <https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/>

<sup>282</sup> In 2018, e-commerce sales in the United States totaled \$514.6 billion. <https://www.statista.com/topics/2443/us-ecommerce/>

people and objects in fenced-in yards or rooftops, even at night, using infrared optics; cell-tower data that can identify the presence of a mobile phone at a given date, time, and location; video surveillance cameras that can document the date, time, and location of a person and potentially identify that person through facial recognition<sup>283</sup>—these are all illustrations of currently available technology-driven information collection. However, use of these technologies brings controversy related to civil liberties and ethics. The law of civil rights establishes boundaries wherein it is legally permissible to collect information via a technology, while ethics addresses whether it is “right” or “proper” to use a certain technology in a certain manner. Neither provides clear answers.

**Privacy, civil rights, and civil liberties.** There is growing guidance in the area of privacy, civil rights, and civil liberties (P/CRCL), notably due to the work of the Criminal Intelligence Coordinating Council<sup>284</sup> (CICC), such as the *Privacy, Civil Rights and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*<sup>285</sup> and a range of additional publications<sup>286</sup> that address various aspects of policy and civil rights in the implementation of information collection technologies. While explicit laws and court decisions vary—and are evolving following the basic precepts of any type of information collection should provide good guidance:

- ◆ Use technologies for information collection as well as the collection of digital evidence (e.g., smartphone data, cell-tower data) following the same principles that are used for physical evidence: Obtain a warrant or apply one of the four exceptions<sup>287</sup> to the Fourth Amendment search warrant requirement with a thorough descriptive record of the probable cause and/or circumstances.
- ◆ Particularly with regard to the use of potentially invasive information technologies, be cognizant of the person’s reasonable expectation of privacy.
- ◆ Follow the guidelines of 28 CFR Part 23—information should be retained in a criminal intelligence records system only if there is a documented criminal predicate at the level of reasonable suspicion as related to the person about whom the information was collected.
- ◆ Retention of collected data in the noncriminal intelligence police records management system (RMS) or investigative records systems should have guidelines for collection and retention as well as a review process for purging, explicitly for personally identifiable information about persons for whom there is no nexus to a crime, a traffic offense, or an investigation or as witnesses.

Not surprisingly, research has found that digital evidence is increasingly used in criminal investigations, most notably information taken from computers and tablets that reflect contents of emails, documents, messages, and Internet search topics. The most frequent legal issue arising from the use of digital evidence on appeal was the propriety of the search and seizure.<sup>288</sup> While the collection of digital evidence provides more options for surreptitious information collection than the collection of physical evidence, the issue is not “What could be collected?” but “What should be collected?” Until there is more precedent defined in court cases, the safest collection is to conservatively adhere to established criminal procedure for physical evidence.

---

283 For a good resource on facial recognition application to law enforcement, see: *Law Enforcement Facial Recognition Use Case Catalog*. (2019). Alexandria, VA: IACP and IJIS Institute. <https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog>

284 <https://bja.ojp.gov/program/it/global/groups/cicc>

285 <https://bja.ojp.gov/library/publications/privacy-civil-rights-and-civil-liberties-policy-development-template-state>

286 <https://it.ojp.gov/global/working-groups/cicc/resources>

287 The four exceptions to the Fourth Amendment search warrant requirement are (1) search incident to arrest; (2) Plain View doctrine, (3) consent, and (4) exigent circumstances. While there is little settled law on the application of these exceptions to digital evidence, documentation of the logic used should be detailed, applying well-settled law of physical evidence.

288 Novak, M. (2020). “Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration.” *Journal of Digital Forensics, Security and Law*. Vol. 14, No.4, Article 3. <https://commons.erau.edu/jdfsl/vol14/iss4/3>

Documentation of the rationale to collect information or evidence is always valuable. Somewhat surprisingly, many law enforcement agencies have experimented with information collection technologies and even adopted some of the technologies without full policy review and support. Automated license plate readers (ALPR), drones, body cameras, and video surveillance networks are among the most common where, collectively, terabytes of information have been collected and stored with no review or purging. These are the kinds of situations that can lead to court challenges of police policy and potentially lawsuits against an agency. For example, information collected by ALPRs records data indiscriminately from all vehicles that pass the devices. The Coral Gables, Florida, Police Department recorded information on 30 million vehicles in one year and stored the information in a searchable database that could track the time, dates, locations, and identities of all vehicles. When the department was challenged in court, a Florida judge found merit in the argument that this collection and retention of information might violate state privacy laws.<sup>289</sup> Similarly, a Fairfax County, Virginia, judge ordered the Fairfax County police to stop maintaining a database of photos of vehicle license plates, with the times and locations where they were taken, ruling that “passive use” of data from ALPRs on the backs of patrol cars violates Virginia privacy law.<sup>290</sup> Law enforcement agencies routinely retain such information without review or purge information about vehicles where there is no criminal nexus—while the investigative value of such databases is understood, the practice should be reviewed and voluntarily changed before being forced to change by a court ruling.

**Ethics.** Ethical issues are even more difficult to apply because they reflect moral and social standards of what is “right,” which will vary between communities. It may be *lawful* to use a certain type of information collection technology, but is it *right*? That idea is captured in the often quoted saying, “With great power comes great responsibility.” Information collection and surveillance technologies in the hands of a law enforcement agency are indeed power. The ethical standard is to use the power not only in a lawful but also in a responsible manner.

If the use of technology is not consistent with the general moral sentiment of a community, then consideration should be given to not use the technology or to use it only in very restrictively defined circumstances. As an example, facial recognition technology is a form of image analysis that is widely used to aid in the identification of people. As the technology has become more readily available and less expensive, police departments across the country have increasingly used it as a routine tool in investigations,<sup>291</sup> potentially integrating it with body-worn cameras. However, the City of San Francisco has banned the use of facial recognition technology by police and other agencies<sup>292</sup> out of concerns for accuracy, particularly as it is used to identify racial and ethnic minorities, and for potential overreliance on the technology to identify criminal offenders. Those concerns have spread to other communities<sup>293</sup> in the United States; while not formally banning its use, if the sentiment of a community opposes facial recognition technology, it may be considered unethical for law enforcement to adopt it.

This is a simple illustration to emphasize the point that “just because it is legal does not mean it is right.” Part of the responsibility of a public law enforcement agency is to reflect the values of the community. Despite the value law enforcement may see in adopting a lawful technology, it is an obligation to consider the ethical aspects of the technology in light of predominant community attitudes. As noted by the Institute of Electrical and Electronics Engineers, “While ethical behavior is about doing the right thing, it doesn’t follow that the right thing is intuitively obvious.”<sup>294</sup> Introspection about emerging technology use should be part of the adoption process.

---

289 <https://www.thenewspaper.com/news/68/6823.asp>

290 <https://www.washingtonpost.com/crime-law/2019/04/02/judge-orders-fairfax-police-stop-collecting-data-license-plate-readers/>

291 <https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251>

292 <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>

293 <https://www.usatoday.com/story/tech/2019/12/17/face-recognition-ban-some-cities-states-and-lawmakers-push-one/2680483001/>

294 <https://www.standardsuniversity.org/e-magazine/march-2017/ethics-and-technology/>

The technologies that are increasingly adopted by law enforcement have significant capabilities, and the near future holds even more possibilities: driverless patrol cars with heads-up screens, collecting information as the cars patrol the streets; augmented reality to aid in training, crime scene reconstruction, and criminal investigation; “smart” police uniforms that could monitor and report on officers’ stress levels and the surrounding environmental conditions and provide situational awareness to supervisors about their officers. The question is not whether these technologies will be developed, but rather, should law enforcement use them when they become available? And, if so, how should the technologies be used?

We think these challenges can best be addressed by developing and using a digital ethics framework and a set of guiding principles that help create digital trust. Such a framework can help police leaders and their stakeholders think through the potential effects of technologies on officers and communities, identify unintended consequences and address the use of advanced technology for public safety.<sup>295</sup>

Digital ethics is broader and includes *how* technology and the data are used and the outcomes of that use. Transparent data and digital ethics create digital trust. Today, a successful business must understand the social and ethical consequences of using technology and work to mitigate negative consequences. Given the importance of the public trust that law enforcement holds, this is inescapably true for law enforcement as well. Just as police leaders today work to build community trust, in the very near future they will have to be concerned with building digital trust. Digital trust is created when an organization has good data integrity, security, and control and its use of technology and data is governed by a code of ethics. Digital trust between police agencies and their stakeholders could allow for a more rapid adoption of promising technology and mitigate some of the risks associated with it.<sup>296</sup>

**Types of information collection technologies and concerns for its use.** The key to the technologies described in this section is that they collect and/or compare information about specific persons that identifies them and often documents their behavior, including dates, times, and locations. While the technologies vary, the information from each can easily be used in the intelligence process, providing valuable data for the analysis of a threat. Increasingly, we are seeing companies that are *integrating* technologies such as body-worn cameras with facial recognition or acoustical gunshot detection systems that will activate cell-site simulators. As information collection technologies integrate, they not only become more powerful but also more controversial.

Critics of many technological developments argue that they are invasive, unreliable, and easily abused by law enforcement. While, for the most part, critics realize that these technologies will not be eliminated, they push for strong legislative limitation and policy guidance for their use by law enforcement. Legal precedence has been slow to keep up with the technology; hence there is somewhat greater pressure on law enforcement to establish reasonable guidelines. This has been occurring, in some cases with guidance of the Criminal Intelligence Coordinating Council<sup>297</sup> as well as the International Association of Chiefs of Police (IACP).<sup>298</sup> In other cases, policy guidance has been developed as a reaction to criticisms and, in a few cases, lawsuits.

With respect to information collection for the intelligence process, several of the more common technologies are described in Tables 4-1 and 4-2. The first table identifies the collection technology and provides a brief description of how it is used. The second table lists the same technologies with concerns expressed by critics. The lesson is to develop or amend policies and procedures associated with each technology to provide a strong justification for how it is used and the rationale for its use.

---

295 Technology and Police Operations Blog, Nola M. Joyce, Former Deputy Commissioner, Philadelphia Police Department, National Police Foundation, <https://www.policefoundation.org/technology-and-police-operations/>.

296 Ibid.

297 <https://it.ojp.gov/GIST/Browse>

298 <https://www.theiacp.org/iacp-technology-center>

These technologies can provide a wide array of detailed information useful for both the intelligence process and criminal investigations. Being cognizant of the concerns about the technologies and ensuring that policies and practices effectively address those concerns is a responsibility that should be proactively addressed. Moreover, personnel must be trained on the proper use of information collection technologies, and supervisors have the responsibility to ensure that policy guidance is followed.

Certainly, there are additional technologies that could be added to the lists—the intent, however, is not to be exhaustive in describing ever-changing technological developments. Rather, it is to provide an exercise of examining technological applications and then logically examining the legal and social issues that may arise. This can help guide adoption decisions and policy development before the technology is implemented.

**Next-Generation Identification.** Police agencies have been using fingerprints to identify people for over a century. Now, there is an ever-expanding array of biometric (and behavioral) characteristics being utilized by law enforcement and the Intelligence Community. These include voice recognition, palm prints, wrist veins, iris recognition, and gait analysis, among other examples. In an effort to harness new technologies and improve the application of tenprint and latent fingerprint<sup>299</sup> searches, the Federal Bureau of Investigation’s (FBI) Criminal Justice Information Services (CJIS) Division developed and incrementally integrated the Next Generation Identification (NGI) system, which provides the criminal justice community with the world’s largest and most efficient electronic repository of biometric

TABLE 4-1: TECHNOLOGY AND INFORMATION COLLECTION APPLICATIONS

Technology	Applications
AUTOMATED SOCIAL MEDIA MONITORING	Software is available to scan social media posts to identify threatening posts or those that suggest criminal activity. The amount of social media information is so vast that automated monitoring using artificial intelligence and machine learning is significantly more efficient and effective.
AUTOMATIC LICENSE PLATE READERS	Computer-controlled cameras are mounted to fixed locations or specially equipped mobile units, automatically capturing all license plates that come into view along with locations, dates, times, and photographs that are loaded onto a server, checked for wants and warrants, and retained to aid in criminal investigations.
BODY-WORN CAMERAS	Originally developed and used by police agencies for accountability to the public during police-public interactions, some video records have also been useful in criminal investigation and raw information collection.
DNA FROM COMMERCIAL BUSINESSES	People pay a fee and submit their DNA to a commercial business for an explicit purpose—typically, an ancestry analysis and/or a health analysis. The DNA is retained in the company records, with some companies permitting access to the records by law enforcement.
CELL-SITE SIMULATORS	These devices simulate actual cell phone towers that awaken and connect cell phones to log the dates, times, locations, and identifying numbers of cell phones in the area; some devices have the capability to intercept communications.

299 A tenprint consists of the intentionally recorded fingerprints of a known person, such as on a fingerprint card or digital imagery, as a record of that person. A latent fingerprint is that of a person who is typically unknown at the time the fingerprint is found, where it has been transferred from the person to the object.

TABLE 4-1: TECHNOLOGY AND INFORMATION COLLECTION APPLICATIONS (CONTINUED)

<p>DRONES/ UNMANNED AERIAL VEHICLES</p>	<p>Drones with video, audio, and even infrared capabilities are being used by law enforcement to monitor disasters, as search and rescue tools, to monitor crowds and public demonstrations, and in some cases to respond to major crime scenes. Some drones can even detect a person’s vital signs, as we learned during the 2020 pandemic. The drones provide comprehensive information from unique perspectives and aid in protecting the safety of first responders.</p>
<p>SMARTPHONES</p>	<p>Smartphone data can include content from texts and emails, photos, videos, and call history that can provide valuable insights for both investigations and intelligence analysis.</p>
<p>SURVEILLANCE AND SECURITY CAMERAS</p>	<p>Surveillance cameras in public and private areas are pervasive and can be used for crime prevention, criminal investigation, and general public safety. They are often available to law enforcement, including real-time access to police officers for observations.</p>
<p>FACIAL RECOGNITION</p>	<p>Algorithms map and measure facial features—such as bone structure, distance between the eyes, etc.—which are then rapidly compared with facial maps in databases wherein the identity of the mapped face is known.</p>
<p>TATTOO RECOGNITION</p>	<p>Borrowing from biometric technologies such as iris scanning, fingerprinting, and facial recognition, this technology focuses on the minute details of a tattoo, which are argued to be “minutely unique” since they are created by the hand of a tattoo artist who presumably cannot duplicate all details of a tattoo in the same minute detail (to include distances, shading, and thickness of lines).</p>

TABLE 4-2: INFORMATION COLLECTION TECHNOLOGY AND LEGAL/ETHICAL ISSUES

Technology	Issues
<p>AUTOMATED SOCIAL MEDIA MONITORING</p>	<ol style="list-style-type: none"> <li>1. Privacy issues wherein this approach is a “dragnet” looking at social media posts for which there are no reasonable grounds to target and collect information posted by most individuals.</li> <li>2. First Amendment issues wherein law enforcement is monitoring free speech.</li> </ol>
<p>AUTOMATIC LICENSE PLATE READERS</p>	<ol style="list-style-type: none"> <li>1. LPRs may chill privacy protections by collecting information, including patterns, when a vehicle is near sensitive places such as immigrant centers, hospitals, or the sites of religious activities or protests.</li> <li>2. Law enforcement agencies retain LPR information on vehicles for long periods, even when drivers have broken no law, and/or long after the information is needed.</li> </ol>
<p>BODY-WORN CAMERAS (BWCs)</p>	<ol style="list-style-type: none"> <li>1. BWCs can be used to surveil people where a third party might not realize he/she is being video recorded.</li> <li>2. Videos may record in a person’s home or office, potentially violating a reasonable expectation of privacy.</li> </ol>

TABLE 4-2: INFORMATION COLLECTION TECHNOLOGY AND LEGAL/ETHICAL ISSUES (CONTINUED)

DNA FROM COMMERCIAL BUSINESSES	Permitting law enforcement to have access to a person’s DNA for use in a criminal investigation, when the DNA was submitted for explicit personal analysis, may violate the person’s Fourth Amendment rights.
CELL-SITE SIMULATORS	The use of an artificial cell-tower signal explicitly to conduct a general search by activating cell phone information and capturing the information on a police-operated device is argued to be a Fourth Amendment violation.
DRONES/UNMANNED AERIAL VEHICLES	Drones have the capability to provide detailed video and images, including infrared, and be integrated with other technologies such as facial recognition to provide detailed, often surreptitious, personal information about people that potentially violates their privacy.
SMARTPHONES	Viewed as a locked digital diary, a smartphone may pose significant—and somewhat unresolved—First, Fourth, and Fifth Amendment issues. If a person is forced to unlock a smartphone and incriminating information is found, is this a violation of the Fifth Amendment? Is the forced unlocking of a smartphone a Fourth Amendment violation?
SURVEILLANCE AND SECURITY CAMERAS	Concerns are about unrestricted police access to private surveillance camera video and images that are operated in private facilities for purposes of security. It is argued that this violates a reasonable expectation of privacy.
FACIAL RECOGNITION	Critics argue that the technology is error-prone and is particularly inaccurate regarding racial and ethnic minorities, leading to misidentification and false implications in crimes.
TATTOO RECOGNITION	Because tattoos express many beliefs—including religious and political beliefs—and the comparative technology is not yet validated, the technology is argued to violate the First and Fourth Amendments.

EXAMPLE OF A THREAT POSTED ON A MAINSTREAM GAMING WEBSITE

A criminal complaint states that Farca, using the handle “Adolf Hitler (((6million))),” repeatedly posted online threats against “high value” Jewish targets and police officers, praised Christchurch mosque shooter Brenton Tarrant as a “hero,” and boasted of violent plans: “Wanna see a mass shooting with a body count of over 30 subhumans?” The platform hosting these threats: Steam, the leading storefront and social platform for PC games. Steam, the largest and most important online store for PC gamers, with more than \$4 billion in revenue in 2017, has recently gained popularity among white supremacists for being a platform, such as Gab and Telegram, where they can openly express their ideology and calls for violence. The difference between Steam and social media platforms such as Telegram or Gab is that while the latter do not share a formal business relationship with the wider social media industry, Steam has direct and lucrative relationships with most major game companies, including 2K, Electronic Arts, Xbox Game Studios, Ubisoft, and others. Many of these game companies have made public statements about and dedicated significant resources towards keeping their products safe from the kinds of hateful ideologies espoused by extremists— while continuing to work with Steam.

This is Not a Game: How the Gaming Website ‘Steam’ Harbors Extremists *Anti-Defamation League* (2020). <https://www.adl.org/steamextremism>

and criminal history information.<sup>300</sup> Mobile fingerprint identification, rapid DNA,<sup>301</sup> advanced fingerprint identification technology, and facial recognition all are methods to help law enforcement more quickly identify offenders, victims, and witnesses as a result of emerging technologies.

## SOCIAL MEDIA

Social media is far-reaching—a truly global phenomenon—and evolving as new technologies and applications (software) are created. It can be defined as a collective of software applications and online platforms intended to provide information, human interaction, and communication and to broadly share content in any media form (i.e., written, graphic, audio, and video). It can include social networking, social bookmarking (i.e., tagging), social curation (sharing and marketing), providing forums to discuss virtually any issue or topic, and microblogging. These unique characteristics of social media mean it has been adopted with equal vigor by individuals, organizations, movements, ideologies, businesses, and virtually any other global entity that wants to share and consume information. Different types of social media tend to have different types of content, yet most overlap. While social media platforms can be classified in a number of ways, the following categories fit well within the current discussion of intelligence but are not meant to be fully comprehensive (for example, there are also “economy-sharing social networks” such as Airbnb and Rover which, except for unusual situations, would have little value to the intelligence process). Categories with primary law enforcement intelligence implications include the following:

- ◆ Social networking (e.g., Facebook, LinkedIn, Google+)
- ◆ Microblogging (e.g., Twitter, Tumblr)
- ◆ Photo sharing (e.g., Instagram, Snapchat, Pinterest)
- ◆ Video sharing (e.g., YouTube, Facebook Live, Periscope, Vimeo)
- ◆ Discussion sites (e.g., Reddit, Quora)
- ◆ Blogs and vlogs (e.g., Mashable, Fark)
- ◆ Messaging (e.g., WhatsApp, Telegram)

From a law enforcement perspective, there are two fundamental, but somewhat divergent, roles social media plays: (1) as a law enforcement communications tool and (2) as an information collection resource.

**Social media as a communications tool.** Law enforcement agencies have been increasingly using social media to provide direct information to the community quickly about crime, threats, community safety issues, public safety information, and information that may help develop police-community relationships. From an intelligence perspective, communicating to the public to solicit information on suspicious activity and notifying the public when explicit types of information are being sought can both have value. While many agencies have sites where suspicious activities can be reported, social media also permits police agencies to be *proactive* in soliciting information rather than simply waiting for a member of the public to see an object or behavior and report it (i.e., “If You See Something, Say Something®”). While this is valuable, it is also reactive. However, tweeting the description of a person or a vehicle or describing types of behaviors, all related to a specific inquiry or threat, is a *proactive* action that can be a useful information collection technique.

Importantly, managing an effective police social media strategy is not simply an “add-on” assignment. Performed correctly, it is labor-intensive and requires constant attention to trends, issues, and details. Hence, it requires an investment by the agency, particularly with personnel trained in managing a social media initiative. Model policies,

---

300 <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>

301 <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna>

tutorials, and applications of social media can be found at the International Association of Chiefs of Police Center for Social Media.<sup>302</sup>

**Social media as a tool to monitor threats, trends, and patterns.** Social media has become such a pervasive force in current global culture that the lawful search of social media platforms should be standard practice in any type of threat assessment and many investigations. In most cases, social media provides indicators of trends, potential targets, and potential offenders. In some cases, social media posts provide direct evidence of criminality. In virtually all cases, privacy remains a constant issue. (These issues as applied to social media are discussed in detail in Chapter 7, which deals with civil rights and legal issues.)

While the social media platforms illustrated above are commonly known corporate entities, there are many smaller platforms—some of which are “niche platforms”—that fit into these categories as well. Valuable information for intelligence and investigation can often be found on the corporate sites—but the niche platforms on the deep Web and dark Web<sup>303</sup> may yield even greater information.

Niche platforms focus on singular issues, such as white nationalism, anti-government ideology, methods and tools for cyberfraud, and Incels, to name some examples. Niche platforms have also been on issues that are expressly criminal—for instance, people who are infatuated with violence and seek to commit it, child pornography, and sexual assault. Most require the Tor<sup>304</sup> browser and are difficult to locate and even more difficult to be “added.” When achieved, they have proven to provide significant information for investigations and intelligence.

**Monitoring discussion forums and darknet marketplaces for trends and threats.** For the intelligence process—particularly strategic intelligence—there is value in monitoring information on extremist forums, gang social media, and darknet marketplaces, even if individuals who are potential offenders are not identified. Examining discussions of threat trends, identifying potential conflicts among gangs, or identifying trends of contraband sales on darknet sites all can provide valuable raw information for analysis. The result can be redefined threat pictures and targeted evidence to look for during inquiries. For example, as fentanyl and other synthetic opioids became more plentiful, traffickers of these substances—many of which were from China—reduced the income of heroin traffickers. To make up for market loss, heroin production increased; and the drug was available at lower prices, both on the street and at darknet marketplaces. Observing these trends can provide insights into traffickers, distribution networks, and geographic movement of the changing drug trends. As another illustration, right-wing extremism began to rebrand itself around 2015. The phrases “white supremacy” and “white right” began to be replaced with “white nationalism.” The language of the movement—and even sometimes the appearance of adherents—began to change to make it appear more mainstream. Evidence of these changes can be found by analyzing white nationalist discussion boards and forums. In many cases, to fully understand trends requires an analysis of many posts from multiple social media platforms.

**Evidence of criminality and threats on social media.** There is a broad array of scientific research and anecdotal evidence that social media is used by both criminals and extremists. For example, it is estimated that about 80 percent of street gang members use social media, sometimes posing with weapons or drugs, and often “. . .using online tools to plan crimes, recruit members or challenge and threaten rivals. . ..”<sup>305</sup> Similarly, as the National Consortium for the Study of Terrorism and Responses to Terrorism (START) observed, “. . .evidence suggests that [social media] has contributed to the acceleration of radicalization of U.S. extremists. . ..”<sup>306</sup> As observed by the European Agency for Law Enforcement Cooperation (Europol), darknet markets, also known as crypto markets,

---

302 <http://www.iacpsocialmedia.org/>

303 <https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/>

304 <https://www.torproject.org/>

305 <https://www.govtech.com/public-safety/Most-Gang-Members-Use-Social-Media-Study-Finds.html>

306 [https://www.start.umd.edu/pubs/START\\_PIRUS\\_UseOfSocialMediaByUSExtremists\\_ResearchBrief\\_July2018.pdf](https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf)

“. . .provide a largely anonymous platform for trading in illicit goods and services.”<sup>307</sup> One particularly heinous illustration of criminal evidence on social media was the mosque attacks in Christchurch, New Zealand, detailed in the case illustration below. The significant point is that it is not unusual to find overt evidence of criminality on social media—a valuable source of raw information for the intelligence process.

## CASE ILLUSTRATION—THE SOCIAL MEDIA ASPECT OF THE CHRISTCHURCH, NEW ZEALAND, MOSQUE ATTACKS

Fifty-one people were killed by an attack at two mosques in Christchurch, New Zealand, by a self-avowed white nationalist<sup>308</sup> on March 15, 2019.<sup>309</sup> An unprecedented aspect of these attacks was that the attacker used two social media platforms to further the impact of the attack. One platform was 8chan<sup>310</sup>—an unrestricted message board posting a diverse array of controversial content that is self-described as the “darkest reaches of the Internet.” The other was Facebook, a platform many of us look at every day.

. . .the gunman posted a link on 8chan to the Facebook page where he would live-stream his attack. Posting to 8chan, he wrote: “The Facebook link is below, by the time you read this I should be going live.” He encouraged users to spread his message. Within minutes, users were applauding the gunman [as he killed worshippers in real time] and sharing the link. . . .<sup>311</sup>

According to Facebook, around 200 people watched the attack live. However, the video was shared extensively. According to YouTube,

We’ve removed tens of thousands of videos [of the attack] and terminated hundreds of accounts created to promote or glorify the shooter. The volume of related videos uploaded to YouTube in the first 24 hours was unprecedented both in scale and speed, at times as fast as a new upload every second.<sup>312</sup>

Facebook officials said they took down the original stream after it had been watched about 4,000 times. They also added the video to an internal ban list and began blocking it almost immediately, removing 1.5 million videos of the shooting within the first 24 hours.<sup>313</sup> There is a saying that “What happens on the Internet, stays on the Internet,”<sup>314</sup> meaning that efforts to delete content that has been posted and shared, particularly this extensively, will never be fully successful because it is so easily and quickly reposted and stored.

Among other things, the posting and the video showed the gunman’s commitment to the attack. The video and the posting provide evidence for arrest and prosecution, yet the attacker was unconcerned. Understanding his willing commitment to further the ideology demonstrates the threat such a person represents to society.

Two implications become apparent concerning the attack video. First, it will be used as a motivator to push other white nationalists who have contemplated an attack closer toward that end. Second, it sets a standard that some other extremist—espousing white nationalism or another ideology—will likely want to copy or exceed.

307 <https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy>

308 The attacker wrote a “manifesto” that he posted online to explain his ideology, his rationale, his motivation for the attack, and his vision. It serves as a useful intelligence resource to understand the motives, methods, and targets of the white nationalist ideology.

309 <https://www.nbcnews.com/news/world/new-zealand-mosque-shootings>

310 <https://8ch.net/index.html>

311 <https://news.sky.com/story/what-is-8chan-the-site-used-by-nz-terrorist-to-spread-hate-11666123>

312 <https://twitter.com/YouTubeInsider/status/1107645354361741312>

313 [https://www.washingtonpost.com/technology/2019/03/19/fewer-than-people-watched-new-zealand-massacre-live-hateful-group-helped-it-reach-millions/?utm\\_term=.d263feb18afd](https://www.washingtonpost.com/technology/2019/03/19/fewer-than-people-watched-new-zealand-massacre-live-hateful-group-helped-it-reach-millions/?utm_term=.d263feb18afd)

314 <https://www.digitaltrends.com/computing/what-happens-on-the-internet-stays-on-the-internet/>

Hence, a search for evidence of criminality or criminal extremism<sup>315</sup> on social media can be a very fruitful source. However, there are *caveats* to note:

- ◆ Take steps to ensure that the information is accurate—verify digital facts from independent sources and avoid “fake news” or “fake facts.” Remember, a post may be reposted thousands of times on hundreds of platforms or websites—finding a repost is not independent verification. Sources must be painstakingly checked to independently verify them.
- ◆ Remember, identities can be spoofed.<sup>316</sup> Take steps to ensure that attributions of statements are accurate.
- ◆ Images and video can be manipulated to appear legitimate even though they are not. Do not assume that digital audio and video statements and actions are legitimate—verify them.
- ◆ Research the dates and times of original statements or postings. Information online essentially lasts in perpetuity and can easily be reposted or found in a search. A post on Myspace<sup>317</sup> in 2005 may be found in a Web search but most likely does not have relevance today.

**Privacy and free speech.** The primary concerns in collecting and retaining information from social media for the intelligence process are the issues of privacy<sup>318</sup> and the First Amendment protection of free speech, even if it is hate speech.<sup>319</sup> With respect to technology and the online world, there remains unsettled law that only gets more complicated as technology evolves. Some basic principles provide guidelines:

- ◆ Does a post or statement contain personally identifiable information (PII)? If not, then the information may be safely collected.
- ◆ Is the information or statement posted on an open, publicly accessible discussion forum or a blog? Even with the PII of the writer, if the media is openly available to anyone online, there is no reasonable expectation of privacy; hence information with a criminal nexus could likely be collected.<sup>320</sup>
- ◆ Is the information or statement posted on a forum that requires users to join the forum to see a post? This most likely depends on the requirements and processes for joining the forum. If one simply has to sign up and there is no vetting of persons joining the forum, then there is likely no reasonable expectation of privacy. Vetting of forum applicants can take many forms—answering questions, providing a background, paying a fee, agreeing to forum confidentiality, providing a personal statement of ideological agreement to the forum’s theme, and so forth. The safest avenue is to assume that the more vigorous the vetting, the greater the likelihood that privacy rights attach.
  - To the extent possible, retain copies of forum application statements, logs, and emails, and provide a written statement of efforts to ensure privacy rights and the rationale on which the information was collected and retained. Transparency and evidence that the collection was done in good faith, consistent with known constitutional standards, will strengthen the case for the propriety of the collection and provide support that law enforcement efforts to collect information were not negligent in the protection of civil rights. Apply the rules of collecting physical evidence to digital evidence.
- ◆ If probable cause exists, get a warrant.

315 It has been argued that social media posts suggesting ideological extremism should not be collected and retained by law enforcement unless those posts show evidence of “threat to life.”

316 Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as another source. <https://www.techopedia.com/definition/5398/spoofing>

317 Myspace, <https://myspace.com/>, was at its peak usage from 2005 to 2008. While its use has significantly dwindled, the platform is still live.

318 For a perspective of privacy and the online world, see Kerry. Cameron. F. (2018). *Why Protecting Privacy is a Losing Game—and How to Change the Game*. Washington, DC: Brookings Institution. <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>

319 <https://www.loyola.edu/academics/emerging-media/blog/2016/freedom-of-speech-on-social-media>

320 This is the Third Party Doctrine, discussed in detail in Chapter 7. Also see <https://fas.org/sgp/crs/misc/R43586.pdf>.

The collection of information from social media can be easy and fast. Do not let these factors dissuade you from taking the proper steps to ensure civil rights protections.

## **ANALYSIS OF QUANTITATIVE AND QUALITATIVE RAW INFORMATION, PARTICULARLY WITH ARTIFICIAL INTELLIGENCE (AI) APPLICATIONS**

Intelligence analysts deal with both quantitative and qualitative information. Quantitative refers to information in numerical form—for example, the number of people in a gang, the amount of money made by a criminal enterprise, the number of victims of human trafficking, or the number of victims of a cyberattack. In the case of illegal drug trafficking, these measures may be in quantities of drugs (e.g., weight or number of pills, packets) or in dollar value of the drugs. These are simple illustrations—each of the variables can be broken down into smaller variables and quantified for more detailed analysis. For example, looking at human trafficking victims, we can count males versus females, ages or age groups, countries of origin, locations where the victims have been taken, descriptions of what the victims are forced to do—such as work in the sex trade, domestic services, manufacturing, and so forth. Therefore, quantitative analysis deals with any type of information that can be expressed as a number. It can provide information about patterns and characteristics that can be used to prevent victimization, apprehend offenders, and identify threats. As the number of cases increases, the reliability—or dependability of the analytic outcomes—tends to increase.

Qualitative information is descriptive and not inherently numerical. Analyzing the behaviors of terrorists, analyzing the smuggling methods of human traffickers, understanding the modus operandi—method of operation—of a drug trafficking operation, understanding the factors that make rival gangs enemies, and understanding the ideological factors that drive violent criminal extremists are all illustrations of qualitative information. The analytic output of these data can provide valuable tactical and strategic intelligence as well as identify various indicators of criminal behaviors.

Effective analysis requires the use of the scientific approach to problem solving. Intelligence analysts have used this approach for decades. With the advent of mainframe computing, followed by personal computing, the tools for analysis became not only faster but also more detailed and accurate. The current generation of analytic technology that has important applications for law enforcement intelligence employs artificial intelligence (AI) and machine learning (ML).

AI is essentially the science of training a machine to perform human tasks. In the case of law enforcement intelligence, that includes linking a diverse array of large quantities of information in logical sequences that identifies threats, crimes, trends, and offenders. A machine using ML employs algorithms that look for patterns of data and draws conclusions on how to apply those patterns to AI decision making. The machine is first asked a question on which it collects data and “trains” the AI algorithm. It tests the outcomes, collects feedback on accuracy, and further trains the algorithm based on more data and the feedback. Hence, AI consists of decisions based on the information learned from ML. With large volumes of granular data from diverse sources, AI decision making becomes more accurate, from an intelligence perspective, aiding in the identification of potential threats from any type of crime or from any type of ideologically motivated attack. Moreover, AI can essentially integrate quantitative and qualitative information that will provide a more robust, hence more accurate, analysis.

As an example, a collective analysis of audio and video can be performed using AI. Audio analysis can detect speech patterns and styles that can identify the geographical speech pattern as well as unique characteristics of a given person’s speech that can help identify that person. Video analysis can establish behavioral patterns, biometric analysis of persons in the video—for example, identifying a gait or walking style of a person—and, of course, facial recognition. Video may come from surveillance cameras, smartphones, police officers’ body-worn cameras and dash cameras—virtually any video source. Integrating a large body of qualitative audio and video data into a range

of quantitative variables provides a robust analytic picture of the crimes and offenders in question. These are extraordinarily powerful analytic tools that bring both legal and ethical considerations.<sup>321</sup> Not only can AI identify patterns, it can also identify anomalies, which may themselves be indicators of threats.

As valuable as this technology is, it must be remembered that during the analytic process, there is always room for error. Some error may occur because the data on which AI decisions are made are not sufficiently robust. Other errors may result from the structure of the algorithms. Indeed, critics argue that forecasting algorithms often have implicit bias<sup>322</sup> from the programmers that will cause AI errors (although there is some scientific evidence to suggest this concern is overstated)<sup>323</sup>.

Research in industries from banking to logistics shows that the greatest benefit of AI comes when human workers use technology to “move up the value chain.” For intelligence analysis, leveraging AI to instantly pull otherwise hard-to-spot suspicious activity out of massive and diverse data could allow human analysts to do the higher-value work of determining whether a given suspicious activity represents a valid threat. An important distinction between understanding the analytic role of the analyst and AI is . . .

. . . in understanding the difference between *specialized [intellect]* and *general [intellect]*. Even a simple pocket calculator can outperform the best math whiz at some tasks. But while it is fast and accurate, arithmetic is the only task the pocket calculator can perform. It has a very narrow, specialized [intellect]. Humans, on the other hand, tend to outperform even the most advanced computers in general [intellect].<sup>324</sup>

This means that the analyst interprets and gives context to AI analysis by bringing in a wide array of diverse experiences, knowledge, and judgments. Artificial intelligence makes decisions on how to integrate and organize related data, but it requires a human to draw conclusions about that data.

In the context of these issues, AI is not without its critics, particularly when applied to law enforcement activities.<sup>325</sup> It is essential to develop policies and procedures for the use of AI in the intelligence process to ensure that the information that is captured and retained is not only consistent with constitutional standards, but also the community’s ethical standards. As a result, based on a review of diverse sources for the use of AI in law enforcement, policies for the use of AI should answer several key questions:

- ◆ Is the use of AI done in a manner that protects community members’ privacy, civil rights, and civil liberties?
- ◆ Is information collected using the technology stored and protected in a secure manner?
- ◆ Have efforts been made to ensure that the algorithms of AI and the data on which ML is developed are free of bias and sufficiently inclusive of different races, ethnicities, gender, and age?
- ◆ Has the technology and analysis been demonstrated to be valid, reliable, and fair, free of bias and error?
- ◆ Is the process by which AI is used and applied to law enforcement operations transparent?
- ◆ Is there a system for ongoing evaluation and accountability of AI applications?

---

321 As an illustration of both the analytic power and the use of these tools, see <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.

322 <https://perception.org/research/implicit-bias/>.

323 Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). “Does Predictive Police Lead to Biased Arrests? Results from a Randomized Controlled Trial.” *Statistics and Public Policy*. Vol. 5, No. 1, pp. 1–6. <https://doi.org/10.1080/2330443X.2018.1438940>

324 <https://www2.deloitte.com/us/en/insights/industry/public-sector/artificial-intelligence-impact-on-future-intelligence-analysis.html>

325 For a discussion of the most current civil rights issues, search “AI and ACLU” and “AI and EFF” for current position statements and issues from the American Civil Liberties Union and the Electronic Frontier Foundation, respectively.

Monitoring and documenting AI-related applications in the course of law enforcement actions will help ensure compliance with policy and law while at the same time providing cutting-edge police service.

**Creative analysis through a social intranet.** Staying on the theme of analysis, but moving away from AI, another technological avenue to be considered is development of a social intranet to aid in collective analysis. Social media tools used on the Internet can be built into an agency’s intranet to ask questions and share work-related information. On the intranet, an analyst group—similar to a Facebook group or an internal secure wiki<sup>326</sup>—can share ideas, approaches, and interpretations on different projects, such as cases, threat assessments, or other analytic problems. As another example, an “analysts’ community” on Microsoft Teams can link analysts from different agencies. While not replacing face-to-face communications, use of the intranet permits the sharing of analytic output, images, graphics, videos, resources, and other materials that may help in the collective analysis of an issue.<sup>327</sup>

## TECHNOLOGY FOR INFORMATION AND INTELLIGENCE SHARING/ DISSEMINATION

The value of the intelligence process is to develop products<sup>328</sup> that can be shared with those in the field who have the right to know and the need to know the information. Sharing can obviously be enhanced by technological means in diverse—even creative—ways compared with past methods.

Because of the developments in memory, software design, processing times, and wireless communications, intelligence products can take on new designs with relative ease. For example, images, audio, and video products can provide more illustrative means to share analytic results. Even animation to demonstrate suspicious behaviors, indicators, or crime modus operandi can be used effectively to share intelligence.

Part of the information sharing process may require rethinking how and to whom the information is shared. For example, under current practice, intelligence products are generally widely shared among law enforcement personnel, often through email. Too frequently, however, recipients state they are overwhelmed with reports and do not read them all. Technology can help—but is only one part of the system—to get information into the hands of those who need it and avoid sending unnecessary information to other users. Some factors to consider are the following:

- ◆ Should new intelligence products be developed and placed in different formats?
- ◆ Can we define “communities of interest” among intelligence consumers to target the dissemination of intelligence products for those who need the information? For example, human trafficking investigators do not need intelligence products about street gangs. Moreover, such pushed intelligence products may need to be stratified. As an example, investigators working criminal extremist cases typically do not need intelligence products on drug trafficking patterns, unless there is evidence that an extremist is involved in drug trafficking—such information could be selectively shared to the investigators or analysts working those relevant cases. (AI can make these distinctions to push the intelligence products to those who need the information.)
- ◆ Under what circumstances may a law enforcement user be subscribed and unsubscribed to a community of interest?
- ◆ What structure of intelligence product—including length, detail, and format—best meets the need of each community of interest member?
- ◆ Should intelligence products regularly include “for more information” links to intranet resources?

---

326 [http://wikieducator.org/images/3/34/Newbie\\_Tut1.pdf](http://wikieducator.org/images/3/34/Newbie_Tut1.pdf)

327 For more detailed information, see *The Social Intranet: Insights on Managing and Sharing Knowledge Internally* at <http://businessofgovernment.org/sites/default/files/The%20Social%20Intranet.pdf>.

328 Intelligence products are discussed and described in detail in Chapter 11.

- ◆ Should intelligence products be electronically monitored to determine whether they are opened, when they are opened, and the length of time the product is open, all as measures for evaluation of the products?
- ◆ Should the forwarding of intelligence products be encouraged, prohibited, or controlled, depending on the nature of the product? Should digital monitoring be in place to track forwarded products?
- ◆ Should all intelligence products be pushed to users when the products are available or a notice sent to users to access new products? Should this vary depending on the nature of the product and the user?
- ◆ When individuals use their personal smartphones for work, should intelligence products be pushed to those devices?

Given the types of technology currently available for information sharing, law enforcement is using relatively simple and inefficient methods. If products and dissemination methods are refined, the value and utility of intelligence products can be significantly increased.

## ACCOUNTABILITY OF THE INTELLIGENCE PROCESS

In previous years, law enforcement intelligence violated citizens' civil rights by collecting and retaining information on people when there was no criminal nexus.<sup>329</sup> There are many people in the civil rights community who believe these violations continue. Indeed, successful federal civil rights lawsuits have been filed against police departments for the way in which they collected, retained, and managed information in their criminal intelligence records systems. At the heart of those lawsuits was that the police were negligent in the protection of citizens' civil rights. To avoid negligence and maintain informed control of all criminal intelligence, a law enforcement agency needs to have a process for accountability.

Accountability provides checks and balances to ensure compliance with requirements and standards of police processes; ensure that employees are performing in a manner consistent with policies and procedures; and help employees and organization initiatives stay on task with goals, objectives, and responsibilities. For example, to ensure that the intelligence process is following the law and guidelines to protect citizens' privacy, civil rights, and civil liberties, there must be an accountability mechanism to monitor information collected, retention requirements, information sharing, and information security. Technology can be a significant factor in monitoring information transactions in the intelligence process. Documenting dates and times of information transactions, developing automated audit logs of users and their activities in the system, tagging information to provide review and purge alerts, providing an information entry protocol to ensure that only allowable information is entered into the system, and developing information dissemination logs are all examples of how technology can help with accountability.

## CONCLUSIONS

The amount of technology available to law enforcement is overwhelming in its capabilities, its applications, and its evolution. This chapter was intended to be a primer on technology from the perspective of law enforcement intelligence. It is food for thought with respect to how intelligence may be used and the issues associated with the technology. The acquisition and use of technology are the last steps in a planning process to determine technological needs. The first steps include assessing the propriety of the technology for a specific agency's mission and needs; selecting the technologies that will be adopted; developing guidelines for use, monitoring, and evaluation; and providing training on the proper use of the technology. A solid foundation needs to be laid for technology's most effective and proper use.

---

<sup>329</sup> For a perspective of these concerns, see the discussion and links by the American Civil Liberties Union (ACLU) Spy Files Web page: <https://www.aclu.org/issues/national-security/privacy-and-surveillance/spy-files>.



# CHAPTER 5

## INTELLIGENCE-LED POLICING: HISTORICAL FOUNDATION AND CONCEPT



The International Association of Chiefs of Police intelligence summit in 2002 recommended the adoption of intelligence-led policing (ILP) by America's state, local, and tribal law enforcement agencies in the post-September 11, 2001 (post-9/11), era. Similarly, the *National Criminal Intelligence Sharing Plan* (NCISP) observed:

Our nation's public safety community must be prepared for the threats of today and tomorrow by embracing intelligence-led policing and use the NCISP as the blueprint for our homeland and hometown threat mitigation strategy.<sup>330</sup>

ILP was envisioned as a tool for information sharing to aid law enforcement agencies in identifying threats and developing responses to prevent those threats from reaching fruition in America's communities.<sup>331</sup> This call by the NCISP to adopt ILP has been echoed broadly by law enforcement leaders and reflected in a growing body of research on the success of the concept.

The challenge, however, was that there were differing views of the ILP concept and its application. Indeed, there is a movement toward the adoption of ILP without a universally accepted definition or a manual of practice, although increasingly, there is research providing evidence-based practice of what works.<sup>332</sup> The intent of this discussion is to

<sup>330</sup> NCISP, Version 2.0, (2013). Ibid., p. 13.

<sup>331</sup> <https://www.theiacp.org/sites/default/files/2018-08/CriminalIntelligenceSharingReport.pdf>

<sup>332</sup> For a comprehensive review of the research, see Carter, J. G. (2018). *Bibliography of Intelligence-Led Policing*, Oxford Bibliographies. <https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0250.xml>

provide a perspective of ILP in the context of contemporary developments in law enforcement intelligence, integrating the more commonly accepted applications of ILP with a focus on the processes required to implement the concept.

Implementation of ILP requires a realistic understanding of the current intelligence capacity across the spectrum of American law enforcement and a flexible approach to meet the capabilities and needs of major cities and counties as well as small departments and rural communities.

## CONCEPTUAL FOUNDATIONS

The NCISP states:

...all law enforcement agencies should participate in terrorism and crime prevention activities by establishing an intelligence capability in their operations, partnering with their respective state or major urban area fusion center, adopting intelligence-led policing (ILP) processes, and supporting effective response for disasters and incidents.<sup>333</sup>

How is this accomplished? As noted earlier, there is no manual of practice for ILP because, like community policing, it must be tailored to the characteristics of each individual agency. ILP may be characterized as an underlying philosophy of how intelligence fits into the operations of a law enforcement organization. Rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the organization's overall mission.

Thus, the concept of ILP must be created through an inclusive development process to ensure that it is integrated with an agency's goals and functions, its capabilities, and the characteristics of both the agency and the jurisdiction it serves. It is not an add-on responsibility for the agency but an adaptation to more efficiently and effectively deal with multijurisdictional threats and serious crime that touch communities. There are no shortcuts in the process—it requires creativity, organizational introspection, and a willingness to adapt within the organization. The following discussions provide a framework to understand the diverse aspects of the ILP concept. Building on this understanding, the following chapter discusses the policy and organizational dynamics necessary to effectively implement ILP.

## DEFINING ILP

There is no universally accepted definition of ILP, although the components of most definitions are the same, or at least similar. In an unpublished 2007 document titled "Intelligence-Led Policing and the Bureau of Justice Assistance" (BJA), which was produced to guide the solicitation and review of violence reduction grants using ILP processes, the conceptual foundation of ILP was articulated as building on the lessons of problem-oriented policing and CompStat and applying these principles to a threat-based environment of multijurisdictional complex criminality. The conceptual foundation embraces recent initiatives in law enforcement intelligence, ranging from the operation of the Regional Information Sharing Systems (RISS) to the products of the Global Justice Information Sharing Initiative (Global) to the development of the National Information Exchange Model (NIEM).

In the document, BJA states:

ILP can be defined as a collaborative law enforcement approach combining problem-solving policing, information sharing and police accountability, with enhanced intelligence operations.

---

333 NCISP, Version 2.0. (2013). Ibid. p. 23.

Another definition, developed by a BJA working group, defined ILP as:

Executive implementation of the intelligence cycle to support proactive decision making for resource allocation and crime prevention.<sup>334</sup>

Building on these foundations, this author proposes an operational definition of ILP as:

The collection and analysis of information related to crime and conditions that contribute to crime, resulting in an actionable intelligence product intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats.

Breaking the definition down into its critical components will provide better understanding.

**Collection.** An essential part of the intelligence process is collecting raw information that may be used in the analysis. Collection should be focused to identify and understand threats that emerge within a jurisdiction. This focus is often determined by an analyst, who will define intelligence requirements and be based on information received from officers, confidential sources, and community members in the form of tips, leads, and suspicious activity reports (SARs). The key point is that collection seeks raw information within defined parameters that is essential for effective analysis. Ideally, law enforcement leadership would set the tone for collection through their planning and direction.

**Analysis.** As noted in Chapter 3, analysis is the scientific approach to problem solving. It relies on deductive and inductive reasoning to define requirements and forecast threats. Analysis may be quantitative, notably for strategic analysis, but it is frequently qualitative (for both tactical and strategic analysis). The Office of the Director of National Intelligence (the ODNI) has stated that analysis is “a process in the production of intelligence in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions.”<sup>335</sup> The ODNI goes on to make the following distinctions between raw information and analyzed information (i.e., intelligence):

- ◆ Raw information:
  - Provides input
  - Builds awareness
- ◆ Analyzed information (intelligence):
  - Provides understanding
  - Reduces uncertainty
  - Enables better decisions

The analytic process is synergistic, providing integrated meaning and deriving knowledge from diverse raw facts. Moreover, analysis is used to define “intelligence gaps” and articulate requirements.

**Crime and conditions that contribute to crime.** Since ILP focuses on threats, it becomes essential to identify variables within a community and the surrounding region that support the generation and maturation of crime. These can be wide-ranging, including, for example, the emergence of organized criminal elements within the region who traffic in people, drugs, or guns; the emergence of an extremist group that articulates hate or violence; evidence of growing violence and crimes associated with gang activity; and a variety of unique characteristics that are idiosyncratic to a given community, such as proximity to an international border. It is important that the information collected provide insight on the existence of the conditions, factors that will exacerbate the conditions, and individuals who may be instrumental in exploiting the conditions to commit terrorism or crime.

---

334 The author was part of this working group; however, at this writing, no publication has been developed using this definition for a citation.

335 Ramsey, T. (May 9, 2007). *Global Maritime Intelligence Integration (GMII) Enterprise*. PowerPoint Presentation. Washington, DC: Office of the Director of National Intelligence.

**Actionable intelligence.** Paraphrasing former FBI Executive Assistant Director for Intelligence Maureen Baginski, intelligence helps law enforcement officers make decisions. Essentially, for intelligence to be useful it must provide direction to develop and execute plans. A law enforcement agency must be able to take an intelligence product and implement some type of activity that will prevent or mitigate crime. This means that the intelligence produced by an analyst will drive operational responses and strategic planning for threats.

With actionable intelligence, a law enforcement agency has sufficient information to develop preventive interventions to threats. The product may describe either imminent threats to a community or region, wanted persons who may pose threats, or threat methodologies about which law enforcement officers should be aware. The basic premise is this: The agency must be able to use the information in some manner. Moreover, actionable intelligence should ensure that the right information is placed in the hands of the people who can do something about the threat.

**Tactical responses to threats.** Both tactical and strategic intelligence are extensions of actionable intelligence. Depending on the nature of the threat, a wide array of tactical responses may be deemed appropriate, ranging from increasing mass transit security procedures to being aware of suspicious activities at a potential intelligence target. Tactical intelligence is all about prevention: using information related to terrorism and crime threats for strategies that will eliminate or mitigate short-term and immediate threats. Tactical intelligence is epitomized by the question, What type of operational response can be developed using this intelligence?

**Strategic planning related to emerging or changing threats.** Threats within a community typically change over time. Strategic analysis is used primarily for planning and resource allocation to understand the changing nature of the threat environment. Information is provided to decision makers about the changing nature, characteristics, and methodologies of threats and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources. For example, if a community has never had a problem with right-to-life extremists and a new clinic opens providing abortion procedures, a strategic analysis may provide insight on whether the clinic and its personnel will be subject to any type of threat by extremist groups.

When strategic analysis is used, plans may be developed to either prevent a threat from maturing or to mitigate the threat should it emerge. It is epitomized by the question, What future plans and resources must be configured, and how must they be configured, to meet threats defined in the strategic analysis?

## FUNDAMENTAL PERSPECTIVES ON THE HISTORY OF ILP: THE BRITISH EXPERIENCE

To refine our vision of ILP, context is needed. The concept of ILP was based on the British experience, which has similarities to U.S. policing but also notable differences, particularly in structure. Specifically, one needs to understand dynamics within the American law enforcement environment that will influence the implementation of ILP as well as limitations to adopting the British National Intelligence Model, as some have proposed, for U.S. law enforcement.

### PERSPECTIVE 1: THE CURRENT STATE OF AMERICAN LAW ENFORCEMENT INTELLIGENCE

Some evidence suggests that ILP can provide an important element to community security to prevent (or at least mitigate) terrorism, violence, criminal extremism, organized crime, and complex criminality. This author agrees. The concern, however, is how ILP is implemented. At one meeting, a strong ILP advocate urged law enforcement leaders to take the Nike® approach and “just do it.” The problem is that many American law enforcement agencies are neither structurally nor substantively ready to support the ILP infrastructure. Just like a building, the foundation must first be in place. Most American law enforcement agencies have gathered some bricks, but they are a long way from completing the foundation.

Over the past 20 years, the author has provided intelligence training to literally thousands of law enforcement personnel, representing hundreds of agencies at all levels of government from every state and most territories.<sup>336</sup> Yet this is still a small proportion of American law enforcement. It has been learned that agencies that have a robust intelligence capacity are the exception, rather than the rule. Moreover, what is commonly called an intelligence unit or an intelligence capacity in most agencies is, in practice, more of a hybrid organizational entity that may be doing crime analysis and/or investigative support. In many cases, the integration of crime analysis and intelligence analysis may not have fully developed either capacity.<sup>337</sup> In other cases, there may be multiple intelligence capacities that are function-specific, such as gang intelligence, drug intelligence, and/or organized crime intelligence. Once again, many of these activities are more akin to investigative support than to intelligence.

Historically, the vast majority of American law enforcement agencies have had little intelligence capacity or training on the intelligence function and processes—they were typically viewed as something needed by the largest agencies, with the remaining agencies having no need for an intelligence capacity. Of those that did have an intelligence capacity, as discussed earlier, the legacy has also been somewhat problematic. While dossier-building practices generally no longer exist, the legacy lives on, with many members of the public remaining suspicious of current law enforcement intelligence activities.

Beyond these issues, the intelligence function was often ill-defined, typically remaining out of the mainstream of state and local law enforcement activities. There were few analysts, and many were poorly trained, often inheriting the title of analyst as a result of longevity, not expertise. Hence, it was often difficult to distinguish what the intelligence unit, as an organizational entity, contributed to the total law enforcement mission. While there were certainly exceptions to this characterization, this was the status quo for most American law enforcement intelligence initiatives. Although this has changed dramatically, history remains a difficult obstacle to overcome.

In the post-9/11 era, this began to change. An increasing number of agencies have some form of intelligence capacity, yet on a comparative basis, the numbers are still small. Moreover, many agencies—even moderate-sized departments—still either do not see the need for an intelligence capacity or feel they cannot justify devoting resources to develop an intelligence capacity because of competing demands, notably increasing violent crime rates and managing calls for service. For a notable number of these agencies, the chief executive—as well as others in the chain of command—is typically relying on historically based assumptions about intelligence and does not understand the rapid evolution and value of the modern law enforcement intelligence function. Considering these factors, there is limited motivation for such agencies to adopt ILP. The issue is not that agencies do not want to participate in fusion centers and the ISE; typically, they do not see the comparative value given other responsibilities.

Based on these issues, an earlier point warrants repeating: Most American law enforcement agencies do not have the foundation to implement ILP. An intelligence foundation must first be constructed.

## **PERSPECTIVE 2: THE BRITISH NATIONAL INTELLIGENCE MODEL AND CHALLENGES IN ADAPTING IT TO U.S. LAW ENFORCEMENT**

When seeking to employ a new concept, we often look to other models to learn what works and adopt (or adapt) that practice. Britain has a longer and more sophisticated legacy in law enforcement intelligence than does the United States. All 43 provincial British constabularies have had some form of fairly long-standing intelligence unit to deal with organized crime, drugs, and other complex crimes unique to their jurisdictions. As an example, many British

---

<sup>336</sup> The author has also provided intelligence training to law enforcement agencies in Europe, Asia, and Australia.

<sup>337</sup> Crime analysis assesses the interactive effects and covariance of explicit variables of crimes that have occurred to determine perpetrator methodologies, with the intent to clear the crimes and prevent future incidents through the apprehension of the perpetrator. Intelligence analysis deals with threats, whether from terrorism, criminal extremism, or organized crime, through the analysis of information that suggests a threat, the identification of intelligence requirements, and the use of both target and vulnerability assessments, with the intent of preventing the threat from reaching fruition.

constabularies have a football intelligence unit to deal with “hooliganism” at soccer matches. At a national level, the National Drugs Intelligence Unit was created in the 1980s to deal with the significant increase in transnational drug trafficking and associated crime (such as money laundering). The unit relied on personnel assigned (i.e., “seconded”) from police forces throughout England and Wales. In 1992, the National Drugs Intelligence Unit was expanded and renamed the National Criminal Intelligence Service (NCIS) to deal with all forms of organized crime. In particular, the NCIS evolved in response to the changing political environment associated with the European Union (EU), where, among other factors, immigration and customs checkpoints were eliminated for persons traveling between the EU member countries. In 2006, a new agency was created, the Serious Organised Crime Agency<sup>338</sup> (SOCA), which integrated the NCIS along with a national investigative body, the National Crime Squad (NCS), and the drug enforcement functions of Her Majesty’s Revenue and Customs (HMRC) Service.<sup>339</sup>

In the 1990s, the British government began implementing a business plan philosophy for all elements of government service. This had two fundamental initiatives: either privatize portions of government service or apply a business model to remaining government services. This move had wide-ranging effects. For example, the British National Rail Service—BritRail—was sold in pieces to various private companies. Similarly, local governments privatized such functions as vehicle maintenance and janitorial service. The national police training function in England and Wales was also changed to a quasi-private organization called CENTREX, which evolved once again (in April 2007) to be part of the National Police Improvement Agency (NPIA). The point is that the mandate to use business processes permeated virtually every aspect of British government, including police agencies.

As part of this movement, in the late 1990s, NCIS, with advice from Her Majesty’s Inspectorate of Constabulary<sup>340</sup> (HMIC), developed the British National Intelligence Model<sup>341</sup> (NIM), which was initially released in 2000 and formally adopted in 2002 as accepted policy by the British Association of Chief Police Officers (ACPO), a national police policymaking body. The NIM followed the government policy of using a business process model to deal with crime control.

The adoption of the NIM by ACPO meant that the chief constables of the 43 provincial police forces in England and Wales agreed to adopt the NIM and adapt it to meet the needs of their policing areas.<sup>342</sup> The intelligence function within the constabularies largely deals with violent crime, football hooliganism, nonserious (local) organized crime, and unique local recurring crime problems.

The British police movement to ILP in accordance with the NIM was not easy. Many did not understand the concept; It required a reallocation of resources and added a significant analytic component to each police force. The NIM was criticized by many as being an esoteric model that created a great deal of data and new processes that were not providing “good value for money.” Its full implementation was much slower than anticipated, and, as one might

---

338 In 2013, SOCA was dissolved, since its responsibilities were merged into the United Kingdom’s (UK) National Crime Agency. <https://nationalcrimeagency.gov.uk/>

339 SOCA was an intelligence-led agency responsible for dealing with major organized crime. The UK Security Service (MI5) is responsible for dealing with threats to UK national security, with the greatest emphasis on terrorism, but also espionage, including domestic intelligence. The Secret Intelligence Service (MI6) is responsible for collecting intelligence outside the UK.

340 The HMIC is an organization in the British Home Office responsible for inspecting British police forces to ensure that they are efficient organizations employing “good practice” and providing “good value for money” in their service.

341 More detail on the National Intelligence Model can be found in the Association of Chief Police Officers (ACPO) document at <https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf>.

342 England and Wales have 43 provincial constabularies, in each of which the chief constable is responsible to the local police authority (somewhat akin to a board of police commissions). The commissioner of the London Metropolitan Police reports to the British Home Secretary and has much broader authority and flexibility. While ACPO policy is not binding on the London Metropolitan Police, it has also adopted the NIM. An additional police service called the City of London Police, the smallest police agency in the UK., is responsible for a small geographic area known as “the square mile,” which largely encompasses the London financial district.

assume, some police forces have embraced the concept much more openly than others, some of which employed the NIM largely in name only.

Despite these problems, there have also been important successes as a result of the NIM. Many lessons learned from the NIM can be adopted in the United States, and there is a unique body of model practices, including analytic models, that are available from the HMIC<sup>343</sup> (of course needing adaptation to the United States). However, American law enforcement agencies have a significantly different experience in law enforcement intelligence that prohibits broadscale adoption of British ILP, with some notable exceptions in the predominantly larger U.S. major cities and counties. Some perspective will provide greater understanding.

As mentioned previously, there are 43 police forces in England and Wales as a result of the amalgamation of many smaller police agencies in the 1960s. The smallest of these constabularies has around 900 sworn constables who police sizeable geographic areas that have both urban and rural characteristics. Most of the agencies have 1,200 to 1,600 sworn personnel. While these constabularies do not comprise a national police force, there are national standards that apply to all agencies for training, promotion, operations, and salary. Indeed, personnel may laterally transfer between the constabularies.

Given the size of these police forces and their reasonable operating budgets,<sup>344</sup> all have the resources to hire analysts and the flexibility to reassign personnel to meet the needs of a comprehensive new initiative such as ILP. This is not meant to infer that the constabularies are flush with money and people; rather, one finds significantly more flexibility, resources, and diverse expertise in large agencies than in the small departments typically found in the United States. Moreover, with its solid history of sophisticated law enforcement intelligence analysis, the British police service was able to adopt the NIM and ILP with greater ease.

## COMPARING U.S. AND UK LAW ENFORCEMENT INTELLIGENCE

Compared with the British police structure, America's roughly 16,000 law enforcement agencies, most of which have ten or fewer sworn officers, have diverse policing standards both between and within states. They often have limited budgets, typically coming from local funds, with some exceptions in the form of short-term federal grants. Federal standards and recommendations are largely unenforceable unless tied explicitly to the special conditions of a grant.

In light of these radical differences and the significantly different history of law enforcement intelligence, when one compares U.S. and UK policing, it is unreasonable to assume that the basic practices of the NIM, as found in the United Kingdom, and, by extension, ILP, can be effectively implemented in the United States on a short-term, wholesale basis. In America, we need to start at a far more basic level. A functional model of ILP must be developed that has both flexibility and applicability to the American law enforcement landscape.

At the outset, ILP should be viewed as a philosophy, not a process. Indeed, American law enforcement agencies should rely on this philosophy to develop new intelligence-based processes that functionally balance each agency's jurisdictions, characteristics, and resources. The lessons learned from community policing can be a valuable guide.

Developing ILP in a law enforcement agency requires two developmental activities. One activity is devising the information collection and analysis framework to identify and manage threats within a jurisdiction, the other to develop the organizational infrastructure to support the ILP initiative. These activities will be discussed in detail in the following chapter.

---

343 Go to the HMIC website at <https://www.justiceinspectorates.gov.uk/hmicfrs/> and search for "intelligence."

344 The national budget, through the Home Office, provides 51 percent of the funding for each of the provincial police forces; 49 percent comes from local funds. This permits the Home Office to exert greater influence for national standards and priorities, although each chief constable retains significant autonomy in practice.

## ILP, COMMUNITY POLICING, PROBLEM SOLVING, AND COMPSTAT

A common concern expressed by police executives is that the shift toward ILP—initially in large part due to increased counterterrorism responsibilities—may require a shift of resources away from community policing. It becomes a question of how community policing and ILP are integrated. As will be seen, there are more commonalities between the two than one may intuitively expect. Indeed, new dimensions of ILP depend on strong community relationships. Crime will continue to be a core responsibility for police agencies, as will the need for community support. Moreover, with increased social tension as a result of growing domestic threats largely due to right-wing extremism and targeted violence, the need is even greater to maintain a close, interactive dialogue between law enforcement and the community.

Many law enforcement officers have developed community policing skills that directly support new ILP responsibilities: The scientific approach to problem solving, environmental scanning, effective communications with the public, fear reduction, and community mobilization to deal with problems are among the important attributes community policing brings to this challenge. The NCISP observed that ILP:

... extends the basic concepts of community policing to include prosecutorial authority, community organizations, and intelligence-led operations. [It] blends the core elements of community policing with the corollary approaches of community prosecution. This new model strives to connect the criminal justice system and the community through seamless communication and partnerships to develop initiatives on a foundation of actionable intelligence.<sup>345</sup>

Furthermore, DHS has noted the importance of community policing in homeland security by observing:

Community engagement and community-oriented policing are related tools that focus on building trust with local communities and engaging with them as partners to develop information-driven community-based solutions to local issues.<sup>346</sup>

These factors are part of the underlying philosophy of how intelligence fits into the operations of a law enforcement organization. As mentioned earlier, rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the organization's overall mission. In many ways, ILP is a new dimension of community policing, building on tactics and methodologies developed during years of community policing experimentation. Some comparisons illustrate this point. Both community policing and ILP rely on:

- ◆ Information management
  - Community policing—Information gained from citizens helps define the parameters of community problems.
  - ILP—Information input is the essential ingredient for intelligence analysis.
- ◆ Two-way communications with the public
  - Community policing—Information is sought *from* the public about offenders. Communicating critical information *to* the public aids in crime prevention and fear reduction.
  - ILP—Communications *from* the public can provide valuable information for the intelligence cycle. When threats are defined with specific information, communicating critical information *to* citizens may help prevent a terrorist attack and, like community policing, reduce fear.

---

345 NCISP, Version 2.0 (2013), p.19.

346 [https://www.dhs.gov/sites/default/files/publications/GCTF%20CVE%20Good%20Practices\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/GCTF%20CVE%20Good%20Practices_1.pdf)

- ◆ Scientific data analysis
  - Community policing—Crime analysis is a critical ingredient in the CompStat<sup>347</sup> process.
  - ILP—Intelligence analysis is the critical ingredient for threat management.
- ◆ Problem solving
  - Community policing—Problem solving is used to reconcile community conditions that are precursors to crime and disorder.
  - ILP—The same process is used for intelligence to reconcile factors related to vulnerable targets and trafficking of illegal commodities.

Community relationships are not just a local law enforcement concern. The FBI has stated:

The better we know our communities, the better we can protect them. The Community Relations Unit at FBI Headquarters and FBI community outreach specialists in field offices across the country create and strengthen relationships locally and nationally with minority groups, religious and civic organizations, schools, non-profits, and other entities. These partnerships have led to a host of crime prevention programs, enabling families to stay safe from fraudsters and cyber predators, businesses to protect themselves from hackers and economic espionage, schools and workplaces to safeguard against violent rampages and illegal drugs, and all citizens to become alert to potential acts of terror and extremism.<sup>348</sup>

These words reflect the operational essence of the interrelationship of law enforcement intelligence and community policing. Like community policing, ILP requires an investment of effort by all components of the organization as well as the community. Gone are the days when intelligence units operated in relative anonymity. Based on the precepts of the ILP philosophy and the standards of the NCISP, law enforcement intelligence is an organization-wide responsibility that relies on a symbiotic relationship with residents.

## COMPARING ILP AND COMPSTAT

The CompStat process, with its origins at the New York Police Department, has been an important tool for law enforcement agencies to effectively deal with crime on a timely basis.<sup>349</sup> The process has been adopted—in varying forms—by many mid-sized and large law enforcement agencies across the United States and several foreign countries with consistent success. There has been a solid foundation of research supporting CompStat as a crime management tool that demonstrates the value of innovative approaches to law enforcement problems.<sup>350</sup>

As law enforcement personnel grapple with understanding ILP, many have suggested that it is the same as CompStat. Certainly, there are important similarities that will help in the adoption of ILP. However, there are also important substantive differences that must be similarly recognized. At the heart of the matter is this fact: CompStat and ILP are different based on many functional variables illustrated in Table 5-1.

As can be seen, ILP is concerned with all crimes and all threats, not just terrorism. However, the nature of crime that ILP focuses on is typically multijurisdictional and often complex criminality, such as criminal enterprises.

The value of CompStat is the identification of the emergence of a significant crime series or serious crime within a jurisdiction (i.e., hot spots), based on a timely analysis of incident reports. The analysis of data captured via crime reporting can provide important information—such as place-based parameters and modus operandi—that can be used to forecast continued criminal incidents in the immediate future; aid in problem-solving; and provide descriptive

<sup>347</sup> For a good contemporary discussion of CompStat, see Shane, Jon. (2004). "CompStat Process." *FBI Law Enforcement Bulletin*. Vol. 73, No. 2. (April). Pp. 12–23.

<sup>348</sup> <https://www.fbi.gov/about/community-outreach>

<sup>349</sup> Police Executive Research Forum. (2013). *COMPSTAT: Its Origin, Evolution and Future in Law Enforcement Agencies*. Washington, DC: Bureau of Justice Assistance. <https://www.bja.gov/Publications/PERF-Compstat.pdf>.

<sup>350</sup> A great deal of research and literature can be found at <https://www.ojp.gov/ncjrs>—use the search utility for "CompStat."

information, such as behaviors, targets, and criminal instruments that operational units may use to apprehend perpetrators, disrupt criminal activity, or alter crime-generating environments.

Conversely, ILP focuses on *threats* rather than crimes that have occurred (although a threat may also include a threat emerging from a crime series, such as a serial murder). The threat information may be derived from suspicious activity reports filed by an officer, tips and leads submitted by community members, significant changes in sociodemographic characteristics within a region, or other indicators (some of which may be collateral crimes) that reasonably suggest the presence or emergence of a serious multijurisdictional crime problem. Rather than analyze information and evidence derived from incident reports, the intelligence analyst must define intelligence requirements consisting of information that the analyst needs to more definitively identify a threat and factors contributing to the threat's evolution.

Similarly, to be effective, both community policing and ILP require feedback on information analysis—whether it is crime analysis or intelligence analysis—so that officers may be consistently informed of potential problems or threats that they may encounter during the course of their shifts.

In this regard, what types of information do street officers need from intelligence units? Ideally, intelligence analysis should address four broad questions:

- ◆ **Who poses threats?** This response identifies and describes people in movements or ideologies who pose threats to community safety.
- ◆ **Who is doing what with whom?** This includes the identities, descriptions, and characteristics of conspirators or people who provide logistics in support of terrorism and criminal enterprises.
- ◆ **What is the modus operandi of the threat?** How does the criminal enterprise operate? What does the terrorist or extremist group typically target, and what are the common methods of attack? How do members of the extremist group typically integrate with the community to minimize the chances of being discovered?
- ◆ **What is needed to catch offenders and prevent crime incidents or trends?** What specific types of information are being sought by intelligence units to aid in the broader threat analysis?

Both CompStat and ILP are prevention-oriented and driven by an information flow coming from the line level upward. Intelligence awareness training for street officers recognizes that officers on patrol have a strong likelihood of observing circumstances and people that may signify a threat or suggest the presence of a criminal enterprise. Patrol officers must be trained<sup>351</sup> to regularly channel such information to the intelligence unit for input into the intelligence cycle for analysis. Like community policing, this requires new responsibilities for patrol officers and organizational flexibility to permit officers to explore new dimensions of crimes and community problems that traditionally have not been part of their responsibilities.

While there are fundamental similarities, the methodology and focus of ILP is notably different from—and more difficult than—CompStat because of the differences in the raw data. Understanding these differences and, more important, the role ILP fulfills, is an important foundation for the following discussions.

---

<sup>351</sup> Training, including line-officer training, is discussed in detail in a later chapter.

FIGURE 5-1: SIMILARITIES OF COMPSTAT AND INTELLIGENCE-LED POLICING

### SIMILARITIES OF COMPSTAT AND INTELLIGENCE-LED POLICING

There are important lessons learned from CompStat that can be applied to ILP

- Both have a goal of prevention
- Commitment to the concept by the chief executive is essential
- Analysis serves as the basis for operational responses
- Processes for constant raw information flow for analysis must be in place
- Community engagement is critical for reporting suspicious activities
- Intervention activities are driven by definable evidence of crime and threats
- Administrative and organizational flexibility are required
- Research and lessons learned serve as the basis for creative intervention
- Managers and supervisors are held demonstrably accountable

While principles and processes are similar, there are also substantive differences

<h3> COMPSTAT</h3> <ul style="list-style-type: none"><li>● Intra-jurisdictional</li><li>● Incident-driven</li><li>● Analysis based on known facts from reported crime data and investigations</li><li>● Focuses on crime sprees and incident trends with intent to apprehend specific offenders</li><li>● Relies on crime mapping; incident analysis; modus operandi analysis</li><li>● Time-sensitive (24-hour feedback/response)</li><li>● Predominant focus on street crime (burglary, robbery, homicide, assault, theft, etc.)</li><li>● Reported criminal incidents drive collection and analytic parameters</li></ul>	<h3> INTELLIGENCE LED POLICING</h3> <ul style="list-style-type: none"><li>● Multijurisdictional</li><li>● Threat-driven</li><li>● Analysis-based tips, leads, suspicious activity reports, and information collection</li><li>● Focuses on root causes and conditions that contribute to serious crime and terrorism</li><li>● Relies on link analysis, commodity flow, transaction analysis, and association analysis</li><li>● Strategic (inherently long-term)</li><li>● Predominant focus on criminal enterprises (terrorism, organized crime, violence, etc.)</li><li>● Intelligence requirements drive collection and analytic parameters</li></ul>
--	--

## ETHICAL ISSUES

Another important characteristic similar to both community policing and ILP is the emphasis on ethical decision making. In community policing, the need for ethical decision making was based on, among other reasons, the need to develop trust between police officers and the community. Without this trust, the public would not provide the critical information needed for crime control. The need for ethical decision making in ILP is similar but goes a step farther. Because of the types of information being collected by law enforcement and the way that information is retained in records, concerns have been expressed that law enforcement may violate citizens' rights in the quest for criminal offenders. Of particular concern is (1) whether law enforcement is infringing on First Amendment-protected expressive activity and (2) whether privacy is being protected during law enforcement information collection. As a result of these concerns, the aura of ethical decision making and the propriety of actions must be unquestioned in the law enforcement intelligence function.

## CIVIL RIGHTS AND ILP

A unique challenge in dealing with ILP is maintaining privacy and protecting individuals' civil rights. CompStat and crime analysis each have an entirely different set of legal rules. Typically, CompStat deals with aggregate data of criminal incidents and the attributes of those incidents. In those types of analysis, individuals are not identified; thus, civil rights do not attach to the data. If the crime analysis focuses on the identification of individuals, identification is a result of evidence obtained during the criminal investigation, leading to probable cause for arrest. The law of criminal evidence and procedure applies to the further collection of evidence, and the information is retained in the law enforcement agency's records management system (RMS), which has rules of wide latitude for keeping information on criminal suspects, witnesses, and victims.

Conversely, as noted previously, ILP deals with threats and conditions that may facilitate the threats. Since the intelligence process identifies individuals and organizations for which there is only a reasonable suspicion that they may take advantage of the conditions to commit criminal acts in the future, the information is classified as criminal intelligence information. As such, this information may only be entered into a separate criminal intelligence records system, not the RMS. Consequently, there must be adherence to the guidelines of 28 CFR Part 23.<sup>352</sup> Failure to do so could open the law enforcement agency to civil liability.<sup>353</sup>

For the current discussion of ILP, the point is simply this: There are significantly different rules for the collection, retention, and dissemination of criminal intelligence information as compared with criminal investigation information. Beyond the information management differences, there are conceivable differences in the method of analysis that is performed when individuals are identified as either intelligence targets or suspects and witnesses. As such, there must be a separate records system and supporting policies developed for ILP as well as training on the proper method of processing information used in ILP.

## PUBLIC EDUCATION

As noted previously, public education is critical for effective ILP. The lessons learned from community policing provide important insights. The public encompasses many different constituent groups, and different public

<sup>352</sup> Technically, 28 CFR Part 23 applies only to federally funded multijurisdictional criminal intelligence records systems operated by state, local, and tribal law enforcement agencies. However, in practice it must be assumed that 28 CFR Part 23 applies to all state, local, and tribal agencies for two reasons: (1) the NCISP recommends that all agencies adopt these guidelines as a national standard of good practice; and (2) precedent in federal civil rights cases suggests that adherence to the federal guidelines can be an affirmative defense should a civil rights case be brought against an agency for the types of information being retained in a criminal intelligence records system.

<sup>353</sup> *Privacy, Civil Rights and Civil Liberties Compliance Verification for the Intelligence Enterprise*. (2010). Washington, DC: Global Justice Information Sharing Initiative. <https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Privacy,%20Civil%20rights,%20and%20Civil%20Liberties%20Compliance.pdf>.

education initiatives need to be provided to each. For example, what does an agency want to accomplish with a public education program: Fear reduction? Development of volunteers for the police department? Resolution of community tensions, such as rumors of crime or threats circulating on social media? Is the goal simply to give citizens information about criminal indicators to aid in prevention? The important point is that specific goals should be related to the public education initiative.

Such a program may also stratify the community to give specific types of information to different targeted audiences. Who in the community should be identified as likely candidates for an education program to support ILP? The business community? Civic and church groups? Graduates of the Citizens Police Academy (CPA)? Non-law-enforcement government employees? Teachers and students? Members of the private business sector? The general community? Demographically defined segments of the community?

Different segments of the community may have different needs. For example, since approximately 85 percent of America’s critical infrastructure is owned by the private sector, a special public education program may focus on threat-related issues for this specifically defined community. Conversely, a completely different kind of public education may be directed toward graduates of the CPA who may be trained to work as volunteers during crises or a heightened alert status. Yet a different public education agenda would be directed toward particular racial, ethnic, or religious communities within a city. Typically, a police department will have somewhat different goals for each segment of the community.

These segments may be further divided, particularly if there are unique targets within the community. For example, the business community may be broken down into different segments: Different threats may target a nuclear plant, a telecommunications switching station (both critical infrastructures), a meat-processing plant, or a university genetic research laboratory (both of which may be targets of domestic environmental extremists).<sup>354</sup> The law enforcement agency will have to conduct a threat assessment to fully understand the character of the threat within the community, as well as to understand the agency’s intelligence requirements. Collectively, these elements have a symbiotic relationship to aid in the development of a public education program.

TABLE 5-1: EXAMPLES OF TOPICS IN A PUBLIC EDUCATION PROGRAM

<ul style="list-style-type: none"> <li>◆ Understanding terrorism</li> <li>◆ What is terrorism (defined/explained)</li> <li>◆ Why people commit terrorist acts</li> <li>◆ Perspectives of terrorism</li> <li>◆ Asymmetric warfare</li> <li>◆ An act of terror is defined by the victim</li> <li>◆ How terrorism can touch your community:               <ul style="list-style-type: none"> <li>• As a target</li> <li>• Logistics and support provided to terrorists</li> <li>• Activities that fund terrorist organizations</li> </ul> </li> <li>◆ New preparedness resources for local emergency services</li> </ul>	<ul style="list-style-type: none"> <li>◆ What is being done at the national level:               <ul style="list-style-type: none"> <li>• National strategies developed</li> <li>• National threat assessment by the FBI</li> <li>• FBI reprioritized and reorganized to aid state and local law enforcement</li> </ul> </li> <li>◆ What is being done at the state and local levels:               <ul style="list-style-type: none"> <li>• Participation in Joint Terrorism Task Forces (JTTFs)</li> <li>• Officers receiving anti-terrorism training (SLATT)</li> <li>• New communications and information sharing (HSIN, RISS, LEO) give local law enforcement more access</li> </ul> </li> </ul>
---	---

<sup>354</sup> Often, targets may not be readily apparent in a community. Does East Lansing, Michigan, appear to be a terrorist target? From the author’s personal experience, in 1992, the Animal Liberation Front (ALF) started a fire in the Michigan State University (MSU) mink research facility and caused more than \$2 million in damages. On December 31, 1999, a fire in MSU’s Agricultural Hall caused \$700,000 in damages and destroyed years of research. Earth Liberation Front (ELF) claimed responsibility, targeting genetic research.

Community education programs should also have a specific intended outcome. Whether it is to reduce fear or to enlist support for volunteer efforts, all public education initiatives should incorporate several factors related to the intelligence function:

- ◆ Know how to observe.
- ◆ Know what is suspicious.
- ◆ Know what to report.
- ◆ Know how to report.
- ◆ Know what happens next.

To maximize the quality and quantity of information provided by the community, law enforcement must provide a framework of knowledge. The more that law enforcement can educate the community, the more robust the feedback from the community.<sup>355</sup> In this regard, Tables 5-1 and 5-2 illustrate a range of items that may be incorporated into a public education program from both a topical and an outcome perspective.

TABLE 5-2: EXAMPLES OF ACTIONS THE PUBLIC CAN TAKE

- |  |   |
|--|---|
| ◆ Keep informed to know what to look for and report to the police <ul style="list-style-type: none"><li>• Law enforcement must be prepared for information sharing with the public</li></ul> | ◆ Information on how to talk/deal with children regarding crime, violence, and terrorism <ul style="list-style-type: none"><li>• As an example, see <a href="https://www.safety.com/crime-prevention-tips-for-kids/">https://www.safety.com/crime-prevention-tips-for-kids/</a></li></ul> |
| ◆ Be aware, yet be fair  | ◆ Information on how to protect the family <a href="http://www.ready.gov">http://www.ready.gov</a>  |
| ◆ Be cognizant of threats, but avoid stereotyping—focus on <i>behaviors</i> , <i>not appearances</i>   | ◆ Know community safety resources   |
| ◆ Be aware of personal safety issues and how to avoid victimization  | ◆ Communications information  |
| ◆ Develop a safety checklist   | ◆ What awareness means  |
|  | ◆ Equipment and resource checklist  |

## COMMUNITY MEMBERS AS LAW ENFORCEMENT VOLUNTEERS

Often, community members ask what they may do to aid in local crime prevention, ranging from burglary to counterterrorism.<sup>356</sup> One important role is serving as a volunteer for the local law enforcement agency. Experience has shown that community volunteers can save an agency money and often provide unique expertise. Money can be saved when citizens are able to perform tasks that would otherwise have to be performed by a law enforcement employee or a contractor.<sup>357</sup>

355 Ideally, a law enforcement agency should be able to provide feedback to citizens about information that has been reported. Many times, this is not feasible in the intelligence environment; however, feedback provided to citizens serves as positive reinforcement.

356 Research shows that local crime concerns often differ from national policy. For example, an increase of burglaries in a neighborhood will increase the fear of crime among residents. Similarly, one homicide in a community that has had no crimes of violence will heighten fear.

357 Dobrin, A. (2017). Volunteer Police: History, Benefits, Costs and Current Descriptions." Security Journal. Vol. 30, No. 3., pp. 717–733.

Obviously, a law enforcement agency needs to develop some means to screen volunteers as well as provide structure for their work agreement and for administrative controls when they are performing activities on behalf of the agency. In this regard, an important resource is Volunteers in Police Service (VIPS).<sup>358</sup> The VIPS website provides a wide array of resources, documents, policies, and tips that can make a law enforcement volunteer program functional and easy to manage.

Volunteers with unique occupational experience may be particularly valuable to the intelligence function. Attorneys, accountants, people with experience in researching land titles, computer scientists, social network analysts, and academic researchers are examples of professional volunteers who could provide important assistance to the intelligence function. (Of course, background checks and nondisclosure agreements must be required of all such volunteers.)

## A QUICK REVIEW OF RELEVANT ILP RESEARCH

In policing, as in other disciplines, we seek to ensure that our programs and initiatives are effective. As such, we rely on evidence-based practices.<sup>359</sup> ILP is one area of intelligence for which a significant amount of research examining different aspects of its operational application has been conducted.<sup>360</sup> While the Intelligence Guide is not intended to provide a comprehensive scientific literature review of ILP, there are some salient findings of interest.

A variety of conceptual models of ILP have been implemented to meet the unique needs of each agency.<sup>361</sup> Frankly, this is to be expected because ILP needs to be tailored to the crime problems in the community, the structure and character of the jurisdiction, and the resources of the agency. Furthermore, research has suggested that a successful application of ILP occurs when it is integrated with community policing and problem solving.<sup>362</sup> As noted previously, both community policing and ILP require an information sharing relationship. Moreover, both ILP and problem solving require objective analysis of data, facts, and circumstances to be effective. Thus, the intersection of community-focused policing efforts and ILP relies on similar information collection and analytic needs as well as effective communications with the public.

While initially this was *assumed* to be true by policymakers and theoreticians, there is now research to empirically support the assumption. Using interviews with varying personnel from a police department, one researcher demonstrated how information generated from community policing practices can be integrated into the analytical process at the heart of ILP and how such analytical products can improve community policing.<sup>363</sup> In another study, a systematic interview protocol was used to gather data from police personnel across a four-year period. Citizens provided information to neighborhood policing teams, and the information was analyzed to develop community intelligence reports to guide police operations. Results indicated improved public confidence in the police and decreased perceptions of community crime and disorder.<sup>364</sup> This is important not only from a crime control perspective, but also for the decreased fear of crime among community members.

---

358 <https://www.theiacp.org/projects/volunteers-in-police-service-vips>

359 For more information on evidence-based practices in policing, see <https://cebcp.org/evidence-based-policing/>.

360 As an example of the breadth of research in ILP, see the Oxford Bibliographies annotated bibliography on ILP at <https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0250.xml>. In addition, a special issue of *Policing: An International Journal*, Vol. 42, Issue 1 (2019) focused exclusively on ILP: <https://www.emerald.com/insight/publication/issn/1363-951X/vol/42/iss/1>.

361 Carter, J. G. 2013. *Intelligence-Led Policing: A Policing Innovation*. El Paso, TX: LFB Scholarly.

362 Clarke, C. 2006. Proactive policing: Standing on the shoulders of community-based policing. *Police Practice and Research*, 7:3–17.

363 Bullock, K. 2013. Community, intelligence-led policing and crime control. *Policing and Society*, 23:125–144.

364 Lowe, T., & Innes, M. 2012. Can we speak in confidence? Community intelligence and neighborhood policing v2.0. *Policing and Society*, 22:295–316.

As has been previously discussed, information sharing is a critical component in successful ILP. Often, information collected by uniformed officers—for example, from field interviews (FI), tips, leads, and suspicious activity reports—is not routinely forwarded to intelligence analysts. Often, it is not seen as a priority in the context of all other patrol officer responsibilities. Officers do not see immediate results, as they do when responding to a call or making an arrest. Yet information collection for the intelligence process can have significant effects on the larger crime picture. In one study, officers were trained to focus on information collection and report to analysts as part of their daily patrol activities. In return, analysts provided intelligence reports for officers to address problems in their patrol areas. This study provides a thorough discussion of program implementation and reports initial results from a pilot precinct. Survey data of officers in this project suggest that the officers supported the ILP program and that officers who more actively shared information reported highest levels of support. This research shows that effective relationships between officers and analysts are a factor for greater success of ILP.<sup>365</sup> (Essentially, the value of officers collecting and sharing this information needs to be marketed to patrol officers.) Building on this, another study found that intelligence training is needed for both officers and analysts to cultivate a more productive working relationship to make ILP an operational success. Primary areas of concern in developing an ILP approach were a lack of understanding of ILP between analysts and officers, their roles in the agency, and their desired inputs and outputs.<sup>366</sup> Hence, training, defining concepts and expectations, and communications with all personnel were found to be essential.

From another perspective, drawing on a national sample of 345 state and local law enforcement agencies, one study reports findings on the types of analytic activities, sources of information, and analyst performance evaluation within police agencies in the United States. The findings show that agencies tended to access more information via databases as compared with receiving information from outside agencies, hence limiting their ability to solve cross-jurisdictional crime problems.<sup>367</sup> The implication is that barriers remain in cross-jurisdictional information sharing, regardless of the demonstrated value. As in the case of patrol officers sharing information with analysts, cross-jurisdictional efforts need to be given higher priority than is currently the case in many agencies.

Examining information sharing from a different perspective, one study explored the level of interaction among state and federal agencies, an aspect of state policing that is heightened under an ILP framework. Their findings suggest that state agencies have increased their level of involvement with federal agencies following the 9/11 terrorist attacks. However, resource allocation to facilitate these activities had no impact on the level of engagement across agencies.<sup>368</sup> While at first blush, these findings may seem counterintuitive, they indicate that policy and training have a more significant impact on information sharing than do resources.

Not surprisingly, concerns consistently arise in the literature about ILP that focus on individual rights, police accountability, ethics, and overall effectiveness.<sup>369</sup> As seen previously, there remains a level of distrust about law enforcement intelligence efforts, largely under the assumption that the police will collect information without regard to civil rights. Public education needs to continue to overcome this perspective.

---

365 Telep, C. W., Read, J., & Bottema, A. J. 2017. Working towards intelligence-led policing: The Phoenix police department intelligence officer program. *Policing: A Journal of Policy and Practice*, <https://www.ojp.gov/ncjrs/virtual-library/abstracts/working-towards-intelligence-led-policing-phoenix-police-department>.

366 Cope, N. 2004. Intelligence led policing or policing led intelligence? Integrating volume crime analysis into policing. *British Journal of Criminology*, 44:188–203.

367 Carter, J. G. (2015). Intelligence analysis within U.S. law enforcement agencies: Empirical insights from a national sample. *Journal of Intelligence Analysis*, 22:1–24.

368 Schaible, L. M., & Sheffield, J. (2012). Intelligence-led policing and change in state law enforcement agencies. *Policing: An International Journal of Police Strategies and Management*, 35: 761–784.

369 Maguire, M. (2010). Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society*, 9:315–336.

In sum, while there is evidence that ILP can successfully reduce crime,<sup>370</sup> some conceptual and pragmatic factors also must be addressed for it to be fully successful.<sup>371</sup>

## CONCLUSIONS

As noted in a publication by the Office of Community Oriented Police Services,

For the past 20 years, community policing has encouraged law enforcement to partner with the community to proactively identify potential threats and create a climate of safety. Its emphasis on problem-solving has led to more effective means of addressing crime and social disorder problems. In the 21st Century the community policing philosophy is well positioned to take a central role in preventing and responding to terrorism and in efforts to reduce citizen fear.<sup>372</sup>

Prudent executives will explore these avenues as part of a comprehensive, communitywide security strategy. Because of the concern for targeted violence, criminal extremism, and threats from gangs and criminal enterprises, the need to embrace all elements of the community becomes an even higher priority.

---

370 Heaton, R. (2010). The prospects for intelligence-led policing: Some historical and quantitative considerations. *Policing and Society*, 9:337–355.

371 James, A. (2014). *Examining Intelligence-Led Policing: Developments in Research, Policy and Practice*. Basingstoke, Hampshire, England, UK: Palgrave MacMillan.

372 Scheider, M., Chapman, R., & Seelman, M. (2004). "Connecting the Dots for a Proactive Approach." *Border and Transportation Security*. Washington, DC: Office of Community Oriented Policing Services. <https://cops.usdoj.gov/RIC/Publications/cops-w0245-pub.pdf>.



# CHAPTER 6

## DEVELOPING AND IMPLEMENTING INTELLIGENCE-LED POLICING



The previous chapter established the concept and issues associated with intelligence-led policing (ILP). Building on those concepts, this chapter will identify the processes and elements required to implement ILP in a state, local, or tribal law enforcement (SLTLE) agency. Because of the conceptual nature of ILP, it must be designed to meet the explicit needs of a given agency. This is complicated by the fact that a wide range of resource and environmental variables will also influence implementation.

The important point is that there is no single model of ILP that can be plugged into an agency. Rather, as will be seen, there are tools that can be used to identify the intelligence needs of an agency and then craft the policies and processes to make ILP functional for each department.

Essentially, a core responsibility is to effectively manage information—specifically, the information that is needed to identify threats of concern to a community, to include sufficient information about the threats to develop operational responses to prevent or mitigate them. As depicted in Figure 6-1, this is a three-phase process as related to the integration of ILP into a law enforcement organization. The first phase examines the elements necessary for the information management process to be effective—it begins with developing an information management plan. The second

FIGURE 6-1: THREE PHASES OF ILP DEVELOPMENT IN AN SLTLE ORGANIZATION

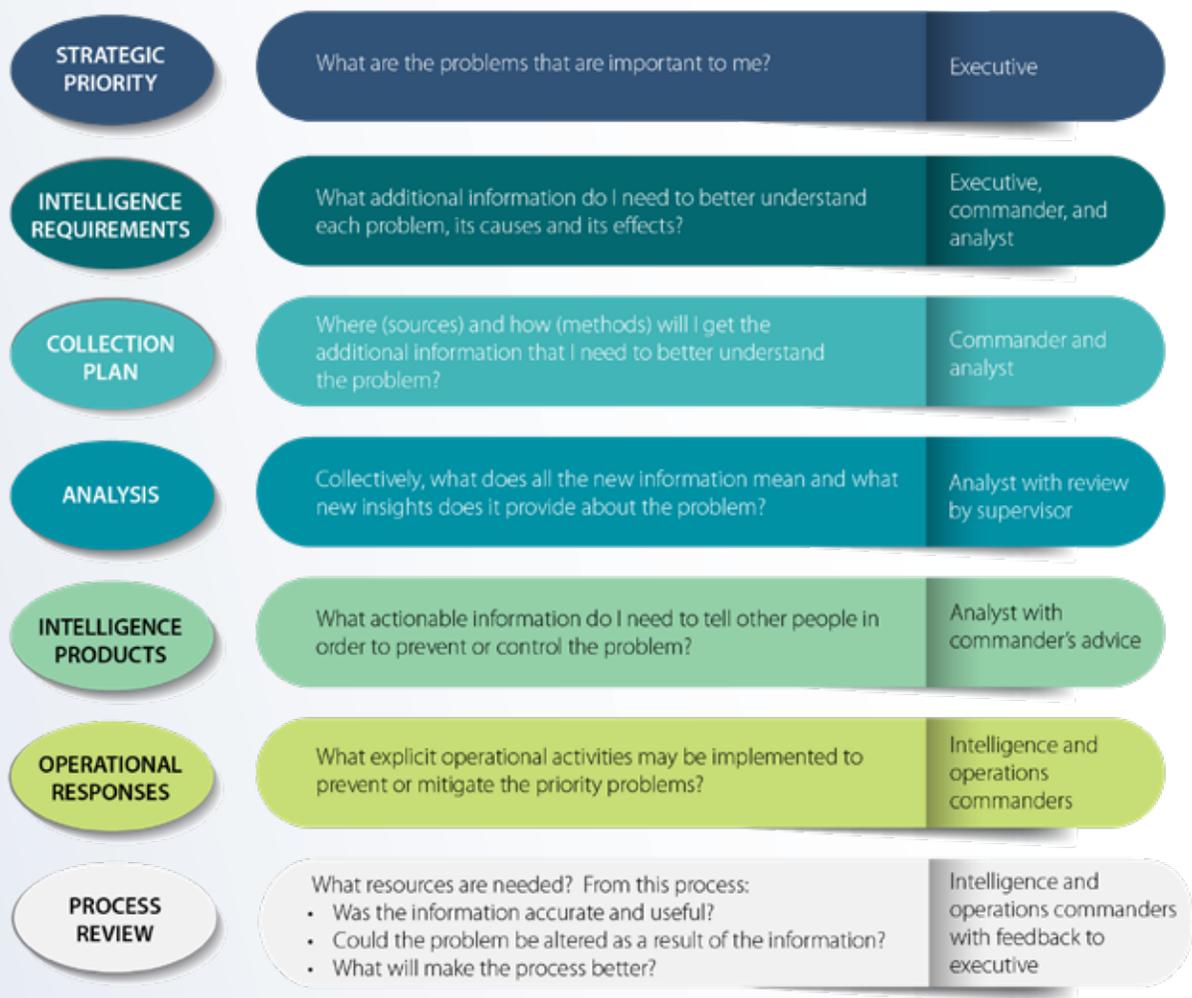


phase is creating the organizational infrastructure to make the information management plan functional. The third phase is implementation. The following discussions address these three phases.

## ESTABLISHING A FRAMEWORK FOR STRATEGIC PRIORITIES AND INFORMATION PROCESSING: THE INFORMATION MANAGEMENT PLAN

The information management framework is a business plan that guides a focused series of processes for the intelligence function. This plan identifies priority problems and institutionalizes a process for monitoring the problems through the application of seven critical components. A rudimentary approach is used in Figure 6-2 to explain each component by indicating the kinds of questions it is intended to answer and the organizational positions most likely to be responsible for answering the questions.

FIGURE 6-2: COMPONENTS OF THE INFORMATION MANAGEMENT PLAN



Integrated within the information management plan is the *intelligence process* (as discussed previously in Chapter 3). The six phases of the intelligence cycle operationalize the acquisition and processing of information needed for the intelligence function. The information management components collectively create the information management plan; the intelligence cycle is the mechanism to ensure that information is collected, assessed, and processed in a manner that is scientific and consistent with accepted practice.

As illustrated in Figure 6-3, the intelligence process is a critically important subsystem for the information management plan. The current discussion, however, focuses on the essential components necessary to develop and implement the plan. It lays the foundation for operationally responding to threats as well as providing a quality control mechanism for both information management and information processing.

## THE INFORMATION MANAGEMENT PLAN

The management plan has seven core components that integrate the intelligence function with all other agency responsibilities. It should be emphasized that these are *management* components, not operational components per se. For example, the analysis component of the management plan focuses on the role analysis plays in information management. Conversely, the analysis phase of the intelligence process is focused on developing intelligence from raw data. The following discussions provide a brief description of each of the plan's components.

FIGURE 6-3: STRUCTURE OF THE INFORMATION MANAGEMENT PLAN



## ESTABLISHING STRATEGIC PRIORITIES FOR INTELLIGENCE-LED POLICING

Intelligence strategic priorities are the articulated criminal and extremist threats that must be monitored and managed by a law enforcement agency, considering the impact these threats have on public safety and security. A strategic priority must be articulated in the context of the local community and the law enforcement agency's intent to manage that priority.

Defining intelligence priorities can become a complex process because law enforcement organizations have a wide range of potential responsibilities ranging from traffic control to counterterrorism. Pragmatically, because of resource limitations, these different responsibilities cannot be treated equally. As a result, each responsibility must be given a priority that will guide the allocation of resources and the amount of organizational effort that will be devoted to addressing the responsibility. The goal is community safety—thus the investment in the priorities is a balance among threat probability, threat severity, and availability of resources to invest.

Even within each responsibility, there will be additional prioritization. To use a familiar example, it is inescapable that virtually every state, local, and tribal law enforcement agency will have a strategic priority related to traffic control. Within the traffic control strategic priority, there will be subprioritizations such as:

1. Traffic accident investigation
2. Driving under the influence enforcement
3. Speed enforcement
4. Vehicle registration and regulatory enforcement
5. Parking enforcement

This does not mean there will be no parking enforcement, but under normal circumstances, parking enforcement may occur only when there is a complaint. Priorities can also change with circumstances. For example, parking enforcement may be given a high priority when vehicles must be moved from an emergency snow route or a hurricane evacuation route because of weather conditions. Thus it is essential that a law enforcement agency identify priorities within a dynamic framework that prescribes the conditions under which priorities will change and how those priorities are to be addressed (for example, during a weather emergency, parking enforcement would be rigorously applied to the emergency traffic routes but little used in commercial loading zones).

Strategic priorities are influenced by the systemic influence of several environmental factors. These include the following:

- ◆ Known public safety threats
- ◆ The seriousness of each known threat
- ◆ Political priorities within a community
- ◆ Resources of the law enforcement agency
- ◆ Expertise of the law enforcement agency
- ◆ Special funding obligations (such as the conditions of a grant award or legislative budget mandates)
- ◆ Obligations in partnership agreements with other law enforcement agencies, public safety agencies, or the private sector
- ◆ Personal/professional priorities/commitments of the law enforcement executive

These are all legitimate factors because their effects on organizational prioritization are a product of an interactive balance among the factors. This process applies throughout the law enforcement organization, including intelligence.

Obviously, there are many different foci that ILP may address, particularly considering the all-crimes, all-threats, all-hazards approach to intelligence. Important information must be gained by executives, both empirically and ideologically, that will help focus the prioritization process. In setting strategic priorities for ILP, the law enforcement executive may seek answers to a variety of questions, such as:

◆ **ILP and the Overall Agency Mission**

- What is the priority of ILP in relation to the mission, responsibilities, and other strategic priorities of the law enforcement agency?
- What proportion of the agency's work force will be *exclusively* dedicated to ILP?
- What facility, equipment, supply, and service needs are required to support the various ILP full-time assignments?
- What are the time/resource requirements to support personnel whose time is partially devoted to ILP (including training)?

◆ **Threat-Related Assessment Factors**

- What known threats to public safety exist within the jurisdiction?
- What threats may emerge?
- What critical infrastructure<sup>373</sup> (CI) is in the jurisdiction?
- What unique characteristics exist within the community that may heighten/aggravate either a criminal or a homeland security threat (for example, proximity to an international border; ports; refineries; a geographic area that is disproportionately susceptible to natural disasters)?
- What unique crime problems in the community need to be addressed (for example, firearms violence; gangs; drug trafficking)?

---

373 <https://www.dhs.gov/cisa/critical-infrastructure-sectors>

#### ◆ Administrative and Environmental Factors

- What political mandates exist as related to real or perceived threats that must be addressed?
- What resources and expertise does the agency have or have access to that will support ILP (for example, analysts; analytic software; fee-based information systems)?
- What intelligence-related agreements has the agency entered into that obligate the agency and its resources (for example, fusion center; JTTF; regional task forces)?
- What obligations does the agency have to focus on specific intelligence-related initiatives, processes, and/or outcomes as a result of grants or special funding (such as a crime control tax or a human trafficking grant)?

#### ◆ Executive Prerogatives

- What personal and/or professional commitments and/or philosophies of the chief executive must be addressed in establishing strategic priorities (e.g., ensuring safety of undocumented residents, addressing the needs of the homeless population)?

The answers to these and other questions unique to the jurisdiction will provide the framework from which strategic priorities for ILP may be articulated and prioritized. The next phase is to operationalize the priorities. For example, assume that a law enforcement agency identified four ILP strategic priorities as:

1. Violent extremism
2. Homeland security
3. Violence by firearms
4. Gangs

Within each of these priorities, a subset of priorities must be operationally defined as they apply to the agency. For example, the FBI defines violent extremism as “encouraging, condoning, justifying, or supporting the commission of a violent act to achieve political, ideological, religious, social, or economic goals.”<sup>374</sup>

While suiting the FBI’s needs, these definitions are not likely to be as useful for a state, local, or tribal law enforcement agency that is defining its strategic priorities. Rather, an agency may use a more simplified definition to meet its needs. For example, the strategic priority of *violent extremism* may be articulated simply as:

- ◆ Violent extremism<sup>375</sup>
  - Individuals directed or inspired by international ideological terrorist groups (such as ISIS or al-Qaeda)
  - Individuals embracing an extremist ideology or belief likely to result in violence (such as white nationalism, ecofascism, or Incels)
  - Individuals who have a motive for mass violence or targeted violence (such the Las Vegas shooter or any of a number of school shootings)
  - Environmental criminal extremists (such as the Earth Liberation Front or Animal Liberation Front)

With respect to the strategic priority of *homeland security*,<sup>376</sup> a state, local, or tribal law enforcement agency should define the priority within the context of unique characteristics of a jurisdiction. For example, the homeland security priority of an agency located near the U.S.–Mexico border may include strategic awareness of tuberculosis; a community where there is a high density of cattle being raised for beef processing may include “mad cow” or hoof-and-mouth disease; an agricultural community that raises crops may focus on the accidental or intentional

<sup>374</sup> <https://cve.fbi.gov/whatis/>

<sup>375</sup> Note that each subcategory specifically includes the conditional modifier of “terrorist” or “criminal.” This is an important factor, since state, local, and tribal law enforcement agencies may collect and retain information that identifies individuals and organizations only where there is a criminal nexus, not just an extreme ideology.

<sup>376</sup> The reader should recall that homeland security intelligence deals with all hazards that have implications for law enforcement public safety and order maintenance functions.

introduction of a communicable crop disease such as “soybean rust.” The significant point is that with the current all-threats and all-hazards approach to homeland security intelligence, there are factors beyond the traditional expertise of law enforcement that need to be explored when identifying threats and hazards, as well as defining strategic priorities for homeland security.

In light of the all-crimes, all-threats, all-hazards approach used in contemporary intelligence activities, the strategic priorities for intelligence will tend to be broader than was historically the case. Strategic priorities for the law enforcement agency will be defined throughout the organization and take many different forms. For ILP, an example of strategic priorities may be listed as illustrated in Table 6-1.

Within the framework of strategic priorities, an assessment must be made of what is already known about the nature of each priority. Gaps in the information are then articulated as intelligence requirements.

## INTELLIGENCE REQUIREMENTS

While the use of intelligence requirements has been a long-standing practice of the Intelligence Community, it is a comparatively new practice for SLTLE. Again, because of jurisdictional differences, requirements have slightly different applications for the law enforcement community.

Information that is *missing* but needed to understand a threat, a target, or a suspect is an intelligence gap. Information that is identified *to fill this gap* is an intelligence requirement. Requirements help law enforcement administrators and commanders make decisions, which vary widely:

- ◆ Determining whether a reasonable suspicion of threat exists
  - Assessing the probability of the threat being carried out
  - Whether to prepare for a new threat if it is low probability—and the potential ramifications
  - Alternatives for preparing for a new threat or hazard
- ◆ What resources to deploy
  - Identifying special equipment or supply needs not currently met by the agency (e.g., infrared drones, hazardous materials [HAZMAT] detectors, fentanyl protective equipment)

TABLE 6-1: EXAMPLE OF ILP STRATEGIC PRIORITIES

The Anytown Police Department’s strategic priorities for intelligence-led policing are as follows:

- ◆ Violent extremism
  - Individuals directed or inspired by international ideological terrorist groups
  - Individuals embracing any extremist ideology or belief likely to result in violence
  - Individuals who have a motive for mass violence
  - Environmental criminal extremists
- ◆ Homeland security
  - Critical Infrastructure (CI)
    - Anytown water treatment plant
    - Anytown Naval Air Station
    - Anytown electrical substation
    - FastCar Assembly Plant of Anytown
    - Anytown grain elevator complex
    - GoodBeef Stockyards and Auction Barn
- ◆ Violence by firearms
  - Homicide by firearm
  - Robbery by firearm
  - Assault by firearm
- ◆ Gangs
  - All criminal gang activity
- ◆ Organized crime activity
  - Loan sharking
  - Protection rackets

- ◆ Determining whether a new target exists within a community
  - Do new police-community relationships need to be made, such as with an immigrant community?
- ◆ Determining whether new partnerships need to be developed to manage a change in the threat picture
  - Will new partners have an associated expense?
  - What types of agreements must be in place for partnerships, and what are the limitations?
- ◆ Determining whether a new expertise needs to be developed to manage a threat
  - Will new expertise be developed in-house, from a partner agency, or as a contract (such as digital forensic analysis)?
- ◆ Identifying new training personnel an agency will need to deal with the changing threat picture
  - Who will need the training in the agency, and how much training is needed to effectively address the threat?
- ◆ What kind of personnel reallocation will be needed and for how long to deal with the threat?

The significant point is that requirements define the types of information that need to be collected to address the strategic priorities. Collecting information to fill the intelligence requirement requires a proactive deployment of resources. These may include open sources (including social media); law enforcement and intelligence information systems; human sources; undercover officers; patrol officers; informants; community partnerships; public-private partnerships; or the use of technical surveillance resources. These are articulated in the collection plan.

## COLLECTION PLAN

The *collection plan* is a systematic procedure for gathering relevant information from all lawful sources that responds to intelligence requirements to produce an intelligence product. Usually, the collection plan includes a specified time frame, although in the case of a standing intelligence requirement, that time frame may be ongoing. The collection plan is related to the strategic priorities via the intelligence requirements by collecting targeted information on threats from both strategic and tactical perspectives. Some factors to be considered in the collection plan include the following:

- ◆ Is the requirement sufficiently clear to locate and identify the specific information that is needed?
- ◆ Have open sources been used as the “source of first resort”?
- ◆ Has any portion of the information already been collected in the form of tips, leads, or suspicious activity reports (SARs)?
- ◆ Are partnerships available that can assist in responding to the intelligence requirement (for example, private sector partnerships, the fusion center, or community partnerships)?
- ◆ What sources will be used to collect the information?
- ◆ If not available from open sources or previously collected information, what method(s) will be used to collect the information?
- ◆ What unique technological methods, if any, are needed to collect the information?
- ◆ Are there legal and/or administrative restrictions on collecting the information?
- ◆ Are explicit legal processes, notifications, or approvals required for the collection of specific types of information?
- ◆ Are extra costs associated with collecting the information? (For example, some technology and social media companies charge a fee for searches and for extracting and providing information.)
- ◆ Can source validity and information reliability be accurately assessed? (If not, other collection sources and methods should be explored.)

Collected information is processed using the constructs of the intelligence cycle. As sufficient valid and reliable information is collected and analyzed, intelligence products are developed that are used to monitor the strategic priorities to determine what, if any, operational responses are needed to address threats in each priority area.

## ANALYSIS

When raw data are collected according to the collection plan, they have little value until they have been analyzed. Relying on the scientific approach to problem solving, logical reasoning, and objective interpretation of data, the analytic process gives an integrated meaning to diverse individual pieces of information. Analysis establishes connections between the different data, causes and effects, and correlations of activities and behaviors. The new knowledge derived from analysis can provide insights on imminent and emerging threats as well as potential intervention methods.

Certainly, a goal of effective analysis is to ensure that the conclusions drawn from the process are actionable. That is, when information from an analysis is given to operational units in a law enforcement agency, there is sufficient detail for operational units to develop specific plans to prevent and/or mitigate threats. This actionable information is presented in a written form known as an intelligence product.

## INTELLIGENCE PRODUCTS

Intelligence products are the types of reports and delivery mechanisms used to convey the findings of the analytic process. Ideally, an intelligence unit or fusion center will establish a menu of products designed to meet the specific needs of its various consumers. The products should have a consistent format and appearance (i.e., a brand) that will aid consumers in selecting the products most applicable to their responsibilities. For example, when a threat is identified and reported, managers will need different types of information than line officers. Situational awareness, a strategic assessment, and tactical indicators all represent intelligence products that have a different focus on the same threat.

Each intelligence unit and fusion center will determine the types of intelligence products it will produce. Importantly, the products are the primary methods the intelligence unit will communicate with its customers. The overall utility of the intelligence unit will be judged by the intelligence products it disseminates. The products must be of sufficient quality, substance, and utility that the agency's operational units are able to develop tactics and strategies to prevent threats from reaching fruition.

Ensuring that these characteristics are embodied in each intelligence product maximizes the utility of the product which, in turn, contributes to public safety and security.

## OPERATIONAL RESPONSES

Identifying threats through the intelligence process is an important ingredient for public safety. However, threat identification is only part of the equation. The critical next element is for operational commanders to develop intervention strategies that will stop or mitigate a threat. Some of the operational responses will be fairly simple, such as providing indicators of the threat so that officers will be aware of them while performing their daily responsibilities. Other interventions may be more sophisticated, such as using suppression tactics (e.g., saturation patrol), proactive intervention (e.g., consistent car stops and field interviews of persons and their associates reasonably believed to part of the threat), target hardening, and community education; developing a task force; and aggressively using traditional investigative tactics that may serve to identify and apprehend offenders. It is important to note that operational units should rely on the intelligence function as a resource when developing intervention strategies. The analyst has the most comprehensive insight about the threat and may provide valuable feedback to operational planning.

Implementing operational responses inevitably requires the expenditure of resources. While resource allocation is part of the operational commander's responsibility in developing intervention methods, the intelligence function can assist in prioritizing and focusing strategies. This can translate into a more efficient use of resources.

## REVIEW OF THE PROCESS

A final step is to conduct a review of the process to establish what intelligence was developed and whether any new gaps have emerged. It should ask such questions as:

- ◆ Was the information/intelligence accurate?
  - Was the threat accurately identified?
  - Was the nature of the threat and its characteristics accurately identified?
- ◆ Was the target accurately identified?
  - Were the vulnerabilities of the target accurately identified?
- ◆ What was learned from victims, witnesses, offenders, and locations?
- ◆ Was there useable information from any technical or surveillance activity?
- ◆ What was learned about intelligence gaps, and is there information that can be collected on a standing basis to avoid future intelligence gaps?
- ◆ Did the threat change after the operational response? If so, what is a probable explanation?
- ◆ Did the operational activity cause displacement, which will, in turn, cause new threats to emerge in a different geographic area?
- ◆ What operational responses were used, and are the threats vulnerable to the same approach in the future?
- ◆ Have new threats been identified, or have new threats emerged?
- ◆ Were partner agencies (including in the private sector) involved in any aspect of the collection or response? If so:
  - What were the benefits of this?
  - What feedback have the partner agencies provided?
  - What feedback have they received?
- ◆ What measures have been put in place to minimize the possibility of the threats arising again?<sup>377</sup>

The review is an important tool for evaluating the information management plan, intelligence process, operational responses, and status of strategic priorities. Indeed, the review can also be critical for defining new intelligence requirements and reordering priorities.

## SUMMARY

As should be evident, the information management plan is like a skeletal structure linking the components. It serves as the framework to make the organizational components functional for ILP.

---

<sup>377</sup> Based on: National Centre for Policing Excellence. (2005). *Guidance on the National Intelligence Model*. London, England, UK: Association of Chief Police Officers, p. 94.

## ORGANIZATIONAL INFRASTRUCTURE FOR ILP

Before the ILP concept can be introduced into a law enforcement agency, a number of components (see Figure 6-4) must be developed, each of which complements the definition of ILP provided in Chapter 5. The complexity and detail of these ingredients vary widely between agencies, depending on such factors as:

- ◆ Size of the agency
- ◆ Resources
- ◆ Demographics of the jurisdiction
- ◆ Character of crime problems in the jurisdiction and region
- ◆ Location of the jurisdiction
- ◆ Character of the jurisdiction (e.g., industrial, commuter population, central city, suburb)
- ◆ Relationship with the community (e.g., supportive, conflictual, large undocumented population)
- ◆ Perspective on intelligence by elected officials and community leaders

An assessment of these variables—many of which will be intuitive to the agency—will help guide the development of each ILP component.

## COMMITMENT

The change to ILP must start with the chief executive. If the leadership of a law enforcement agency does not understand and buy into the concept, it will never be functionally adopted. The law enforcement executive's commitment must be demonstrated through allocation of personnel and resources to both develop and implement the concept. If agency personnel do not believe the leader is committed to the new program, implementation efforts will not be effective.

An excellent example of a leader's demonstration of commitment is seen in the following experience:

When Dr. Gerry Williams was Chief of Police in Aurora, Colorado, in the late 1980s, he decided to implement community policing. There was a great deal of resistance, and he recognized the need to educate Aurora police personnel on the concept. He asked a team from the National Center for Community Policing at Michigan State University to prepare a four-hour awareness program, mandatory for all Aurora police department employees to attend, on the change in policing philosophy. He also asked the team to offer the training at 12 different times throughout the day (over a two-week period) to cover every shift so all personnel would have the opportunity to attend the training on their regularly scheduled shifts. At each of the 12 sessions—whether in the middle of the night or the middle of the day—Chief Williams opened the training by making a firm statement that the movement to community policing was going to be the unquestioned policing philosophy to be used by the Aurora Police Department and that resources would be committed to ensure that the change would take place. Chief Williams then sat down in the middle of the front row, where everyone was certain to see him, and sat through every one of the 12 sessions. It did not take long for the word to spread through the department that “the chief is serious about this” because he set other duties aside to attend all sessions in their entirety. This was an important sign of commitment. Moreover, the chief answered questions during the sessions and interacted with officers on breaks to reinforce his commitment.

Commitment begins with the chief executive's understanding of the concept. In some cases, this has been achieved after the chief executive attended a training program developed exclusively from the executive's perspective (such as the FBI's Law Enforcement Executive Development Seminar). Such a program provides fundamental concepts to show

the value of intelligence, demonstrates how intelligence integrates with the department's overall mission, and permits the chief to interact with others who may not only provide reciprocal support but also may participate in an exchange of ideas on how ILP may be used.

The chief executive also should formally articulate his/her support of the concept in a policy statement. The policy statement provides the organizational parameters of ILP and gives all members of the agency a tangible reference point to understand how ILP is to be implemented and used.

Perhaps the best symbol of commitment is the dedication of resources to ILP. When personnel in the agency are trained, people are assigned to the intelligence function, and funding is dedicated to the development and execution of ILP, this sends a strong message to agency personnel about the executive's commitment.

FIGURE 6-4: COMPONENTS OF ILP



It is also critically important to gain commanders' and managers' commitment to the concept. They are responsible for the actual execution of ILP. Unless commanders and managers have a clear understanding of how ILP can benefit the agency and understand their ILP responsibilities for directing personnel under their command, full implementation will not occur, regardless of the chief executive's support. In all types of organizations, there have been instances in the management process in which middle managers have defeated a new initiative simply by not thoroughly ensuring that personnel under their command perform the duties necessary to make the initiative work. This reflects an old adage in management: "Managers may not be able to turn the water on, but they can easily turn it off."



## KEY TAKEAWAYS

- ◆ The chief executive must understand and support the concept of ILP:
  - How ILP fits into the department's mission
  - Articulated commitment to the concept
- ◆ Commitment of people and resources
  - Training
  - Infrastructure development
- ◆ Commitment must extend throughout the chain of command

## PARTNERSHIPS

Effective ILP requires that a range of partnerships be developed. There are good examples of this in the counterterrorism area (such as the terrorism early warning groups) as well as the precedent established in community policing. The range of partnerships includes the private sector, non-law-enforcement government service, and the community. Each can be an important source of information for the intelligence process. The fundamental rationale for public-private partnerships is based on the fact that the greater the number of people who know what to observe and how to report it to law enforcement, the greater the probability of collecting information that may be used to stop a terrorist attack or a criminal enterprise.

There is a precedent of success for including community members as part of the information collection process, as seen in programs used by the Turkish National Police, the Israeli Police, and the London Metropolitan Police. Each has developed programs aimed at the community to report specific types of information—essentially, intelligence requirements—to the police to aid in terrorism prevention. Certainly, if community partnerships are effective in these diverse cultures, they can be effective in the United States. Moreover, public-private partnerships are a simple extension of many current programs used throughout the United States that deal with crime, ranging from Neighborhood Watch<sup>378</sup> to Volunteers in Police Service<sup>379</sup> (VIPS).

One question that emerges is whether the average community member is interested in participating in ILP programs. A pilot program offered by the Regional Community Policing Institute at Wichita State University extended an open invitation to local residents in Manhattan and in Wichita and Topeka, Kansas, to attend a public awareness session on citizen reporting of suspicious activities possibly related to terrorism. More than 600 people attended these sessions because of their concern about the threat and their desire to contribute to counterterrorism initiatives.

Engaging the community can significantly increase the information collection parameters for the intelligence process. There are several key ways to make these partnerships work effectively for ILP.

1. The law enforcement agency must establish **trusted relationships** with people through local law enforcement officers. Typically, a meet-and-greet alone will not suffice. Information that may be sensitive, confidential, or even fearful may need to be exchanged. As a lesson learned from community policing, the bond of trust established through an ongoing dialogue becomes a critical element.
2. Once trust is established, an **effective means of two-way communication** must be established with each individual. In some cases, this may be technological, such as via email or telephone. In other cases, individuals may feel comfortable sharing the information only on a one-to-one basis with their trusted law enforcement partners.

378 <https://www.nnw.org/start>

379 <https://www.theiacp.org/projects/volunteers-in-police-service-vips>

3. Just as is the case for officers, training—or public awareness—about the **signs and symbols of terrorism and organized crime** is important in helping community partners identify substantive information that needs to be reported. For example, a community partner may see a symbol, tattoo, or foreign word that is symbolic of a terrorist or criminal entity, yet if the partner has not been trained to recognize these symbols, the information will likely go unreported. Similarly, community and private partners should receive information about behaviors that are unusual and that suggest criminality to enhance their specific awareness.<sup>380</sup>
4. Partner training should also include instruction on the **type of information that should be documented** for reporting to law enforcement. While documentation of behaviors, evidence, vehicles, and personal descriptions is second nature to law enforcement officers, it is not a customary practice for non-law-enforcement individuals. Explaining what types of information should be written down—along with dates, times, and locations—is an important element in partner training.
5. The agency should develop a policy and process to **protect the privacy and safety** of community partners. As will be discussed in detail in a subsequent chapter, there should also be a privacy policy to protect business partners' proprietary information that may need to be disclosed during the information sharing process. Partners need to be informed of these policies to reinforce the trusted relationship.

A number of good partnership examples have emerged, notably in larger law enforcement agencies. The New York City Police Department's (NYPD) Shield<sup>381</sup> is a comprehensive information sharing and public information program; the Delaware Information Analysis Center (DIAC)<sup>382</sup> has established formal relationships with non-law-enforcement government organizations and targeted private sector entities for information sharing; and the Nassau County, New York, Police Department created the Security/Police Information Network<sup>383</sup> (SPIN) as a comprehensive public-private information sharing network that is stratified by sectors and divided between vetted and unvetted information sharing partners using email and periodic meetings. There are certainly other examples; however, the point is clear. Partnerships are critical, and there are models to provide guidance. Nevertheless, the partnerships must be established throughout America's communities, not just in major metropolitan areas.

<sup>380</sup> As an example, the U.S. Department of Homeland Security has a public Web page describing the indicators of human trafficking: <https://www.dhs.gov/blue-campaign/indicators-human-trafficking>.

<sup>381</sup> See <https://www.nypdshield.org/public/>.

<sup>382</sup> See <https://dediac.org/default.aspx?AspxAutoDetectCookieSupport=1>.

<sup>383</sup> See <https://www.pdcn.org/143/SPIN>.

## INTERNATIONAL ILLUSTRATIONS OF PARTNERSHIPS

**Israel.** During the height of the al-Aqsa Intifada, the Israeli Police sought alternate methods to gain information about planned terrorist attacks. One technique was to establish community partnership patrols working with the residential Palestinian population in such cities as Tel Aviv and Jerusalem. The Israeli community partnership officers developed trusted, often confidential, relationships with many Palestinian citizens in these cities with the expressed intent to gain information or indicators about possible terrorist attacks. The motives of the Palestinians were quite simple: Many Palestinians who worked and resided in Israeli cities had been victims of terrorist attacks alongside the Israeli victims.

**Turkey.** After a series of terrorist attacks in Istanbul in November 2003, the Turkish National Police (TNP) interviewed captured terrorists to learn how they were recruited into the PKK and Turkish al-Qaeda. It was learned that many were recruited in high school and often initially participated with the group out of social pressure rather than commitment to the group's cause. As a result, the TNP began outreach and education programs in high schools both to dissuade young people from joining these groups as well as to gain information that could be used in the intelligence process.

As may be expected, the development process and expected outputs differ somewhat between community partners and private sector partners.

**Community partnerships.** Just as any other crime or community problem, it is important to enlist the support of the community. In the intelligence arena, however, there are two factors that make community partnerships more challenging. First, the agency is concerned about *threats*, and second, many community members are uncomfortable with the intelligence role in law enforcement. On the issue of threats, it is insufficient to simply tell citizens to be aware of suspicious activities. More guidance is needed. In many instances, citizens have reported something to this effect: “A man who looks like he’s from a Middle-Eastern country is taking a picture of a bridge.” In such cases, whether intentional or not, citizens are often falling prey to a stereotype. Beyond this factor, there is virtually no value in reporting such information alone. Citizens need to be given guidance about looking at *behaviors* that are suspicious and instruction on how to document those behaviors when reporting the information to a law enforcement agency. This reduces the possibility of stereotyping people and provides more valuable information to the law enforcement agency.

With respect to the second issue, some critics have expressed that forming community partnerships for intelligence is akin to turning citizens into informants on their neighbors. This belief goes hand in hand with the belief many people hold that law enforcement agencies are collecting as much information as possible on all citizens—or at least on citizens who do not share “law enforcement beliefs.” For many individuals, there is an assumption that intelligence activities routinely violate citizens’ privacy and civil rights. The challenge is to educate skeptics on the process, and the importance of citizen involvement in ILP, simply because citizens are often in a place to observe suspicious behaviors more often than law enforcement officers. The notion of citizen participation goes back to one of the seven fundamental principles of modern law enforcement, articulated by Sir Robert Peel in developing the London Metropolitan Police in 1829: “The police are the public and the public are the police.”<sup>384</sup>

As noted previously, providing training sessions for citizens can be quite helpful in this process. In a number of communities, both in the United States and abroad, citizen training programs have been used with reasonable degrees of success. The programs should tell citizens (1) what to look for, (2) what types of information they should document, and (3) how to report the information to a law enforcement officer or agency. Giving citizens this kind of information increases efficiency and decreases the possibility of stereotyping.



#### KEY TAKEAWAYS

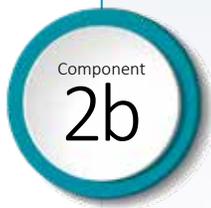
- ◆ Enlist community support:
  - Establish trusted lines of communication with community members.
  - Provide community training so community members will recognize the signs and symbols of terrorism, crime, and other threats facing the community.
  - Tell the community what types of information are needed by the agency.
  - Tell the community how to report information.

**Public-private partnerships.** Public-private partnerships are more structured than community partnerships. While all businesses are subject to partnerships, those that are threat prone (in light of specific threats identified in a region) should be given the highest priority. The private sector has a great deal to offer in information sharing—many have global contacts and communications systems that can also be of value to a law enforcement agency. Whether it is through the assistance of delivery persons who can be alert to suspicious behaviors, security personnel at corporate facilities, or salespersons who can be aware of unusual or suspicious purchases, the value of raw information exchanged with the private sector can be robust.

<sup>384</sup> <https://lawenforcementactionpartnership.org/peel-policing-principles/>

In some cases, a law enforcement agency may develop an intelligence liaison contact with a company. This is an individual who serves as the primary two-way point of contact between the company and the law enforcement agency. Such a partnership will increase the efficiency and effectiveness of the information sharing process. As in the case of community partnerships, the law enforcement agency will need to provide training to appropriate company personnel. In some cases, special training may be provided that is unique to a given corporate sector. This is conceptually similar to the terrorism early warning (TEW) group concept that has been instituted in many communities throughout the United States.<sup>385</sup> Given that law enforcement intelligence focuses on all crimes and all threats, the intelligence liaison contact will be concerned with threats broader than terrorism.

When law enforcement agencies work more closely and have more detailed information exchange with the private sector, two issues of particular importance must be addressed. The first is protection of citizens' privacy. Instances occur in which a citizen's or lawful U.S. resident's identity may be provided to the private sector. For example, this occurs frequently between law enforcement agencies and the airline industry. While there are bona fide reasons for providing information on individuals, care must be taken to (1) ensure accuracy of the information provided and (2) protect the individuals' privacy. The second issue is protecting the proprietary information of companies. In some instances, a company may provide information about its products or business processes to a law enforcement agency as a means to identify and mitigate threats. It is incumbent on law enforcement agencies to ensure that any such proprietary information is protected.



#### KEY TAKEAWAYS

- ◆ Enlist support of the private sector:
  - Give priority to threat-prone sectors, particularly in light of regional threats.
  - Create an intelligence liaison contact.
  - Provide training to recognize the signs and symbols of terrorism, crime, and other threats that may be encountered.
  - Tell the partners the types of information the agency needs.
  - Establish protection of citizens' privacy.
  - Ensure protection of proprietary information.

## INFORMATION SHARING PROCESSES

The heart of effective intelligence is the capture and sharing of critical raw information. Hence, it is logical that each law enforcement agency develop an effective mechanism to record and manage this array of information that is distinct from or segregated from other records in the agency's records management system. This mechanism will have a significantly different structure between law enforcement agencies, typically dependent on an agency's size and resources. Despite these differences, a number of questions must be answered in developing an intelligence or sensitive information records capability within a U.S. law enforcement agency. Among these are:

- ◆ Where and how will this information be stored? It should be noted that there are still agencies in American law enforcement that, because of their small size and rural—sometimes remote—locations, do not have networking capabilities. Some still operate with paper records, photocopies, and faxes.
- ◆ How will SARs, tips, and leads be assessed, managed, and stored?
- ◆ How will source reliability and information validity be evaluated?
- ◆ How will overall information accuracy (including the documentation trail) be ensured?
- ◆ Who has the authority to enter information into the system, and how will entries be audited?
- ◆ How will the information be secured?
- ◆ Who will have access to the information, and under what circumstances is access permitted?

385 Information on the first TEW in Los Angeles can be found at <https://www.hsd.org/?view&did=777733>.

- ◆ Is the records system considered to be for raw information storage or for criminal intelligence records? If the latter, a 28 CFR Part 23-compliant policy should be developed.
- ◆ What are the information sharing rules, and who makes the dissemination decisions?
- ◆ Have policies and procedures been articulated with regard to how and when information will be purged from the criminal intelligence records system?
- ◆ Have adequate measures been taken for security of information?
- ◆ For electronic systems, are data compatibility standards in place? Are data standards consistent with the Global Justice Extensible Markup Language Data Model (GJXDM)<sup>386</sup> and the National Information Exchange Model (NIEM)<sup>387</sup>?

While each of these questions could be discussed at length, for the current discussion it must be recognized that all of these issues must be addressed as part of building an ILP structure. For large agencies, these issues have typically been resolved. However, for the majority of law enforcement agencies, many of which have only a few police officers, this is new ground. Yet if they are expected to collect raw information for the fusion centers and Information Sharing Environment, the questions must be addressed.

Finally, as a result of articulated national standards and precedence in civil law, every agency that develops a criminal intelligence records system should ensure that it meets accepted regulatory and legal standards.



#### KEY TAKEAWAYS

- ◆ Explicit processes and policies must be developed to ensure that the right information is disseminated to the personnel who need it.
  - Ensure that information sharing mechanisms are two-way.
  - Policies must address both intra- and extra-departmental processes.

## OPERATIONAL PLAN

Most law enforcement agencies have an operational plan in place that includes a mission statement, goals, objectives, and a system of directives. Many of these elements apply directly to ILP without any change. For example, standards of personnel conduct or officer safety guidelines apply uniformly. However, elements of a departmental operational plan are typically directed toward criminal investigation and apprehension. Consequently, the ILP operational plan must deal with operational components of managing threats. For example, the goals and objectives of ILP should be clearly articulated. Operational differences between intelligence and investigations should be spelled out, as should the relationship of ILP to the agency's criminal apprehension mission. Even such issues as personnel evaluation will differ in ILP compared with traditional performance measures.

The operational plan is the road map to executing ILP as an agency strategy.

<sup>386</sup> See [https://it.ojp.gov/documents/Global\\_Justice\\_XML\\_Data\\_Model\\_Overview.pdf](https://it.ojp.gov/documents/Global_Justice_XML_Data_Model_Overview.pdf).

<sup>387</sup> See <https://it.ojp.gov/initiatives/niem>.

Component  
**4**

**KEY TAKEAWAYS**

- ◆ The *National Criminal Intelligence Sharing Plan* states, “Our nation’s public safety community must be prepared for the threats of today and tomorrow by embracing intelligence-led policing and use the NCISP as the blueprint for our homeland and hometown threat mitigation strategy.”<sup>388</sup>
  - Each element of the agency’s operational plan should be coordinated to include the ILP mission.
  - An ILP operational plan should also be developed to guide the agency’s intelligence activities.

**ANALYTIC CAPABILITY**

Without analysis, there is no intelligence. However, most American law enforcement agencies are small and do not have an analyst—they simply do not have the budgets. Also, political and collective bargaining implications often need to be addressed if a chief executive explores the hiring of an analyst. On the political side, it is often difficult for lay citizens—including city council members—to understand why funding for an analyst should be allocated in a small law enforcement agency when there is an increase in crime. Unfortunately, in many communities, it would be more difficult to add a police employee who was a nonsworn analyst than to add another sworn officer. Furthermore, in states where there is mandatory collective bargaining, it is difficult to add positions that are law-enforcement-related without either obtaining concessions from the collective bargaining unit or a renegotiated collective bargaining agreement.<sup>389</sup> As a result, for many agencies, other options need to be explored to develop an analytic capability. For example, an agreement with the fusion center, a shared analyst between agencies, the use of volunteer analysts, or the use of college interns as analysts are among the alternatives that may enable an agency to develop an analysis capability. While not perfect, in some cases creative options may be the only recourse.

For example, a fundamental analysis performed by officers may be the only alternative. There is precedent for this, with officers using problem analysis as part of problem-oriented policing. The Center for Problem Oriented Policing<sup>390</sup> has a model POP curriculum available for downloading that can provide instruction on analysis. While not designed for ILP, it can help officers to develop the analytic skills they need for threat analysis.

The point is that rather than relying on intuition, agencies should use an objective assessment of facts to provide a stronger foundation for ILP.

Component  
**5**

**KEY TAKEAWAYS**

- ◆ Analysis is the key to effective intelligence,
  - Of necessity, the analytic capability of agencies varies widely on a continuum ranging from sophisticated to simple.
  - Sometimes, the analytic process is similar to the basic analysis individual officers do in problem-oriented policing.
  - An important element is to develop the analytic mindset.

**TACTICAL AND STRATEGIC RESPONSE ALTERNATIVES**

The distinction between tactical and strategic analysis has been discussed previously. Developing response alternatives to criminal threats represents a different way of thinking about crime. For example, the FBI Counterterrorism Division historically worked cases with the intent of making an arrest as soon as probable cause

388 *National Criminal Intelligence Sharing Plan*, Version 2.0 (2013), p. 13.  
389 The strength of collective bargaining units (CBUs) and the contents of collective bargaining agreements (CBAs) vary widely, even in states with binding arbitration. Accordingly, each CBA must be examined separately.  
390 <https://popcenter.asu.edu/>

was developed. The intelligence-led approach now used in FBI counterterrorism is to gain as much information as possible about all investigative targets rather than making immediate arrests. One approach may be to turn a target to become an informant, permitting the informant to continue to operate. In other cases, a target may remain under constant surveillance, despite the presence of probable cause, so that the agency can identify as many associates as possible, as well as understand the way targets communicate, finance, and generally operate their enterprises, with the goal of disrupting the criminal organization. While many of these targets will eventually be arrested—as is often the case in ILP—arrest is not the only goal. Rather, an important goal is to dismantle the criminal organization to eliminate the threat. As noted by Ratcliffe and Guidetti:

Intelligence-led policing is a conceptual framework for conducting the business of policing. It is not a tactic in the way saturation patrolling is, nor is it a crime reduction strategy in the way situational crime prevention is. Rather, it is a business model and an information-organizing process that allows police agencies to better understand their crime problems and take a measure of the resources available to be able to decide on an enforcement tactic or prevention strategy best designed to control crime.<sup>391</sup>



### KEY TAKEAWAYS

- ◆ Unlike operational activities used to suppress crime or apprehend offenders, new tactics must be used to deal with threats.
  - For example, instead of immediately arresting criminal suspects, an agency may monitor suspects' behavior for further intelligence value.
  - Depending on the nature of threats, creative new initiatives need to be developed to prevent threats; often, this may not involve arrests.

## NEXT STEPS: IMPLEMENTATION

Often, agencies will ask for a template on how to implement ILP. The fact is there is no universal template. Rather, each agency must examine the ILP philosophy and critical components to design an implementation scheme in light of the needs, resources, and articulated goals and tailor the practice of ILP to those requirements. The implementation process is an exercise in organizational change to place the components in action.

## SELF-ASSESSMENT OF AN AGENCY'S INTELLIGENCE CAPACITY

In examining the intelligence capabilities of American law enforcement agencies, the author developed a four-point qualitative scale to describe the intelligence capacity based on policies, expertise, and information sharing capabilities.<sup>392</sup> As illustrated in Figure 6-5, the categories are as follows:

- ◆ No intelligence capacity
- ◆ Basic intelligence capacity for information sharing
- ◆ Advanced intelligence capacity, including an intelligence records system
- ◆ Mature full-service intelligence capacity

While information sharing and connectivity have increased over recent years, most American law enforcement agencies have a minimal intelligence capacity. As such, time and resources—including specialized expertise—are needed to develop the infrastructure and knowledge for a functional intelligence operation within an agency.

391 Ratcliffe, J., & Guidetti, R. (2008), "State police investigative structure and the adoption of intelligence-led policing," *Policing: An International Journal*, Vol. 31, No. 1, pp. 109–128. <https://doi.org/10.1108/13639510810852602>

392 As part of DHS-funded intelligence training programs, the author and his colleagues developed a comprehensive self-assessment tool that measures organizational variables across seven dimensions and provides a refined measurement of a law enforcement agency's ILP capacity. Agencies can have access to this self-assessment at no cost by enrolling in the training.

Resources and external assistance include assistance with policy development, training, access to critical information systems, and other infrastructure components.

The categories describing the intelligence capacity are not dichotomous but exist on a continuum. That is, as illustrated in Figure 6-6, depending on the operational characteristics of the agency's intelligence function, the intelligence capacity will be somewhere on a continuum within that category. As might be expected, the lower on the continuum, the greater the need for external assistance and resources to develop the capacity to a level that is needed for the agency.

FIGURE 6-5: ILP CONTINUUM OF VARIABLES

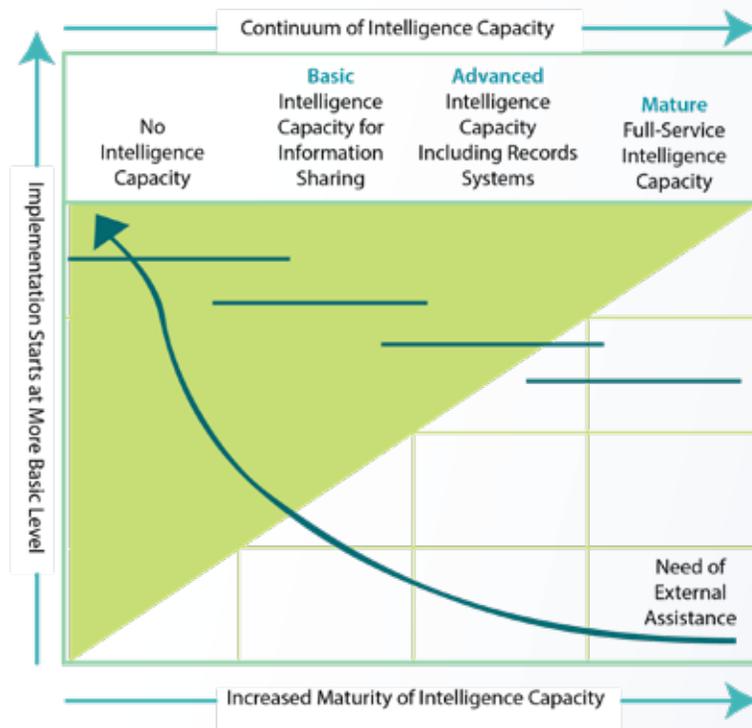
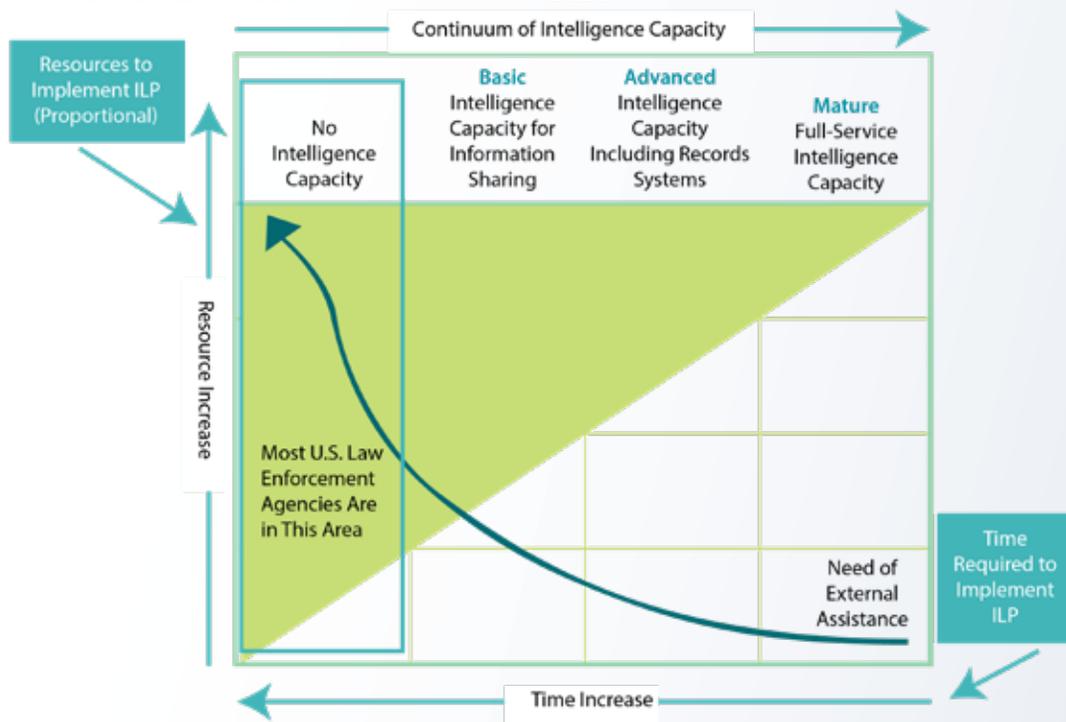


FIGURE 6-6: ILP SUBCONTINUUMS OF VARIABLES



**TABLE 6-2: ORGANIZATIONAL SELF-ASSESSMENT FACTORS OF AN INTELLIGENCE-LED POLICING CAPACITY**

<p><b>No</b> INTELLIGENCE CAPACITY</p>	<p><b>BASIC</b> INTELLIGENCE CAPACITY FOR INFORMATION SHARING</p>	<p><b>ADVANCED</b> INTELLIGENCE CAPACITY INCLUDING INTELLIGENCE RECORDS SYSTEM</p>	<p><b>MATURE,</b> FULL-SERVICE INTELLIGENCE CAPACITY</p>
<p><b>OPERATIONAL CHARACTERISTICS</b></p> <ul style="list-style-type: none"> <li>◆ No systematic intelligence training has been provided to personnel</li> <li>◆ No intelligence policy or procedures</li> <li>◆ No connectivity to intelligence records systems</li> <li>◆ No systematic intelligence initiatives in the agency beyond sharing some intelligence products received from FBI, DHS, fusion center, etc.</li> </ul>	<p><b>OPERATIONAL CHARACTERISTICS</b></p> <ul style="list-style-type: none"> <li>◆ Limited intelligence training, typically an investigator</li> <li>◆ Generic intelligence policy</li> <li>◆ No criminal intelligence records system</li> <li>◆ No or minimal connectivity to intelligence records systems</li> <li>◆ Intelligence activity limited to an individual or two identifying and sharing intelligence products and some BOLOs</li> </ul>	<p><b>OPERATIONAL CHARACTERISTICS</b></p> <ul style="list-style-type: none"> <li>◆ One or two criminal intelligence analysts</li> <li>◆ A formal criminal intelligence records system</li> <li>◆ Connectivity to RISSNET, LEO, and/or LEIU</li> </ul>	<p><b>OPERATIONAL CHARACTERISTICS</b></p> <ul style="list-style-type: none"> <li>◆ Multiple analysts</li> <li>◆ Multisource connectivity</li> <li>◆ Advanced analyst training</li> <li>◆ Comprehensive records system</li> </ul>
<p><b>ACTION STEPS</b></p> <p>Develop intelligence capacity according to NCISP standards</p> <ul style="list-style-type: none"> <li>◆ Awareness training for all agency personnel according to the minimum standards</li> <li>◆ Develop operational plan</li> <li>◆ Establish logistics to receive and store CUI</li> <li>◆ Develop privacy policy</li> <li>◆ Designate intelligence liaison officer for fusion center</li> <li>◆ Establish community partnerships</li> <li>◆ Establish connectivity with RISSNET and/or LEO</li> </ul>	<p><b>ACTION STEPS</b></p> <ul style="list-style-type: none"> <li>◆ Review policies related to intelligence operational plan</li> <li>◆ Awareness training for all agency personnel according to the minimum standards</li> <li>◆ Establish public-private partnerships</li> <li>◆ Establish community partnerships</li> <li>◆ Ensure that CUI meets security standards</li> <li>◆ Ensure that privacy policy is in place or create one</li> <li>◆ Establish an intelligence liaison officer</li> </ul>	<p><b>ACTION STEPS</b></p> <ul style="list-style-type: none"> <li>◆ Ensure that intelligence records are 28 CFR Part 23- compliant</li> <li>◆ Write/review privacy policy for consistency with ISE guidelines</li> <li>◆ Ensure that all officers have received intelligence awareness training</li> <li>◆ Review operational plan according to the NCISP</li> <li>◆ Ensure that analyst training is compliant with the minimum standards</li> <li>◆ Is a fusion center liaison identified?</li> <li>◆ RISS, LEO and LEIU Memberships</li> <li>◆ Community partnerships established</li> <li>◆ Public-private partnerships established</li> </ul>	<p><b>ACTION STEPS</b></p> <ul style="list-style-type: none"> <li>◆ Ensure that all processes are NCISP-compliant</li> <li>◆ Advanced analyst training</li> <li>◆ ILO training program</li> <li>◆ Fusion center liaison</li> <li>◆ RISS, LEO, and LEIU memberships</li> <li>◆ Community partnerships established</li> <li>◆ Public-private partnerships established</li> <li>◆ Review privacy policy with ISE guidelines</li> </ul>
<p><b>Assumption for all four categories:</b> The Criminal Intelligence Coordinating Council standards, guidelines, and promising practices are constantly evolving, and many agencies have not fully addressed them.</p>			

In determining the level of the intelligence capacity and the place to start for developing or reengineering the intelligence function, a law enforcement agency needs to perform a self-assessment of critical variables. Table 6-3 illustrates the operational characteristics that describe each of the four levels. Below each of the operational characteristics are action steps that should be taken to at least maintain the current level or move forward.

Certainly, the operational characteristics and the action steps are not absolutes for determining a law enforcement agency’s intelligence capability. Rather, they represent important milestones that can be identified and assessed in the implementation process.

## THE IMPLEMENTATION STARTING POINT

Any new initiative must have a starting point that provides an accurate picture of an organization's *current state of knowledge and capabilities*. In the United Kingdom, when the National Intelligence Model was introduced to the provincial constabularies, the starting point was fairly unified across all police forces, with a strong foundation, given their history. In the United States, the starting point is at a significantly more fundamental level. To determine this starting point, several questions must be answered in each law enforcement organization:

What is the knowledge level of the chief executive and command staff regarding the current philosophy and practice of law enforcement intelligence, including ILP?

Is there an intelligence unit or intelligence capacity in the law enforcement agency?

- ◆ Does the current intelligence capacity operate in a manner consistent with current practice, including the NCISP and the *Minimum Criminal Intelligence Training Standards*?<sup>393</sup>
- ◆ Has the current intelligence capacity developed a privacy policy?
- ◆ What processes have been addressed and considered in extending the current intelligence capacity to ILP?
  - Is the law enforcement agency accredited by the Commission on Accreditation for Law Enforcement Agencies (CALEA)?
  - If so, what compliance commitments and policies have been put in place to meet the CALEA standard for intelligence?
- ◆ What is the level of general awareness and knowledge of all law enforcement personnel concerning law enforcement intelligence?
- ◆ What internal resources are available to assist in developing and implementing ILP?
- ◆ What external resources are available to assist in developing and implementing ILP?
  - Has the law enforcement agency established any particular relationship and/or processes related to the state or regional fusion centers?
- ◆ Does the agency have someone assigned full- or part-time to a fusion center?
- ◆ Are there any particular obstacles or challenges that must be resolved before implementing ILP?<sup>394</sup>

The intent of these questions is to collectively establish a profile of the law enforcement agency's intelligence capacity, if any, so that the agency has a clear picture of its starting point. This assessment will help guide the agency toward the next step in the implementation process.

As noted previously, a critical tool for socialization is providing *fundamental knowledge to personnel*. The need for training cannot be overemphasized, particularly awareness training for line personnel. New policies and procedures will have little meaning if personnel do not understand the concepts. Once again, the vast majority of America's uniformed law enforcement officers simply are unaware of the intelligence process and their role in it because our pre-9/11 philosophy of intelligence was to have very limited information sharing for operational security purposes. The paradigm has shifted dramatically, and local American law enforcement has a significant learning curve ahead of it.

---

393 [http://www.it.ojp.gov/documents/criminal\\_intel\\_training\\_standards.pdf](http://www.it.ojp.gov/documents/criminal_intel_training_standards.pdf)

394 These can be wide-ranging. For example, some agencies that operate under binding collective bargaining may have to resolve duty changes and training in a new collective bargaining agreement. In some localities, the city council has forbidden a law enforcement agency to develop an intelligence capacity because of privacy and civil rights concerns. In yet other agencies that are operating under an intelligence-related court order or consent decree, changes may need to be made in the order prior to developing and implementing ILP.

When a commitment has been made to implement ILP, clearly one of the top priorities is to provide training at two cognitive levels.<sup>395</sup> The first is awareness, which, in reality, is more like education than training because the intent is to understand the concept of intelligence, how it works, and how it will contribute to the law enforcement mission. The second level is the development of skills and applications of intelligence, such as information collection, reporting processes, and proper intelligence report use. Beyond cognitive-level training, there must be training explicitly directed to the different organizational levels and assignments within an agency that need to have the knowledge and skills to effectively perform in the Information Sharing Environment. The *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies* (minimum standards) provides the critical foundation content that is needed in any of these training initiatives. Moreover, the flexibility inherent in the minimum standards permits each agency to tailor the training program to its particular needs.

Change is a difficult process that most people initially resist. Hence, an early step in the process to introduce ILP is overcoming this resistance or dogmatism. The most effective way to accomplish this is by developing an understanding of ILP and demonstrating the benefits the change will produce for the individual and the organization. In a nutshell, people at all levels of the organization must be sold on the new concept—in this case, ILP. Changing attitudes, values, and beliefs—i.e., *resocializing people*—is a difficult process requiring proactive initiatives, vigilance, patience, and the recognition that some people will never accept the change.

Among the key methods to help the socialization process are demonstrating commitment and allocating resources to ILP.

With the resocialization process under way in a law enforcement agency, an *operational plan* must be developed that articulates the mission and processes of the agency's intelligence capacity. Indeed, the first recommendation of the *National Criminal Intelligence Sharing Plan* addresses the need for an intelligence infrastructure for all American law enforcement agencies "regardless of size."<sup>396</sup> Once again, the operational plan will be unique to each agency. While certain components can be modeled, vast differences among agencies minimize the ability to use a true model operational plan. Instead, assistance should be provided in the process of developing an operational plan that meets the needs and capabilities of each SLT agency.

After training has been provided and the operational plan developed and disseminated throughout the agency, the plan should be *implemented* through a formal notification to all personnel. It should be expected that regardless of the level of planning, there will be some aspects of the plan that simply do not work. The need to obtain *feedback* from personnel to determine what works and what does not is essential. Plans that do not work should not be viewed as failures but as part of the fine-tuning process to make the plan work as effectively as possible.

Finally, an important, yet often overlooked, tool for effective ILP is a performance evaluation system that recognizes and rewards those individuals who are practicing ILP as well as a performance assessment of the entire ILP initiative.

With respect to individual performance assessments, if a traditional evaluation system is in place that is based purely on quantitative variables—number of citations issued, number of reports written, number of arrests made, number of calls answered, and so forth—then the largely qualitative character of individual officers' activities will not be considered in the performance evaluation system. Employees know that organizational success is inextricably tied to the evaluation process. Hence, for success in ILP to be achieved, there must be a personnel assessment system that values the practice.

---

395 Government-sponsored or endorsed intelligence training can be found on the Intelligence Master Training Calendar at <https://mastercalendar.ncirc.gov/>.

396 *National Criminal Intelligence Sharing Plan, Version 2.0* (2013), page vi.

Similarly, the agency's overall success in effectively implementing ILP must be measured. Goals from the operational plan should be stated in a measurable form so that ongoing assessments may adjust the components and modify implementation as necessary to ensure efficient and effective practice of ILP.

## CONCLUSIONS

A theme permeating this discussion is that the introduction of ILP is an exercise in organizational change—a process that is always difficult. While there are important lessons to be learned from the British National Intelligence Model as well as from other countries that have experimented with ILP, such as Australia, American law enforcement agencies have a significantly different experiential and structural demography that prevents comprehensive adoption of the model at this point. Most law enforcement agencies in the United States are just beginning to enter the intelligence arena; therefore, the introduction of ILP must start at a basic level.

In summary, as agencies begin to introduce ILP, there are a number of important lessons from the organizational change process that can help guide this transformation:<sup>397</sup>

- ◆ **There must be a stimulus for change.** There must be a leader with a vision willing to take the first step in challenging the status quo—a change agent. Importantly, this stimulus must be ongoing and widespread. Given this requirement, there are two significant elements that a change agent must address: (1) vigilance in effort and (2) diversity in focus.
- ◆ **There must be administrative commitment.** The effective administrator must provide ongoing support for a new initiative or program; that is, providing consistency between what is said and what is done. If administrators are not willing to try such things as reallocation of resources, amending policies and procedures, or experimentation with new ideas, then there is little reason to believe the sincerity of their pronouncements. If commitment is not shown to either employees or politicians, the probability for success will be significantly reduced.
- ◆ **Any change must be grounded in logical and defensible criteria.** While it is somewhat of a cliché, it is worth noting that changing to simply shake up the organization will be dysfunctional rather than productive. If politicians and employees are going to tie their professional fortunes to change, they must be given good evidence to support the change. Moreover, since change consumes resources, it is wasteful to pursue it unless this change is well grounded in logic and evidence.
- ◆ **People at all levels must be able to provide input.** For a new endeavor, the importance of team building cannot be understated. Any initiative must have participation from as many people as possible. Not only will this diverse input provide new insights, but team building provides ownership and, hence, a sense of investment and responsibility by members of the team.
- ◆ **There must be sufficient time for experimentation, evaluation, and fine-tuning of any new program or idea.** When a new initiative is started, it will inherently have “bugs” in it; not every malady or problem can be anticipated, and some ideas will not work as originally conceived. Just because operational problems arise, it does not mean the idea was bad. Administrators, politicians, and employees must be flexible, adjusting their activities until there has been sufficient time to actually evaluate the initiative's true effects.
- ◆ **Before change is introduced, the plan must be communicated to all persons, and their support must be enlisted.** Politicians, citizens, and employees alike must understand clearly what is being done and why. There is a tendency to assume that everyone knows and understands the issues of a new endeavor to the same extent as those who are immersed in the planning. Lack of communication can destroy a new activity but, fortunately, it is fairly easy to avoid. Remember that communication is more than sending messages; it also

---

397 Modified from Carter, D. L. (2002). *The Police and the Community*. 7th ed. Chapter 9. Upper Saddle River, NJ: Prentice-Hall.

involves gaining feedback from the messages. Be cognizant of the issue, recalling the admonishment, “Don’t leave people in the dark.”

- ◆ **Change takes time in order to have an effect; major change may take a generation.** Americans are generally a short-term, impatient culture. However, when major organizational and behavioral change such as ILP is being implemented, a key ingredient is resocialization of employees, citizens, and political leaders. This is inherently a long-term endeavor that requires patience and stamina before positive results can be seen. This sense of time must be instilled in all involved to minimize frustration and impatience.
- ◆ **Recognize that not everyone will buy in to new ideas.** For virtually any endeavor that is proposed, we must recognize that complete support is improbable; it is the nature of the human psyche to resist change. One must take care, however, to avoid discounting people who oppose new initiatives as being “lost causes” or obstructionists. Listen to their concerns—they may raise some valid issues that need to be addressed. If their ideas are used positively, people who oppose a new initiative may become part of the team. Realism dictates, however, that there will still be those who oppose the new system (frequently for personal reasons). In these cases, an administrator’s options are (1) to continue to try to convince them to change; (2) to ignore or avoid them; (3) to place employees in assignments where they can do little damage; (4) to increase the quality of relationships with those political leaders and employees who support the initiative; or (5) to tolerate employees or politicians until they resign, retire, or lose their influence.
- ◆ **Be flexible and open in your view of organizational, philosophical, and programmatic change.** No matter how much thought is given to a new initiative and how much effort is invested in planning, we still must recognize that many ideas are “losers.” Often, however, we will not know this until an idea has been tried and evaluated. Even in failure, we can learn something. Unfortunately, given the culture of our political environment, there is a tendency to mandate success—a practice that is tantamount to a search for mediocrity. Within both police organizations and the broader political system, we must maintain the “freedom to fail”—without this, creative new ideas will be few and far between.
- ◆ **The chance always exists that one may be placed on the hot seat from a political perspective.** It cannot be denied that any attempt at change carries risks—the more massive the change, the greater the risk. Questioning traditional orthodoxy is not easily accepted by organizations, particularly the bureaucratic organizations typically found in government. Thus, proponents of new initiatives must understand that when they are on the forefront of change, their political necks are on the line. In light of this, administrators must be supportive and empathetic with the politicians and employees supporting the change.
- ◆ **Change requires challenging conventional wisdom or, at least, traditions.** Debating the value of traditions has not been a politically popular avenue for people to follow, yet it is necessary to enable new ventures to be undertaken. When conventional wisdom is challenged, it will be met with resistance, criticism, and, perhaps, ridicule from doubters, dogmatists, and traditionalists. An astute leader must be prepared to deal with these reactions both personally and professionally. Importantly, when those who support the leader’s ideas of change are attacked, the leader has the obligation to reassert their value and contributions to the organization.
- ◆ **The organization’s personnel evaluation system must measure and reward effective involvement in change.** Since change requires a personal commitment or investment, individuals must be able to accrue some benefits from their participation. Benefits do not have to be monetary, but they can include such things as positive reinforcement, job perquisites, creative freedom, recognition, and awards or commendations. Similarly, awards and expressions of appreciation must be afforded to those who substantially help usher in change. In essence, without rewards for accepting change, failure is ensured.

ILP holds great potential for American law enforcement. For success to occur, however, the change process to implement ILP must begin at the most fundamental level; it must be deliberate and tailored to the needs and resources of the agency.

# CHAPTER 7

## PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE LAW ENFORCEMENT INTELLIGENCE PROCESS



Integral to the mission to provide public safety, law enforcement agencies have an inherent responsibility to protect persons' civil rights. The activities associated with the intelligence process are no exception. These freedoms, afforded to every person by the U.S. Constitution, represent some of the most important—and most fundamental—aspects of American life. Despite the perceptions of some critics, law enforcement officials accept the responsibility of protecting civil liberties as part of their duty and consider this responsibility as no less important than that of protecting the community from crime and terrorism. While this is a fundamental truth, there is debate on where the line should be drawn with respect to the degree of intrusion on privacy and personal liberty that the government should be allowed to protect America's citizens and the country's sovereignty from external threats, such as terrorism, targeted violence, or transnational criminal enterprises.

For example, one question that has been debated is whether some civil liberties should be reduced to protect America from terrorism. This issue is embodied in the philosophical question, Which is more important—protecting Americans from a terrorist attack that may kill thousands of people or protecting individual civil liberties, which are the lifeblood of America's most sacred principles? When this question is examined objectively, there is no unequivocal “right” or “wrong” answer. The question is philosophical in nature, and the answer depends on an individual's personal philosophy and life experiences.

Fortunately, intelligence analysts and law enforcement officers do not have to deal with this philosophical debate. Rather, they must focus on fairly explicit rules ensuring that constitutional protections remain intact for the intelligence process. These include the following:

## RECOMMENDATIONS FROM THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN

### Recommendation:

Law enforcement and homeland security agencies should maintain a strong emphasis on the protection of privacy, civil rights, and civil liberties (P/CRCL) in all law enforcement and homeland security actions and operations.

**Recommendation:** Law enforcement agencies should consider adopting the privacy principles promoted by Global and the CICC, and the CICC should continue to support the development of guides and templates that facilitate policy development and compliance.

### Recommendation:

Agencies should follow the tenets of 28 Code of Federal Regulations (CFR) Part 23 regarding the collection/submission, access or storage, and dissemination of criminal intelligence information by law enforcement agencies while conforming to the privacy and constitutional rights of individuals, groups, and organizations.

*NCISP, Version 2.0 (2013), pp. 20–22.*

Law enforcement cannot retain information on individuals for intelligence activities unless there is a criminal predicate. Thus, the law enforcement officer must have reliable, fact-based information that reasonably infers that a particularly described intelligence subject has committed, is committing, or is about to commit a crime.

- ◆ All information collected about an individual for intelligence purposes must be done in a manner that is consistent with the law of criminal procedure.
- ◆ Collected information in a criminal intelligence records system cannot be retained indefinitely. Instead, it may be retained only if there is reliable information that provides sustained evidence of a criminal predicate.

The law enforcement agency has the responsibility of protecting the privacy of information it collects about individuals in the course of intelligence operations. This protection of privacy extends to the dissemination of information only to officials who have the *right to know* and *need to know* the information for purposes of furthering a criminal inquiry.

- ◆ When there is no evidence of a *sustained criminal predicate*, the intelligence records about an individual must be purged (destroyed).

## A PERSPECTIVE ON THE ORGANIZATIONAL FRAMEWORK

Because of the importance—and emotions—on both sides of the debate, there has been a significant increase in the scrutiny of law enforcement intelligence activities to ensure that information is being collected, used, retained, and disseminated in a proper manner. Indeed, many law enforcement agencies have been criticized for their intelligence function, not only because of perceived abuses, but even the *potential* for abuse. This last point deserves special attention.

The potential for abuse does not mean abuse will occur; rather, it means the opportunity for abuse exists *if there are no control factors* in place to prevent abuse. The three most salient control factors are listed below:

1. Policy
2. Training
3. Supervision and accountability

**Policy** establishes the agency philosophy, standards, expectations, and decision-making boundaries on any organizational task and responsibility.

**Training** provides the knowledge, skills, and abilities to perform any occupational task. It specifies the method of performing, what must be done, how it should be done, and what should not be done. It demonstrates the application of policy and typically informs personnel of implications and sanctions if the task is not performed correctly.

**Supervision and accountability** are organizational mechanisms to ensure that policy is followed and performed in the manner specified by the training.

Subordinates' activities and behaviors are monitored by a supervisor to hold the individuals accountable for performing their responsibilities only in a manner that is sanctioned by the agency.

With clearly defined policy, effective training, and responsible supervision, the potential for abuse is dramatically reduced. Two additional factors that can also affect the potential for abuse are systemic to the organization. First is the type of people the agency employs. What are the hiring requirements? What characteristics are sought in new employees? What factors in the selection process shape the type of person who is hired? The clay used to mold the law enforcement officer will significantly influence the effectiveness of policy, training, and supervision.

The second factor is agency leadership. The tone that the leader establishes for the department as well as expectations of the leader will be reflected in the behavior of the employees. A leader who establishes clear expectations of personnel performance and supports those expectations with both rewards and sanctions, as appropriate, will also significantly lower the probability of abuse.

The potential for abuse exists with all types of law enforcement assignments, not just intelligence. Modern law enforcement seeks to perform all law enforcement responsibilities in a lawful, professional manner. To conclude that a law enforcement intelligence unit or an intelligence fusion center is inherently flawed simply because of the "potential for abuse" is fallacious.

## PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES: A FOUNDATION

To begin, some basic definitions are in order. The term *privacy* refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information (PII). Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.<sup>398</sup> The U.S. Constitution does not explicitly use the word *privacy*, but several of its provisions protect different aspects of this fundamental right. Although there is no explicitly stated federal constitutional right to an individual's privacy, privacy rights have been articulated in different contexts by the U.S. Supreme Court.<sup>399</sup> Privacy protections are numerous and include protection from unauthorized collection of personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information.

The term *civil rights* is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship or residency regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. Specifically, they are the rights to personal liberty guaranteed to all persons in the United States by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government. As such, *civil liberties* refers to fundamental individual rights derived from the Bill of Rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Privacy, civil rights, and civil liberties (P/CRCL) all have important implications for the law enforcement intelligence process, particularly in light of past abuses. Critics claim that law enforcement has not changed its intelligence practices and that post-September 11, 2001 (post-9/11), counterterrorism initiatives have made law enforcement agencies even more intrusive. Understanding this concern and the consequent scrutiny of law enforcement intelligence activities by those concerned about P/CRCL abuses provides an important perspective.

---

398 For a review of privacy issues as related to various types of electronic information collection, see Cornell Law School, Legal Information Institute, [https://www.law.cornell.edu/wex/electronic\\_surveillance](https://www.law.cornell.edu/wex/electronic_surveillance).

399 Several state constitutions contain explicit language regarding a right to privacy. See <https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>.

## INCREASED SCRUTINY OF LAW ENFORCEMENT INTELLIGENCE: THE CHALLENGE OF BALANCING P/CRCL AND COMMUNITY SAFETY

Why has scrutiny and criticism of law enforcement intelligence activities increased when there is a demonstrable threat of terrorism that can cause catastrophic effects, as evidenced by the human, social, and economic impact of 9/11? There appear to be several factors.

Perhaps at the top of the list are past abuses. Unfortunately, as described in Chapter 2, there is a documented history of law enforcement (and other government agencies) that improperly collected, retained, and/or disseminated information and behavior about individuals whose public statements and actions were controversial but not criminal. While in many of those instances, law enforcement agencies believed the intelligence target was undermining American sovereignty,<sup>400</sup> the fact remains that the agencies had no authority to collect or retain the information because it was noncriminal “expressive activity.” *It must be emphasized that law enforcement authority to perform any kind of intelligence activity is based solely on the statutory authority to enforce the criminal law, hence the obligation to follow the law of criminal procedure. As such, collecting information about people without an articulable criminal nexus is improper.* Law enforcement agencies remain under scrutiny and are still paying the price for these abuses of the past.

A second reason has its foundation in the Civil Rights Movement that had its birth in the 1960s and is exemplified by U.S. Supreme Court decisions under Chief Justice Earl Warren that expanded the application of civil rights and liberties.<sup>401</sup> The era experienced, for the first time, citizens overtly exercising and testing their rights in the form of public demonstrations and civil disobedience on a major scale as part of the Civil Rights Movement and Vietnam War protests. This atmosphere prompted lawsuits by a new breed of activist civil rights attorneys against police departments and corrections agencies. These actions largely brought a long-standing federal statute, 42 USC 1983—*Civil Action for Deprivation of Civil Rights*—out of dormancy. Collectively, these events placed a new emphasis on the rights of Americans and added a new lexicon to the American justice experience.

A third factor is that many persons do not understand the distinction between law enforcement intelligence and national security intelligence. As such, they assume that actions of the intelligence community may also reflect actions of a law enforcement agency. The National Security Agency’s (NSA) capture of international telephone conversations, or monitoring by the Federal Bureau of Investigation (FBI) of a suspicious person entering the United States and identified by the CIA as a possible threat, are examples of information collection that a state, local, or tribal law enforcement agency will neither perform nor typically have access to. Yet there is often an assumption that law enforcement agencies are involved in such activities and, as such, must be monitored to protect civil rights.

Fourth, the 24-hour news cycle and evolving media sources, including social media, have also contributed to the increased scrutiny of law enforcement operations, including intelligence. Notwithstanding some changes in the print media, the evolution of the electronic media—both broadcast and Internet—have significantly contributed to scrutiny of government activities. The increased number of electronic outlets has added spirited competition to news organizations, increasing competition to capture news stories that will both pique the interests of consumers and meet the need for content on a 24/7/365 basis. Online, news, and social media outlets are all seeking to post stories

---

400 This was particularly true with the fear of communism and members of the American Communist Party and their sympathizers during the 1950s and 1960s.

401 As an example of how law enforcement adapts to change, when many of the Warren Court decisions expanded civil rights protections for the criminally accused, there was a loud cry by many that the court was “handcuffing the police” and that this would lead to more crime. (The *Miranda v. Arizona*, 384 U.S. 436 [1966], decision was a particularly significant decision influencing this sentiment at that time.) Sentiments ran so strong that “Impeach Earl Warren” billboards appeared across America. As new policy and training were put in place in law enforcement agencies, and particularly as new officers were hired, most of whom were college educated, the Warren Court decisions were embraced as “simply the rules we have to follow.” In a comparatively short amount of time, it became a nonissue.

that will attract a lot of attention—so-called “click bait.” As a result, there is more competition for controversial stories that will uniquely resonate with consumers. Moreover, because of the need to fill every hour with content, stories receive more detail and are often repeated many times throughout a day. The consequent effect is bombardment with information on a given topic that gives an impression of an issue that is somewhat disproportionate.

A fifth factor contributing to the scrutiny of law enforcement intelligence appears to be increased partisanship among elected officials and the electorate. This has resulted in a dichotomous environment on virtually every social, political, and economic issue where attitudes and behaviors tend to be drawn exclusively along partisan lines with extreme criticism and little conciliation toward opponents’ views. Virtually any factor at issue—including law enforcement intelligence—can be caught in some type of partisan dispute.

Next, the growth of civil rights advocacy groups<sup>402</sup> has also clearly influenced public scrutiny of law enforcement. These groups identify incidents and trends that heighten their concerns about privacy protections. Through press releases, website stories and updates, white papers, public presentations, and lawsuits, these groups publicize government behaviors they feel are improper. While not always publicly popular, these groups nonetheless bring the issue to the table to open a public debate and often seek to change public policy through litigation, political influence, or public pressure.

Finally, the movement toward open government<sup>403</sup> invites public scrutiny. In its current form, largely beginning in the 1970s in the United States with Watergate, a grassroots movement slowly became known as “open government.” The essential concern was that public officials were abusing the authority of their offices and had the obligation to demonstrate that actions of government officials were lawful and in the best interests of all citizens. The movement continued to gain widespread support, with government officials slowly responding. Open records acts and open meetings acts were increasingly being passed, federal and state Freedom of Information Acts (FOIAs) were expanded, and judicial interpretations of FOIA legislation became increasingly broad. As a result of public demand, elected officials were required to issue financial disclosure statements and public watchdog groups began issuing reports on various actions of officials at all levels of government. Essentially, the movement seeks accountability in government, including all aspects of law enforcement.

Collectively, these factors have contributed to the public’s expectation of a right to know what is going on in government activities, and the public has increasingly sought explanations and pushed for accountability through lawsuits. In recent years, fueled by social media and 24-hour news channels, accountability has grown into second-guessing many government decisions. Publication of some classified documents by the media is one artifact of this movement. In general, mainstream open-government advocates recognize the need to maintain secrecy of content; however, they expect openness as it relates to processes. That is, they recognize the need to keep explicit information confidential but want assurances that information is being collected, retained, used, and shared in a manner that protects their rights. These ideals affect law enforcement intelligence activities at all levels of government and indicate the need to have open processes and privacy policies in place. The ideal of government “of the people, by the people and for the people” is being increasingly demanded and must be taken seriously by policymakers. Intelligence is no exception. This is particularly true with new and emerging technologies that can collect a wide array of information about people. As evidence of this, the American Civil Liberties Union (ACLU) has stated:

Technological innovation has outpaced our privacy protections. As a result, our digital footprint can be tracked by the government and corporations in ways that were once unthinkable. This digital footprint

---

402 See *Defending Rights and Consent*, <https://rightsanddissent.org/>; American Civil Liberties Union, <http://www.aclu.org/>; Electronic Frontier Foundation, <http://www.eff.org/>; or Center for Democracy and Technology, <http://www.cdt.org>. Each has particular areas of concern about privacy, civil rights, and civil liberties as related to all types of governmental policy and actions, not just law enforcement. Each organization provides an important watchdog role, albeit often with controversy. Of course, a watchdog or advocacy organization that does not stimulate controversy is probably not taking much action.

403 <https://opensource.com/resources/open-government>

is constantly growing, containing more and more data about the most intimate aspects of our lives. This includes our communications, whereabouts, online searches, purchases, and even our bodies. When the government has easy access to this information, we lose more than just privacy and control over our information. Free speech, security, and equality suffer as well.<sup>404</sup>

Similarly, the *Defending Rights and Dissent* has stated:

We seek to hold government accountable to We the People and create a nation where police and intelligence agencies cannot be used as tools of repression or to silence dissent. Our work will ensure government accountability and transparency, end profiling based on personal characteristics (such as race, religion, ideology or gender) by law enforcement and intelligence agencies and will protect our private information and activities from unwarranted government spying.<sup>405</sup>

It is important to recognize the need for accountability and the ramifications on a law enforcement agency if accountability is dismissed or ignored. Collectively, these factors represent a significant sociopolitical change in American life and, consequently, affect law enforcement intelligence initiatives.

## LAWSUITS AND DECREES RELATED TO LAW ENFORCEMENT INTELLIGENCE ACTIVITIES

Perhaps the most controversial area of information gathering by law enforcement agencies deals with cases in which individuals are involved in expressive activity that is often controversial, even extreme. People who express extreme views related to animal and environmental protection, anti-government sentiments, anarchy, white supremacy, or any other belief system are often viewed as a threat, even though their specific actions may not be criminal. Indeed, evidence has shown that there is an arena of behavior between “extreme” and “criminal” that is dynamic and often difficult to define. The distinction between making a firm statement of belief and making a threat is often a matter of interpretation connected with behavior that is indicative of a crime. The intelligence process seeks to collect information about individuals who pose threats to the community. However, the behavior a law enforcement officer interprets as having a criminal nexus may be behavior a civil libertarian calls freedom of expression.

The need to understand the subtleties in these distinctions is important to ensure that law enforcement officers are performing their function lawfully while simultaneously protecting the community from harm. Unfortunately, as noted previously, there is a legacy of abuses in which law enforcement agencies have collected information on individuals simply as a result of their political beliefs.<sup>406</sup> While law enforcement agencies have changed significantly over the past several decades, this legacy is difficult to overcome.

The Supreme Court’s broad interpretation of the First Amendment-based right of association, as originally defined in *NAACP v. Alabama*<sup>407</sup> and more recently in *Boy Scouts of America v. Dale*,<sup>408</sup> can protect groups engaged in First Amendment conduct from unjustified political or religious surveillance that causes them cognizable harm. As a result, the state’s interest in protecting the community may, in many instances, be outweighed by the protections afforded to expressive activity found in these court decisions. While limitations on surveillance cannot unduly restrict the government’s ability to conduct necessary information gathering, requiring a reasonable suspicion of criminal activity before investigating First Amendment activity can help achieve a suitable balance between public safety interests and

---

404 <https://www.aclu.org/issues/privacy-technology>

405 <https://rightsanddissent.org/about/>

406 For a good historical perspective, see Chevigny, P. G. (1984). “National Security and Civil Liberties: Politics and Law in the Control of Local Surveillance.” *Cornell Law Review*. 69(April), p. 735.

407 *NAACP v. Alabama*, 357 U.S. 449 (1958).

408 *Boy Scouts of America, et al. v. Dale*, 530 U.S. 640 (2000).



## CONSENT DECREE

A consent decree is a settlement that is contained in a court order. The court orders injunctive relief against the defendant and agrees to maintain jurisdiction over the case to ensure that the settlement is followed. (Injunctive relief is a remedy imposed by a court in which a party is instructed to do or not do something. Failure to obey the order may lead the court to find the party in contempt and to impose other penalties.) Plaintiffs in lawsuits generally prefer consent decrees because they have the power of the court behind the agreements; defendants who wish to avoid publicity also tend to prefer such agreements because they limit the exposure of damaging details. Critics of consent decrees argue that federal district courts assert too much power over defendants. They also contend that federal courts have imposed conditions on state and local governments in civil rights cases that usurp the power of the states.

<https://legal-dictionary.thefreedictionary.com/settlements>

associational rights.<sup>409</sup> This evidence of criminal activity—that is, the criminal predicate—establishes the compelling state interest that justifies law enforcement intelligence inquiries and information retention.

There are two particularly noteworthy court cases with regard to expressive activity and the law enforcement intelligence function. Understanding the lessons learned from these cases provides insight useful for decision making as related to information collection and retention.

*New York: Handschu v. Special Services Division, 605 F. Supp. 1384 (S.D.N.Y. 1985), affirmed, 787 F.2d 828 (2d Cir. 1986).* In the 1960s, the New York Police Department (NYPD) increased surveillance and other investigations to include:

...more undercover and other surveillance of “groups that because of their conduct or rhetoric may pose a threat to life, property, or governmental administration”; of “malcontents”; and of groups or individuals whose purpose is the disruption of governmental activities for the peace and harmony of the community.<sup>410</sup>

While many activists maintained that the NYPD was collecting information on various activists who held nontraditional views but were not committing crimes, they had difficulty demonstrating evidence of this.

During a 1971 trial of 21 Black Panthers charged with attempting to blow up several police stations, information made public through the discovery process, evidence, and testimony in the case revealed that the NYPD kept dossiers on groups defined as radical and activist, as well as others including homosexual groups, educational reform advocates, and some religious and civic groups.<sup>411</sup> As a result of this new information, the Handschu case was filed as a class-action lawsuit against NYPD surveillance activities<sup>412</sup> by 16 individuals affiliated with various ideological associations and organizations.

---

409 Fisher, L. E. (2004). “Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups.” *Arizona Law Review*. 46(Winter), p. 621.

410 *Handschu v. Special Services Division*, 605 F. Supp. 1384 at 1396 (S.D.N.Y. 1985).

411 Lee, C. “The NYPD Wants to Watch You.” *The Village Voice*. Series of articles December 18–24, 2002. <https://www.villagevoice.com/2002/12/17/the-nypd-wants-to-watch-you/>.

412 Specifically identified for these activities was the Special Services Division of the NYPD Intelligence Bureau.

In the suit, plaintiffs contended that “informers and infiltrators provoked, solicited, and induced members of lawful political and social groups to engage in unlawful activities”; that files were maintained with respect to “persons, places, and activities entirely unrelated to legitimate law enforcement purposes, such as those attending meetings of lawful organizations”; and that information from these files was made available to academic officials, prospective employers, and licensing agencies and others. In addition, plaintiffs identified seven specific forms of police conduct: (1) the use of informers; (2) infiltration; (3) interrogation; (4) overt surveillance; (5) summary punishment; (6) intelligence gathering; and (7) electronic surveillance. The complaint alleged, *inter alia*, that these police practices had had a “chilling effect” upon the exercise of freedom of speech, assembly, and association; that they also violated constitutional prohibitions against unreasonable searches and seizures; and that they abridged rights of privacy and due process. The suit requested declaratory and injunctive relief to curtail these practices.<sup>413</sup>

Police officials conceded that their activities included information gathering for the intelligence process was “not limited to investigations of crime, but related to any activity likely to result in ‘a serious police problem.’”<sup>414</sup> Essentially, the police department asserted that it had a need to collect information about people and their activities which, although absent a criminal predicate at the time, held a demonstrably strong potential for criminal activity, arguing that the information collection was necessary for community safety.

The consent decree in *Handschu v. Special Services Division*, which included what is referred to as the Handschu Settlement agreed to in 1985, governs NYPD investigations of groups or individuals who engage in various forms of political activity. The settlement established the Handschu Authority<sup>415</sup> to oversee the activities of the Public Security Section (PSS) of the Intelligence Division.<sup>416</sup> The NYPD could not engage in any investigation of political activity, which the settlement defined as “the exercise of a right of expression or association for the purpose of maintaining or changing governmental policies or social conditions.”<sup>417</sup> The settlement authorized the PSS to commence an investigation only after the NYPD established:

. . . specific information [that] a person or group engaged in political activity is engaged in, about to engage in, or threatened to engage in conduct which constitutes a crime.<sup>418</sup>

Information obtained during investigations of individuals, groups, or organizations could be collected or maintained only in conformity with the settlement. Information “from publicly available sources” could not be maintained with the PSS.<sup>419</sup> Officers were allowed to collect only certain general information about a planned noncriminal event “in order to preserve the peace, deploy manpower for control of crowds and protect the right[s] of individuals to freedom of speech and assembly.”<sup>420</sup> The settlement prohibited developing a file on an individual or group based solely on that individual’s or group’s “political, religious, sexual or economic preference.” In sum, the key elements of the Handschu consent decree are that:

1. Political groups can be investigated only when suspected criminal activity is alleged.
2. The NYPD must obtain a written authorization from a three-person panel—the Handschu Authority—after presenting its suspicions.

---

413 Koehnlein, B. (2003). *The History of the Handschu Decree*. New York Civil Liberties Union.

414 Handschu, *ibid.* p., 1396.

415 The Handschu Authority, similar to an oversight board, consisted of the first deputy commissioner of the police department, the deputy commissioner for legal affairs, and a civilian member appointed by the mayor for a term that was revocable at will.

416 The Public Security Section (PSS) of the NYPD Intelligence Division was the new name for what had been the Special Services Division of the Intelligence Unit when the original class-action lawsuit was filed.

417 Steigman, J. L. (2003). “Reversing Reform: The Handschu Settlement in Post-September 11 New York City.” *Brooklyn Journal of Law and Policy*. Vol. 11, p. 759.

418 *Ibid.*

419 This was a significant limitation on the use of open source information, which has a compounded limiting effect in the age of social media.

420 *Ibid.*, p. 760.

3. The NYPD is prohibited from videotaping and photographing public gatherings in which there is no indication that any criminal activity is present.
4. The NYPD must obtain written agreement from any agency with which it intends to share this information, acknowledging that it will abide by the terms of the Handschu Decree.
5. The court ordered that there be annual reports, open to the public, demonstrating the NYPD's requests for surveillance and the number of requests the panel granted.

In light of the threat environment after the 9/11 attacks—an environment which, of course, was particularly pronounced in New York—the NYPD sought and obtained modification of the consent decree.<sup>421</sup> While the NYPD requested fairly broad latitude for information collected about the activities of persons who were likely political extremists, the court's modification of the consent decree was narrower, yet still permitting some expansion of the original restrictions. The court acknowledged that there was a change in the public safety environment in New York following the 9/11 attacks and modified the Handschu consent decree to be consistent with the *FBI Guidelines*<sup>422</sup> sued by the U.S. Attorney General (which have since been updated<sup>423</sup>):

The *FBI Guidelines* provide for three graduated levels of investigative activity: (1) [permit] checking initial leads [when] information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted; (2) a preliminary inquiry [is] authorized when there is information or an allegation which indicates the possibility of criminal activity and whose responsible handling requires some further scrutiny beyond checking initial leads; and (3) a full investigation [is] authorized when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed.<sup>424</sup>

The modification authorized by the court was viewed as a mixed bag by both the NYPD and civil libertarians; hence one may conclude it was a reasonable compromise. The Handschu Authority for oversight was retained in the modified consent decree. Another motion related to the consent decree requested the court to enjoin enforcement of *New York City Police Department Interim Order 47*, which established procedures and guidelines for the police department's use of photographic and video equipment, arguing it was incompatible with NYPD guidelines, violated the plaintiff's First Amendment rights, and violated previous Handschu judgments.<sup>425</sup>

In February 2007, the court rejected the motions on the grounds that the investigations in question were not politically motivated. The court also stated that, since Order 47 did not constitute a First Amendment violation, it would not grant the plaintiffs' injunctive relief. Later in the year, the court further modified its February decision on the enforceability of the consent decree, requiring that plaintiffs show a systemic pattern of violations before the court would enjoin any police department policy.

In 2018, A federal court overseeing unprecedented reforms in the wake of wrongful NYPD surveillance of Muslim communities released the first annual report of an appointed civilian representative. The report provides the public with its first direct insight into the workings of the Handschu Committee, a body that reviews NYPD investigations of First Amendment-protected religious and political activity for compliance with a judicially enforced agreement. The report revealed that the committee has denied considerably more NYPD applications for such investigations since the civilian representative assumed his position.<sup>426</sup>

---

421 Steigman, J., *Ibid.*, p. 746.

422 The Guidelines are available at: <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>.

423 <https://www.justice.gov/archive/opa/docs/guidelines.pdf>

424 *Handschu v. Special Services Division*, 71 Civ. 2203 (Feb. 11, 2003) Slip Op. at 33–34.

425 <https://www.nyclu.org/en/publications/testimony-police-surveillance-political-activity-history-and-current-state-handschu>

426 <https://www.aclu.org/press-releases/court-releases-first-annual-report-nypd-reforms-after-landmark-muslim-surveillance>

The lessons learned from *Handschu* are that regardless of the threat environment facing a community, surveillance of individuals by a law enforcement agency—including photographs, video and collecting identities—still requires a criminal nexus. While some flexibility was given in the post-9/11 environment, the effects of the *Handschu* case on NYPD intelligence remains decades later. What has not deviated is that the constitutional guarantee of free speech and the freedom of expression remain paramount and must be respected by law enforcement agencies.

***Denver: American Friends Service Committee, et al. v. City and County of Denver, 2004 U.S. Dist. LEXIS 18474.***

On March 11, 2002, the ACLU of Colorado publicly disclosed documents demonstrating that the Denver Police Department (DPD) Intelligence Bureau had been monitoring and recording the peaceful protest activities of Denver-area residents and keeping files on the expressive activities of advocacy organizations about whom there was no evidence of criminal activity. In a letter to the Denver mayor, the ACLU asked the mayor to take immediate steps to stop the department’s practice of keeping files on peaceful protest activities. In the March 11 letter, the ACLU also asked the mayor to take four additional actions:

1. Prohibit the police department from sharing its criminal intelligence information with other law enforcement agencies.
2. Order a full public accounting about the criminal intelligence information that would answer a number of questions.
3. Notify individuals named in the criminal intelligence information and permit them to review the information about them in the files.
4. Preserve the criminal intelligence information because it might be evidence in any forthcoming lawsuits.<sup>427</sup>

On March 13, 2002, at a news conference, the Denver mayor stated:

After a preliminary review of the policy and reviewing a sampling of the files that have been kept on individuals and organizations, it is our conclusion that there was an overly broad interpretation of the policy that resulted in cases where it may not have been justifiable to include certain individuals or organizations in our intelligence gathering activities.<sup>428</sup>

The plaintiffs filed a class action civil rights suit<sup>429</sup> for violating U.S. and Colorado constitutional protections by not adhering to the police department’s intelligence records policy and failing to manage their criminal intelligence records system according to the guidelines in 28 Code of Federal Regulations (CFR) Part 23 (28 CFR Part 23). The *Plaintiffs’ Class Action Complaint for Declaratory and Injunctive Relief*,<sup>430</sup> initially filed on March 28, 2002, challenged a practice of the Denver Police Department of monitoring the peaceful protest activities of Denver-area residents when there is no evidence of criminal activity, maintaining criminal intelligence records files<sup>431</sup> on:

. . .the expressive activities of law-abiding individuals and advocacy organizations, many of which the Department has falsely branded with the label of “criminal extremist;” and providing copies of certain Spy Files to third parties.<sup>432</sup>

---

427 *American Friends Service Committee, et al. v. City and County of Denver*, Class Action Complaint for Declaratory and Injunctive Relief, p. 4.

428 Ibid.

429 42 U.S.C. §1983 – Civil Action for Deprivation of Civil Rights

430 <https://www.aclu.org/other/denver-police-keeps-spy-files-peaceful-protesters#:~:text=The%20ACLU%20filed%20a%20class,the%20files%20to%20third%20parties.>

431 The criminal intelligence files in the complaint and subsequent news releases by the ACLU were referred to as the “Spy Files.”

432 *American Friends Service Committee*, Ibid., p. 2.

The complaint further alleged that the Denver Police Department had:

. . . singled out and selected the plaintiffs and the plaintiff class for surveillance and monitoring based upon their advocacy of controversial or unpopular political positions and opinions.<sup>433</sup>

The plaintiffs also expressed concern that individuals would be less likely to join a rally or to participate in other expressive activities if they feared being photographed by police officers or that their identities would appear in police criminal intelligence files. The complaint goes on to state that the criminal intelligence records on the plaintiffs:

. . . contain nothing but identifying information and facts that show that the targets of the surveillance are engaged in peaceful and legitimate educational activities, political expression, petitioning the government, and political association. The pages contain no facts that suggest that any of the named plaintiffs are involved in criminal activity.

The Department has recorded false and derogatory information about the Plaintiffs. It has mischaracterized the goals and purposes of the Plaintiffs' expressive activity and smeared their personal, political, and professional reputations.

The Department has disseminated the information in the Spy Files to third parties."<sup>434</sup>

Supporting their claims, the plaintiffs demonstrated practices in the department, including memoranda to officers from supervisors that were explicitly in contradiction to the Denver Police Department's criminal intelligence records policy, 28 CFR Part 23, and/or constitutional standards. For example, one memorandum from the Intelligence Bureau Commander to subordinates stated, in part:

Please purge, i.e. shred, [sic] toss or take home, ALL references and files earlier than a 1994 date. The heart of an Intelligence Bureau lies with the ability to maintain integrity of all files and references in the likely event of litigation by political or subversive groups.<sup>435</sup>

It should be noted that a directive from an intelligence commander to a subordinate, as in this case, to "toss or take home" intelligence records with PII, is most likely negligent direction and supervision.

In light of the evidence presented in this case, while not admitting ". . . any fault or liability to plaintiffs, nor any violation of law,"<sup>436</sup> the City of Denver entered into a settlement agreement with the plaintiffs. As part of the settlement agreement,<sup>437</sup> the department established a new, more restrictive intelligence records policy,<sup>438</sup> created an oversight board, purchased a new computerized intelligence records system, and agreed to semiannual audits of compliance with the settlement agreement for five years.

The lessons learned from this case reinforce the requirement of a criminal predicate. Beyond this, the Denver case illustrates: (1) the necessity of recognizing and honoring First Amendment protections, (2) the importance of proper supervision to enforce currently existing policy, (3) the importance of using the right-to-know and need-to-know standards of dissemination, and (4) the importance of complying with the 28 CFR Part 23 guidelines.

---

433 Ibid.

434 Ibid., p. 6.

435 Denver Police Department Intelligence Bureau, Inter-Office Correspondence to "All Troops" from the Intelligence Bureau Commander, Subject: Purge Days, November 2, 1998. <https://www.aclu.org/other/denver-police-keeps-spy-files-peaceful-protesters>

436 *American Friends Service Committee, et al. v. City and County of Denver*, Settlement Agreement, April 17, 2003, p. 5, Section 7.3.

437 Ibid.

438 Ibid.

**Implications from Handschu (New York) and American Friends (Denver).** At the heart of civil rights issues related to law enforcement intelligence are collection, retention, and dissemination of information that identifies individuals and organizations whose expressions and expressive activities pose a threat to public safety and security. The proverbial bottom line that is clear from these two cases reinforces the premise that any collection, retention, and dissemination of such information may occur when there is a nexus between the behavior and a crime. Simply unpopular, unusual, or extreme expressions, along with assumptions that persons making such expressions may eventually commit a crime, do not alone meet the test. There must be demonstrable evidence of a crime. Law enforcement officers should receive training to understand the issues associated with expressive activity and a criminal predicate.

It is also clear from these cases that simply having a policy on criminal intelligence records is not enough—even if the policy is compliant with 28 CFR Part 23. There must also be supervision to ensure that the policy is followed. Law enforcement personnel must have explicit direction on their information collection activities, and that direction must be consistent with standards that are characteristic of both professional good practice and the protection of civil rights and liberties. Similarly, it is important to reinforce that the dissemination of any such criminal intelligence information must meet the right-to-know and need-to-know standards.

These factors will be discussed in detail later. The important point is the role they played in the two important cases just described and the consequences that followed when those standards were not met.

## **CIVIL RIGHTS EXAMPLE: FIRST AMENDMENT FREEDOM OF EXPRESSION—TWO VIEWS**

A common point of conflict over civil rights is found in actions related to freedom of expression by persons involved in protests or demonstrations. Civil rights advocates maintain that their demonstrations are expressive activity protected by the First Amendment and should be given wide latitude to occur without any intervention or interference by law enforcement. As such, they view it as improper for law enforcement agencies to collect and retain information about persons who are involved in planning and participating in demonstrations as well as advocates of those individuals.

Law enforcement agencies maintain that the only information they collect and retain is that related to persons who commit crimes or pose threats to community safety. Civil rights advocates respond that minor crimes—such as trespassing or minor property destruction—are of such low magnitude as not to counterbalance the violation of the broader First Amendment guarantees and that law enforcement agencies use minor crimes as an excuse to collect information about those with whom they disagree. Law enforcement agencies counter that they have the responsibility to protect the property of all victims and that any demonstration that permits property destruction can quickly spin out of control and result in even greater threats. The debate continues, often with opposing arguments, as illustrated in Table 7-1.

These are diametrically opposed positions on the same issue. Which position is correct? Like most issues in which there are clear dichotomous perspectives, the truth is somewhere in the middle of the continuum. The reality is that the burden typically falls on the law enforcement agency to show that its actions were done and the information collected in a manner that protects both civil rights and community safety. To minimize allegations of negligence and impropriety, as well as to demonstrate good-faith actions by the law enforcement agency, a number of action steps should be performed. These include the following:

1. Review the evidence and determine whether there is trustworthy information about which a reasonable person would conclude that a crime may occur.
2. Employ the least intrusive means of information collection.
3. Provide specific direction on the types of criminal behavior that is suspected and the types of information that need to be collected to support the criminal predicate.

4. Ensure that supervision is present to monitor the law enforcement officers' information collection activities.
5. When possible and appropriate, communicate with the protesting group to express concerns about crimes and procedures that will be followed should a crime occur.
6. Ensure that all personnel understand the policy for information collection.
7. Ensure that all law enforcement activities are documented and explained as a matter of record.
8. Provide officers with information and training about the elements of crimes for which there is specific concern.
9. When the demonstration is over, review all information collected and destroy all information that is not needed to support a criminal case.
10. Prepare an after-action report that reviews processes, issues, and concerns—preferably with assistance from legal counsel—and amend processes that may place the agency in legal jeopardy.

## THE NEED FOR MORE CONTROLS OF INTELLIGENCE INQUIRIES THAN CRIMINAL INVESTIGATIONS

At the heart of the diverse reasons why information collection by law enforcement agencies for the intelligence process is met with skepticism and suspiciousness is the belief by many that intelligence inquiries are a greater threat to liberty than criminal investigations. An intelligence inquiry attempts to assess the presence of a threat and determine whether a threat is real, unlike a criminal investigation that occurs after a crime has been discovered. Moreover, intelligence inquiries often engage First Amendment expression, are more secretive, and are less subject to after-the-fact scrutiny. Civil rights activists argue, therefore, that intelligence activities should require stronger compensating protections and remedies for violations. Three primary factors support these notions.

First, intelligence inquiries are broader. While they are limited by the criminal code, the breadth goes beyond crimes that have been committed and moves into the arena of threats. An explicit concern of civil rights activists is about when law enforcement agencies collect information about First Amendment activities. There is often disagreement about the interpretation of language and behavior: whether it is the exercise of free speech or the exhortation of a threat.

Second, intelligence inquiries are conducted in much greater secrecy than are criminal cases, even perpetual secrecy. When a person is accused in a criminal case, normally that person can make public statements about his or her innocence and publicly rebut the criminal assertions in open court proceedings. Moreover, in a criminal investigation, the suspect is often aware of the investigation while it is under way. Similarly, most searches in criminal cases are carried out with simultaneous notice to the target. During intelligence inquiries, in contrast, the target and any individuals scrutinized because of their contacts with the target are rarely told of the government's collection of information about them. While the presumption of innocence is clearly respected in a criminal investigation, it is sometimes argued that there is a presumption of guilt in an intelligence inquiry. This perspective must change.

Third, in a criminal investigation, almost everything the government does is generally exposed to public scrutiny. A prosecutor knows that, at the end of the criminal process, his/her actions will be public. If the prosecutor is overreaching or is on a "fishing expedition," this complaint will be aired with the prosecutor facing public scrutiny, ridicule, and, in extreme cases, disbarment.<sup>439</sup> That is a powerful constraint. Similarly, a police department must ultimately account to the public for crime rates and disorder in a community. However, most intelligence inquiries never result in a trial or other public proceeding. The evidence may be used clandestinely. Sometimes, the desired result is the mere sense that the government is watching.

---

439 This occurred in the case of North Carolina prosecutor Michael Nifong's allegations of sexual assault against Duke University Lacrosse players. For more information, see "Duke Lacrosse Prosecutor Disbarred." *CNN*. <http://www.cnn.com/2007/LAW/06/16/duke.lacrosse/index.html>.

TABLE 7-1: COUNTER POSITIONS ON FIRST AMENDMENT INFORMATION COLLECTION

POSITION OF PROTESTORS	RESPONSE OF LAW ENFORCEMENT
1. Government should not attempt to regulate expressive activity, no matter how repugnant, as long as the activity is done without committing a crime.	1. Often, it is difficult to determine, during the course of a protest or rally, whether a crime is being committed or going to be committed. For example, anarchists have frequently spray-painted private property or broken windows during the course of a protest. Spray-painting the property of another is destruction of property, not an expressive activity.
2. Expressive activity is a fundamental right that is essential to the fabric of American life. As such, law enforcement should take no action to repress expressive activity.	2. Law enforcement has the obligation to protect the rights of all Americans, not just those engaged in expressive activity. As such, law enforcement agencies have the responsibility to take reasonable restrictive actions to protect the rights of others as well as to maintain community safety and security.
3. There should be no expressly defined protest zones that favor one group over another.	3. Some groups have a history of committing crimes during a protest, more than others do. Protest zones are used only in those cases in which there is a history of crime or information that reasonably suggests that a crime will be committed during a protest.
4. Law enforcement should not use pens, barricades, or force to regulate expressive activity.	4. In some cases, pens and barricades are used to protect the protestors or to prevent a conflict between protestors and those opposed to the group’s expressive activity (e.g., Ku Klux Klan rallies).
5. Law enforcement should not use surveillance and infiltration of political or social groups involved in expressive activity.	5. Where there is reasonable suspicion to believe that a crime will occur, the use of surveillance and infiltration is an accepted and lawful method to gather evidence for developing a criminal case for prosecution.



Since intelligence inquiries are broader, more secretive, and subject to less after-the-fact scrutiny, protections must be built in at the beginning. This is accomplished by adhering to professional standards, implementing sound intelligence policies and procedures, providing effective training, ensuring effective supervision, and having processes for review and accountability.

## MAINTAINING PRIVACY IN THE INTELLIGENCE PROCESS

The concept of privacy is broad, encompassing different personal values and interests. A number of privacy-related factors have become relevant in the current law enforcement intelligence environment, which has increased use of technologies for information collection and analysis purposes.<sup>440</sup> Privacy interests may be characterized as representing a diverse array of issues, such as privacy of a person's beliefs, privacy of personal behavior, privacy of personal communications, privacy of personal attributes (such as health or handicaps), and privacy of personal data (information privacy). Private information includes not only information that a law enforcement agency may be collecting about a person's possible involvement in a criminal act, but also information relating to:

- ◆ Name, address, telephone number, or email
  - ◆ Race, national origin, or ethnic origin
  - ◆ Religion
  - ◆ Gender
  - ◆ Marital status
  - ◆ Fingerprints, blood type, or DNA
  - ◆ Financial status, history, or credit condition
  - ◆ Psychiatric or psychological conditions and history
  - ◆ Criminal history
  - ◆ Age
  - ◆ Sexual orientation
  - ◆ Education
  - ◆ Medical history or conditions
  - ◆ Employment history, including employment dispositions
- ◆ Identifying number, symbol, or other character assigned to identify a person (such as a social security number, driver's license number, or university student identification number)

In the course of an intelligence inquiry, a law enforcement agency will collect different types of personal information, but it has the obligation to maintain the privacy of the information regardless of whether the person is an intelligence target, a witness, an informant, or an information provider (such as a citizen).

Privacy of personal data (information privacy) is described as when, how, and to what extent you share personal information about yourself. Information privacy involves the right to control one's personal information and the ability to determine if and how that information should be obtained and used. It entails restrictions on a wide range of activities relating to personal information: its collection, use, retention, and disclosure.<sup>441</sup>

The law enforcement organization has an obligation to protect the privacy of all persons about whom the agency collects PII, including those suspected of committing crimes. Two primary methods are used: *security* and *confidentiality*.

**Security** of personal information means that mechanisms and processes have been put in place to ensure that there is no unauthorized access to that information. Whether private information is in a computer system or in paper records, there must be an adequate mechanism in place to ensure that the information is not obtained by persons without lawful access.

---

440 Criminal Intelligence Coordinating Council. (2019). *Fusion Center Privacy, Civil Rights and Civil Liberties Development Guide. Version 3.0*. <https://it.ojp.gov/GIST/48/Fusion-Center-Privacy--Civil-Rights--and-Civil-Liberties-Policy-Development-Template--Version-3-0>

441 National Criminal Justice Association (NCJA). (2002). *Justice Information Privacy Guide*. Washington, DC: NCJA, p. 12.

**Confidentiality**, particularly as related to information sharing, includes behaviors and processes that seek to prevent unauthorized disclosure of information to third parties. Thus, after private information has been collected, the custodian of the information has the obligation to protect it from being shared with others unless there is a bona fide reason for a third party to receive the information. Once again, the standard of sharing personal information with others is based on their right to know and need to know the information. This is an illustration of processes to ensure confidentiality. Moreover, there is an expectation that those who receive private information will maintain the confidentiality of the information entrusted to them. Confidentiality is about limiting access to personal information (1) to those having specific permission to access<sup>442</sup> the records and (2) preventing its disclosure to unauthorized third parties.

To maximize privacy protection, law enforcement agencies should ensure that privacy protections are in place. The National Strategy for Information Sharing emphasizes this fact by establishing core privacy principles that all agencies are required to adopt. While the focus of these principles in the strategy was on terrorism, it has been expanded in this discussion to apply to intelligence inquiries for any crime:

- ◆ Share protected information only to the extent that it is terrorism information, homeland security information, or law enforcement information related to terrorism or any other criminal law violation.
- ◆ Identify and review the protected information to be shared within the Information Sharing Environment (ISE) as well as that to be shared with other intelligence and investigative personnel at all levels of government.
- ◆ Enable those with whom information is being shared to determine the nature of the protected information to be shared and its legal restrictions (e.g., “this record contains individually identifiable information about a U.S. citizen”).
- ◆ Assess, document, and comply with all applicable laws and policies.
- ◆ Establish data accuracy, quality, and retention procedures.
- ◆ Deploy adequate security measures to safeguard protected information.
- ◆ Implement adequate accountability, enforcement, and audit mechanisms to verify compliance.
- ◆ Establish a redress process consistent with legal authorities and mission requirements.
- ◆ Implement the guidelines through appropriate changes to business processes and systems, training, and technology.
- ◆ Make the public aware of the agency’s policies and procedures as appropriate.
- ◆ Ensure that agencies disclose protected information to nonfederal entities—including state, local, tribal, and foreign governments—only if the nonfederal entities provide comparable protections.
- ◆ It is recommended that state, local, and tribal governments designate a senior official accountable for implementation.<sup>443</sup>

This is accomplished through the implementation of a privacy policy<sup>444</sup> along with effective compliance reviews, audits, training, and supervision.

---

442 “Permission to access” private records can include consent by the individual and permission as provided through lawful regulatory procedures and/or the legal process.

443 *National Strategy for Information Sharing*. (2007). Washington, DC: Executive Office of the President, pp. 27–28. [https://www.dhs.gov/sites/default/files/publications/10\\_0924\\_NSI\\_National-Strategy-Information-Sharing.pdf](https://www.dhs.gov/sites/default/files/publications/10_0924_NSI_National-Strategy-Information-Sharing.pdf).

444 *The Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* may be downloaded at <https://bja.ojp.gov/library/publications/privacy-civil-rights-and-civil-liberties-policy-development-guide-state-local>.

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, access, expungement, and disposition.

The purpose of a privacy policy is to articulate publicly that the agency will adhere to legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.<sup>445</sup>

Assistance in developing policies that can aid law enforcement agencies and fusion centers develop best practices in the protection of privacy, civil rights, and civil liberties, is guidance provided by the Global Advisory Committee in the form of the:

- ◆ Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template<sup>446</sup>
- ◆ Privacy Civil Rights and Civil Liberties Compliance Verification for the Intelligence Enterprise<sup>447</sup>
- ◆ Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component<sup>448</sup>

It is clear that there are unequivocal expectations for law enforcement agencies to meet national professional standards for privacy and civil rights protections. As such, the obligation is not only to implement the policy, but also to provide training and supervision to ensure that the policy is effectively applied.

## LOCATIONAL PRIVACY

Information collection in law enforcement has changed with technology developing new privacy challenges, the vast majority of persons having cell phones that are automatically tracked by geographic location (and time) essentially monitoring the movement of people not only on a real-time basis, but also in data banks where these data are stored and available for review retroactively. Many modern motor vehicles also have Global Positioning Satellite (GPS) tracking technology in different forms, and people often make searches on their smartphones or use mapping applications which, once again, will provide data not only on a person's location but on where they plan to go. (These are referred to as "location-aware mobile technologies".) This occurs millions of times a day in tracking people who are lawfully going about their daily routines.

Of course, this information can also be valuable to law enforcement for intelligence and investigations. For example, it has become routine in homicide investigations to get a "cell tower data dump" from towers covering the crime scene as a tool for the investigation.<sup>449</sup> Whether there is live tracking of an individual or retroactive collection of a person's location through a "data dump," the issue of *locational privacy* is a significant issue that law enforcement must address in policy, practice, and training. Essentially, locational privacy refers to the ability of an individual to move in public areas with the expectation that, under normal circumstances, his or her location will not be systematically and secretly recorded and shared with law enforcement or the government for later use.<sup>450</sup>

---

445 Global Justice Information Sharing Initiative. (2006). *Privacy Policy Development Guide*. Washington, DC: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, p. 4–1.

446 <https://bja.ojp.gov/library/publications/fusion-center-privacy-civil-rights-and-civil-liberties-policy-development>

447 <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy%20civil%20rights%20and%20civil%20liberties%20compliance%20verification%20for%20the%20intelligence%20enterprise.pdf>

448 <https://bja.ojp.gov/library/publications/privacy-civil-rights-and-civil-liberties-audit-guidance-state-local-tribal-and>

449 <https://bostonbarjournal.com/2019/03/18/cell-tower-dumps/>

450 [https://itlaw.wikia.org/wiki/Locational\\_privacy](https://itlaw.wikia.org/wiki/Locational_privacy)

There are three fundamental types of locational privacy issues:

- ◆ **Identity privacy** ensures the protection of a person's identity/PII associated with a specific or inferred geographic location.
- ◆ **Position privacy** ensures the protection of a person's geographic location, whether in real time or in past movements.
- ◆ **Path privacy** ensures the protection of a person's geographic movements, such as the path followed while travelling or walking.

From a privacy perspective, these data are collected second by second by private companies, yet their value to law enforcement is quite clear for both investigations and intelligence. Civil libertarians are concerned about how law enforcement extracts and purges locational information collected on innocent persons and what safety mechanisms are in place to ensure the privacy of innocent people as well as to protect the privacy rights of persons whose behavior is suspected to have a criminal nexus.

The research shows there is some variance in the law on the issue. Clearly, the safest avenue to follow when using data from location-aware mobile technologies is to collect the information under the authority of a search warrant. Beyond that, a law enforcement agency should develop a policy on the use of data from location-aware mobile technologies, purging guidelines, and data protection.

## ISSUES OF INFORMATION COLLECTION AND SOCIAL MEDIA

The evolution of social media has changed the way we communicate. From 140-character tweets to blogs to manifestos posted online, people pour out their beliefs and opinions in text, audio, video, and images, even posting incriminating information. Law enforcement agencies have found social media to be a valuable source of information for a wide range of issues: understanding extremist ideologies; identifying threats ranging from school shootings to terrorist attacks; understanding the language and processes of various online contraband markets; and understanding conflicts and critical players among rival gangs are among the types of information that can be found in social media.

Among the concerns about the collection of information for the intelligence process have been questions about legal guidelines, particularly as related to free speech and privacy issues with respect to social media posts.

## SOCIAL MEDIA AND THE FIRST AMENDMENT

In the intelligence process, notably when dealing with ideological movements, one of the significant challenges is lawfully collecting information that may be indicative of a crime but also may be considered free speech. This is notably an issue with social media posts about a person's beliefs, which can be extreme, offensive, racist, demeaning, and unorthodox, but not unlawful. "Social media" is a collective label for a variety of applications and websites that allow users to create content—such as text, documents, links, images, audio, and/or video—to which other users are able to react. In addition, many social media platforms offer communications (or private messaging) options, some of which are encrypted. Existing social media platforms are constantly evolving, with new capabilities and expanding numbers of users, while new social media platforms with different application capabilities are introduced frequently. While there are publicly funded social media applications used for public information or for managing information related to government functions, social media platforms for the current discussion are typically owned by private companies whose target audience is the public—indeed, the global public. Social media includes not only those platforms commonly used on a daily basis by millions of people for communicating, marketing, and shopping (such as Facebook, Twitter, Instagram, or Tumblr) but also niche sites hosted on Web providers, such as the more extreme

imageboards of 4chan or 8kun.<sup>451</sup> Regardless of the platform, a core question is, What rights to free speech do users have when posting content on social media?

To begin, it must be recognized that there are few constraints on what people may post.

Constraints do not exist for social media. Anyone can post anything online with little fear of repercussion. The anonymous online environment can encourage inflammatory and shocking behavior. Individuals sometimes create screen names or new identities that allow them to act outside their normal inhibitions and sometime participate in caustic and less ethical activities they otherwise would avoid.<sup>452</sup>

But just because a person makes an anonymous, outrageous, or inflammatory statement found to be offensive and disrespectful, that does not mean it is necessarily unlawful. Should law enforcement give any attention to such statements or ignore them since they are lawful?

From an intelligence perspective, a great deal can be learned about an extremist ideology by reviewing social media posts that provide an insight into the belief system. Follow-up comments in the thread of a post can also provide insight about the extent and character of “like believers” as well as derivatives of the ideology. Beyond helping us understand extreme belief systems, social media posts may provide insights about threats. From a free-speech perspective, this is when care must be taken to assess whether language is materially threatening, not symbolic rhetoric—these fine distinctions can sometimes be difficult to determine and articulate.

When digital investigators are able to identify people who post anonymously, First Amendment protections obviously apply. Ironically, an anonymous post may be retained by law enforcement as an illustration of an ideology’s extreme beliefs. However, if the identity of the person who made the statements is known, the statements should not be retained by law enforcement absent a criminal predicate.

**First Amendment Protections of Speech.**<sup>453</sup> The Free Speech Clause of the First Amendment provides that “Congress shall make no law . . . abridging the freedom of speech” and applies to the states through the Fourteenth Amendment. The First Amendment generally applies only against government action. As the Supreme Court has



**CAVEAT ON FIRST AMENDMENT INFORMATION COLLECTION**

It is important to clearly articulate the potential criminal behavior and explain why the political or social views are relevant to that conduct. This information is needed to ensure that information collection aligns with statutory authorities and is supported by a valid law enforcement purpose. This approach guards against the creation and maintenance of dossiers on the exercise of constitutionally protected activities of individuals and organizations in the United States.

<sup>451</sup> 8kun was originally 8chan. In the aftermath of the back-to-back mass shootings on August 3 and August 4, 2019, in El Paso, Texas, and Dayton, Ohio, respectively, where posts related to the shootings were made on the site, it was taken down by the host service and resurfaced under the new name. <https://8kun.top/index.html>.

<sup>452</sup> Waters, G. (2012). Social Media and Law Enforcement. *FBI Law Enforcement Bulletin*, v81, 111, p. 2.

<sup>453</sup> Resources for law enforcement on First Amendment issues include: *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, <https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20Law%20Enforcement.pdf> and *Responding to First Amendment-Protected Events—The Role of State and Local Law Enforcement Officers Training*, [https://www.ncirc.gov/Training\\_First\\_Amendment.aspx](https://www.ncirc.gov/Training_First_Amendment.aspx).

said, “while statutory or common law may in some situations extend protection or provide redress against a private corporation or person who seeks to abridge the free expression of others, no such protection or redress is provided by the Constitution itself.”<sup>454</sup>

The Supreme Court has held that the government cannot restrict access to social media, since such access is protected by the First Amendment.<sup>455</sup> The court, however, has found speech that is obscene to be outside the purview of the First Amendment. The test for obscenity is overtly content-based, allowing the trier of fact to examine whether, “taken as a whole,” statements or pictorial depictions have “serious literary, artistic, political, or scientific value.”<sup>456</sup>

Words that are likely to illicit an “immediate breach of the peace,” such as a fight, are likewise unprotected. Whether a limitation on expression is constitutionally suspect must be assessed both by “the setting in which the speech occurs” and “on exactly what the speaker had to say.” First Amendment doctrine is not rigid; rather, it evolves through case-by-case developments. The specific words used and the context in which they are uttered are pertinent to First Amendment inquiry.<sup>457</sup>

For example, a person posts on a Darknet hackers’ forum programming code that she claims is a unique way to collect personal and financial information that could be used to commit financial fraud on computers of people who are using public Wi-Fi. While the hacker does not use the code herself to steal information, she says, “If anyone happens to use it, let me know how it works.” The acts of posting the code and making this comment are likely protected by the First Amendment. If, however, the hacker stated, “When you are successful at making some money, make a contribution to my Monero (cryptocurrency) account and I’ll make sure you get the next version of the code,” this suggestion would likely not be protected because it is overtly facilitating crime.

Mainstream social media companies have policies for users with respect to the types of content they can post. For example, Facebook’s policies are called “Community Standards”<sup>458</sup> and include the provision that:

...we remove language that incites or facilitates serious violence. We remove content, disable accounts, and work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety.” Facebook policies also state the company will “remove graphic images when they are shared for sadistic pleasure or to celebrate or glorify violence.”<sup>459</sup>

If a law enforcement agency contacted Facebook and told the company to take down a post that was promoting a potentially violent and extremist ideology and the company complied, that might be considered a violation of free speech. However, if Facebook employees discovered this same content and deleted it as a violation of company policy, it would not be a violation of free speech rights.

Federal law does not provide recourse for social media users who challenge a social media company’s policy or judgment about whether to remove a user’s content,<sup>460</sup> once again because only the government is prohibited by the Constitution from censoring speech, not a private individual or a company.

While users have brought lawsuits, they have been largely unsuccessful because First Amendment protections do not apply to private entities. Moreover, Section 230 of the *Communications Decency Act*, 47 U.S.C. § 230,

---

454 *Hudgens v. National Labor Relations Board*, 424 U.S. 507, 513 (1976).

455 *Packingham v. North Carolina*, 137 S.Ct. 1730 (2017). (North Carolina could not make it a felony for a sex offender to access a social networking site where minors are also users.)

456 Tsesis, A. (2017). “Social Media Accountability for Terrorist Propaganda.” *Fordham Law Review*, V86, I2, 605–631.

457 *Ibid.*

458 <https://www.facebook.com/communitystandards/>

459 [https://www.facebook.com/communitystandards/violence\\_criminal\\_behavior](https://www.facebook.com/communitystandards/violence_criminal_behavior)

460 Brannon, V. C. (2019). *Free Speech and The Regulation of Social Media Content*. Congressional Research Service, R45650. See also *Nyabwa v. Facebook*, 2018 U.S. Dist. LEXIS 13981, Civil Action No. 2:17CV24, \*2 (S.D. Tex.) (Jan. 26, 2018).

provides “immunity to providers of interactive computer services, including social media providers, both for certain decisions to host content created by others and for actions taken ‘voluntarily’ and ‘in good faith’ to restrict access to ‘objectionable’ material.”<sup>461</sup> In general, therefore, private social media companies are not guided by First Amendment protections; rather, they make their own decisions on whether or not to allow objectionable material, and users have few recourses if they find material objectionable and/or object to having their own material censored.

Virtually all major social media companies have a process for law enforcement to request records and posts of users.<sup>462</sup> While First Amendment protections do not apply to the platforms as private companies, information supplied to law enforcement by social media platforms must nonetheless pass the First Amendment test. That is, a social media company may take down extremist posts, identify the user, and give that information to law enforcement. However, law enforcement may not use or retain this First Amendment-protected speech unless there is a demonstrable nexus with criminal behavior at least meeting the standards of reasonable grounds.

**Guidelines on First Amendment Protection.** Law enforcement information collectors need to understand First Amendment protections as guiding principles to know what types of statements and social media posts can be collected.

- ◆ The First Amendment protects hate speech from government censorship unless that speech incites or is likely to incite imminent lawless action.
- ◆ The First Amendment protects pornography from government censorship unless it is obscene. Nudity alone is not sufficient to be considered obscene.<sup>463</sup>
- ◆ The First Amendment protects false statements of fact.
- ◆ The First Amendment does not protect true threats (serious expressions of intent to commit acts of unlawful violence) from government censorship.

First Amendment doctrine is not rigid; rather, it evolves through case-by-case interpretations. The specific words used and the context in which they are uttered are always pertinent to First Amendment inquiry. Thus, when collecting statements from social media that are deemed threatening, care must be taken not only to collect the exact language, but to provide a description and illustration of context as well as a description of the logic used to determine that the post was threatening. On this last point, many extremists’ movements have code words and phrases that have explicit meaning for those who follow the ideology. If these are used in a post, having rationale showing the meanings of the coded words and phrases<sup>464</sup> can help support the lawfulness of the information collection if challenged.

**The Impact of Social Media on Law Enforcement Officers and Agencies.** While the focus of this discussion has been on how law enforcement may use social media in the intelligence process, a slight distraction is warranted: What impact does social media have on a law enforcement agency and officers? Portrayals of a department and individual officers can impact their reputations, their effectiveness, their relationships with the community, and even the personal lives of officers, including their mental health and wellness.

There have been several instances in which hackers have posted names and personal data about thousands of police officers on social media sites.<sup>465</sup> In most cases, this is not public information, and having it exposed online increases the potential for threats to law enforcement officers, such as harassing threats to the officers and their families.

---

461 Ibid.

462 <https://www.facebook.com/records/login/> See also, <https://netzpolitik.org/wp-upload/2016/08/facebook-law-enforcement-portal-inofficial-manual.pdf>

463 Obscenity has been difficult to define legally and is inherently subjective, even with accepted legal tests. For a good discussion on the meaning and interpretation of obscenity, see <https://www.law.cornell.edu/wex/obscenity>.

464 As an example, see [https://www.adl.org/hate-symbols?cat\\_id%5B149%5D=149](https://www.adl.org/hate-symbols?cat_id%5B149%5D=149).

465 As one example, see <https://techcrunch.com/2019/04/12/police-data-hack/>.

Several characteristics combine to aggravate the threat from social media posts to law enforcement officers.<sup>466</sup>

- ◆ Constraints do not exist for social media. Anyone can post anything online with little fear of repercussion.
- ◆ The anonymous online environment can encourage inflammatory and shocking behavior. Individuals sometimes create screen names or new identities that allow them to act outside their normal inhibitions and sometimes participate in caustic and less ethical activities they otherwise would avoid.

Specific types of threats to law enforcement officers exist, such as:

- ◆ Threats to personal credibility through attacks on a police officer's character.
  - These can become troublesome in courtroom testimony and investigations as well as by diminishing public trust.
- ◆ Comments posted online can lead to disciplinary action.
- ◆ "Cop baiting" by use of videos of police officers can be harmful.
  - "Cop baiting could become so common that officers may not know whether they are facing a situation that is legitimate, staged, or exaggerated for someone else's benefit. This puts officers' personal and professional well-being at stake."<sup>467</sup>

Beyond these, there are completely different social media concerns related to officers' use of poor judgement when posting. For example, "The Philadelphia Police Department has pulled 72 officers off their regular duties as authorities investigate inflammatory social media posts. . . ." <sup>468</sup> Unfortunately, they are not alone. The Plain View Project<sup>469</sup> is a database of public Facebook posts and comments made by current and former police officers from jurisdictions across the country. While many of the posts are considered "occupational humor" or in bad taste rather than discriminatory, there are also posts with a cynically biased tone. The impacts these kinds of statements can have on a community are significant.

While law enforcement agencies cannot prohibit employees' uses of social media (U.S. citizens have freedom of speech), there should be policy, and perhaps training, on both the hazards to officers from social media and the potential harm that could be done by ill-advised officer posts.

## SOCIAL MEDIA AND THE REASONABLE EXPECTATION OF PRIVACY

One question commonly raised in the intelligence process is how to determine whether there is a reasonable expectation of privacy in social media posts. Password-protected sites, encryption, and law enforcement investigators making false profiles for access to sites, as well as officers making false statements in social media exchanges (essentially being "digitally undercover"), are among the issues that are raised. The Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."<sup>470</sup> This discussion considers whether it is a Fourth Amendment violation to the right of privacy for law enforcement officers to collect and retain information from social media posts as well as to pose as someone else on a social media site without a warrant.

---

466 Waters, G. (2012). "Social Media and Law Enforcement." *FBI Law Enforcement Bulletin*, v81, l11, p. 2.

467 Ibid.

468 <https://www.npr.org/2019/06/19/734241210/72-philadelphia-police-officers-placed-on-desk-duty-over-offensive-social-media>

469 <https://www.plainviewproject.org/>

470 Fourth Amendment. Legal Information Institute, [https://www.law.cornell.edu/constitution/fourth\\_amendment](https://www.law.cornell.edu/constitution/fourth_amendment).

**The Electronic Communications Privacy Act of 1986 (ECPA)**<sup>471</sup> establishes requirements and procedures for government actors intercepting communications as well as accessing stored digital information. Generally, the government cannot access privately stored information without obtaining a search warrant backed by probable cause, especially within the confines of a citizen’s own home. On the other hand, *citizens do not have a reasonable expectation of privacy against government searches or information gathering efforts that occur in public settings or where citizens expose private information to third parties*. Thus, a core issue is whether social media posts on secure, password-protected sites are considered public or private.

**The Third-Party Doctrine and Social Media Postings.** The Third-Party Doctrine severely limits Fourth Amendment protections by creating an exception to the reasonable expectation of privacy. First articulated in *Smith v. Maryland*,<sup>472</sup> the Third-Party Doctrine states that once an individual voluntarily agrees to share information with a recipient, the individual loses any reasonable expectation of privacy associated with that information. Applying the Third-Party Doctrine to social media information, individuals do not have a reasonable expectation of privacy regarding social media posts. As a result, government agents, analysts, or information collectors can gain access to posted social media information without meeting any probable-cause requirements. As soon as one posts information on a social platform, he or she discloses information to the third-party platform operator.

Furthermore, for most social networking posts, all of the members within a user’s social network also receive access to the published information. In “wall-to-wall” type conversations between two users (e.g., the person posting the information and the platform, such as Facebook), the rest of the members of the users’ social network function as third parties to whom the content publisher and the recipient have voluntarily disclosed information. Since the Third-Party Doctrine governs social media behavior, published content voluntarily shared within a private social network loses all reasonable expectation of privacy.

It is noteworthy that critics—on both the political left and right—argue that government monitoring of private social media pages constitutes a deeply invasive form of surveillance. Their argument continues that if government agents employ covert tactics to gain access to private social media networks, then the Fourth Amendment should control government use of that private social media information. There is a compelling argument that social media should be treated differently with respect to reasonable expectation of privacy, and there is value for the student of intelligence analysis to be aware of these arguments.

Despite this argument, however, the current law nonetheless holds that once an individual voluntarily exposes information to another party, that individual waives his or her privacy rights and cannot reasonably expect to limit the recipient’s usage of that information. As the Supreme Court articulated, “what a person knowingly exposes to the public, . . . is not a subject of Fourth Amendment protection.”<sup>473</sup> Under the Third-Party Doctrine, this use includes the ability to share information with the government.

**Password-Protected Sites.** Social media users have no reasonable expectation of privacy in their social media postings, even if they communicate their information behind password-protected sites. For the most part, courts allow the government to search private social media information without applying Fourth Amendment protections. The law treats “private” social media pages as deserving the same protections as if they were publicly posted on the Internet. The key is that the courts have noted that once posts are made on a social media platform, that constitutes the Third-Party Doctrine; hence protections are lost at that point. Under this logic, it is virtually irrelevant if the site is

---

471 Electronics Communication Privacy Act (1986). Justice Information Sharing <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>.

472 442 U.S. 735 (1979).

473 Katz v. U.S., 389 U.S. 347, 351 (1967).

password-protected. *Therefore, courts allow the government to search private social media information without any legally recognizable privacy protections.*<sup>474</sup>

**Application of Voluntary Consent to Social Media Postings.** Similar to the Third-Party Doctrine, individuals also lose a reasonable expectation of privacy when they consent to a government search of private information. Unlike the Third-Party Doctrine, which assesses the expectations of privacy of voluntarily disclosed information, the voluntary consent exception addresses consent to the search itself. As the Supreme Court declared in *Schneckloth v. Bustamonte*,<sup>475</sup> “it is . . . well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.” Thus, if an individual freely consents to a government search, the government may freely conduct one.

**Undercover/False Profile Use by Law Enforcement.** This consent remains doctrinally distinct from cases in which an individual does not knowingly consent to a government search but rather unknowingly agrees to the presence of an undercover government agent. *Undercover government information collectors may lawfully gain access based on a misrepresented identity.* If an individual offers lawful access to his or her private information, then that individual voluntarily assumes the risk that the access might expose the information to the government.

The government may attempt to access social networking data by creating a false account and asking an individual to permit entry into his or her social network.<sup>476</sup> Traditionally, parties have no legal recourse to misreading their friends or from falling prey to overtures by covert operatives. In *Hoffa v. United States*,<sup>477</sup> the court found that information voluntarily offered to an undercover informant as a result of misplaced confidence did not represent a legitimate privacy interest under the Fourth Amendment. Similarly, in *Lewis v. United States*,<sup>478</sup> the court reaffirmed the constitutionality of covert information gathering, relying on an important government interest in maintaining the ability to deploy undercover agents. Together, *Hoffa* and *Lewis* stand for the proposition that “a person does not have a privacy interest in the loyalty of her friends.” As such, when a social media user accepts a friend request from a covert government agent, that acceptance provides the same access as if the individual consented to expose his or her private social media publications to the government agent.<sup>479</sup>

Overall, the court holdings on the issue can be summarized in a few key points:

- ◆ Generally, social media postings are not protected by the Fourth Amendment.
- ◆ The Third-Party Doctrine generally holds that once a person posts information on a social media site, it is no longer a protected communication.
- ◆ This applies to password-protected pages/sites as well.
- ◆ Government agents may lawfully gain access to a person’s social media site through an undercover operation without a warrant.

---

474 When it comes to social media data, the extent to which individuals have a reasonable expectation of privacy in their social network publications determines whether courts will consider government searches of social data information “unreasonable” and therefore protected by the Fourth Amendment.

475 412 U.S. 218, 219 (1973). The *Schneckloth* consent focuses on voluntary and noncoerced consent for an agent to conduct a search.

476 While this typically violates the platform’s user policy, the violation has no Fourth Amendment implications.

477 385 U.S. 293 (1966).

478 385 U.S. 206 (1966).

479 Mund, B. (2018). “Social Media Searches and The Reasonable Expectation of Privacy.” *Yale Journal of Law and Technology*, 19(1), 238–273.

Courts have begun to discuss the appropriation of the old Third-Party Doctrine to the reasonable expectation of privacy in a digital world. Recently, the U.S. Supreme Court in *Carpenter v. United States*<sup>480</sup> held that the government violated the Fourth Amendment by accessing historical records of cell phones without a search warrant. This was a narrowly tailored decision and does not alter the discussion of the Third-Party Doctrine above.

People often mistakenly believe that their social discussions are private. As privacy scholars have noted, social networking users consistently underestimate the exposure inherent in the publication of social information.<sup>481</sup> Social networks create a sense of a private space, leading people to converse as if they were behind closed doors and not in the public view. Social conversations often fulfill the subjective prong of the Katz reasonable expectations test: While users know that the social networking platforms and other users within their networks have the ability to access their conversations, they assume that they have a right to privacy. The existing case law on the reasonable expectation of privacy in social media information finds that the Third-Party Doctrine results in no reasonable expectation of privacy in published social data. As a result of the lack of a reasonable expectation of privacy, the current case law allows government agents to employ information-gathering techniques on social data without triggering Fourth Amendment protections against unreasonable seizures. Recent legislative activity suggests a willingness to reconsider the Third-Party Doctrine's improper equation of privacy with secrecy.<sup>482</sup>

In summary, social media can be an extraordinarily valuable resource for the intelligence process. Because of the potential P/CRCL issues, it is important to have policy, training, and supervision in place to guide analysts and investigators in the proper methods of information collection and retention from social media platforms. With this in mind, the Global Advisory Committee published *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*,<sup>483</sup> which provides law enforcement and justice agencies with guidance and recommendations on issues to consider when developing a social media policy (or updating other relevant policies). The document focuses on access, use, information retention, and information dissemination that was collected from social media platforms for investigative and/or criminal intelligence purposes. It includes recommended policy elements, with an emphasis on potential privacy, civil rights, and civil liberties implications.

## 28 CFR PART 23—CRIMINAL INTELLIGENCE OPERATING POLICIES<sup>484</sup>

As is evident from the previous discussions, an important P/CRCL issue, most notably with respect to criminal ideological extremists, is whether law enforcement agencies are collecting and retaining PII of individuals who are involved in expressive activity, regardless of the forum. Often, it is difficult to distinguish between expressive activity and activity that is a precursor to a crime. If there are *behaviors* that suggest a crime is being planned, then the law enforcement agency has the responsibility to collect information to verify this and take appropriate action. It is not always immediately clear whether a crime is in the preparatory stage; hence criminal intelligence records are retained until the veracity of the threat is verified or dismissed. Because of this fine line, guidelines must be established as a matter of policy to ensure that the information is weighed and appropriately retained or destroyed, depending on what additionally collected information suggests about criminal liability.

---

480 585 U.S. \_\_\_\_ (2018) (Full citation not yet published at the time of this writing.)

481 As James Grimmelman has written, "Over a hundred million people have uploaded personally sensitive information to Facebook, and many of them have been badly burnt as a result. Jobs have been lost, reputations smeared, embarrassing secrets broadcast to the world." James Grimmelman, "Saving Facebook," 94 *Iowa L. Rev.* 1137, 1140 (2009).

482 Mund, B. (2018), op cit.

483 [https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing\\_a\\_policy\\_on\\_the\\_use\\_of\\_social\\_media\\_in\\_intelligence\\_and\\_inves.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_inves.pdf)

484 Readers should monitor the National Criminal Intelligence Resource Center website, accessible through the RISSNET portal and LEO, to monitor changes to the regulation. Also see [https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing\\_a\\_policy\\_on\\_the\\_use\\_of\\_social\\_media\\_in\\_intelligence\\_and\\_inves.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_inves.pdf).

The guiding regulation for managing a criminal intelligence records system for state, local, and tribal law enforcement agencies is the federal regulation titled Criminal Intelligence Systems Operating Policies, codified in 28 CFR Part 23. The regulation was created largely as a response to past practices of law enforcement agencies that collected and retained information about people based on their activities and/or expressed nontraditional beliefs that were often “extreme” or unpopular, but not criminal. The regulation seeks to provide procedural guidance for the management of criminal intelligence records systems that is consistent with constitutional guarantees. However, the federal government cannot mandate this regulation to independent state and local governments. As a result, adoption of the regulation is a condition that state, local, and tribal law enforcement agencies must meet to receive certain federal grant funds. That is, if a local police department accepted federal funds to purchase a computer system that would be used to maintain a multijurisdictional criminal intelligence records system, adoption of 28 CFR Part 23 would be a requirement to receive the funds.

Since this regulation was the only clear guideline for managing criminal intelligence records, it became the de facto standard that most agencies adopted, whether or not federal funds were received. Broad adoption of the regulation gained further momentum when the *National Criminal Intelligence Sharing Plan* (NCISP) recommended that all law enforcement agencies adopt 28 CFR Part 23. As a result, the regulation became a recognized national professional standard. Thus, while it is not required for every state and local law enforcement agency that has a criminal intelligence records system, it is good practice that is not only recommended by the NCISP but also by the Association of Law Enforcement Intelligence Units<sup>485</sup> (LEIU) and the International Association of Law Enforcement Intelligence Analysts<sup>486</sup> (IALEIA).

Agencies that embraced the regulation understood the regulatory language; however, it was not easily translated to policy. Moreover, the regulation had some gaps from an operational perspective. As a result, LEIU developed a model operational policy and procedures that translated both the language and the spirit of the regulation into something more easily adopted by a law enforcement agency. This practical interpretation of 28 CFR Part 23 is known as the *LEIU File Guidelines*.<sup>487</sup>

The *LEIU File Guidelines* represent an important step in the management of criminal intelligence records systems to ensure constitutional integrity. Based on litigation, experience, and concern expressed by civil libertarians, the management of a criminal intelligence records system must also consider elements beyond this practical interpretation of 28 CFR Part 23. Thus, the current best practice is an amalgamation of different sources relying on a conservative integration of accepted practice and regulation. Those sources include 28 CFR Part 23; the *LEIU File Guidelines*; established law of criminal evidence and procedure; and precedent from lawsuits arising from civil rights lawsuits involving criminal intelligence records. It should be noted that this information reflects general practice, not unique state laws that may have different requirements. The decision tree in Figure 7-1 is a visual representation of the following discussion as related to factors that should be considered before retaining information in a criminal intelligence record system. This conservative interpretation of these factors has been made to provide the safest guidance on information.

When information is collected, one of the first issues is to determine whether the information identifies either a person or an organization. Identity is not limited to a name but can include any descriptive information from which a reasonable person may identify an individual to the reasonable exclusion of others. For example, providing an address and a physical description of a person living at that address may constitute “identity.” Determining whether the information identifies an organization is somewhat more challenging, since 28 CFR Part 23 includes the names of organizations as protected criminal intelligence information but does not explicitly define the term “organization.” Based on precedent and experience, an organization is a distinguishable entity that has a definable

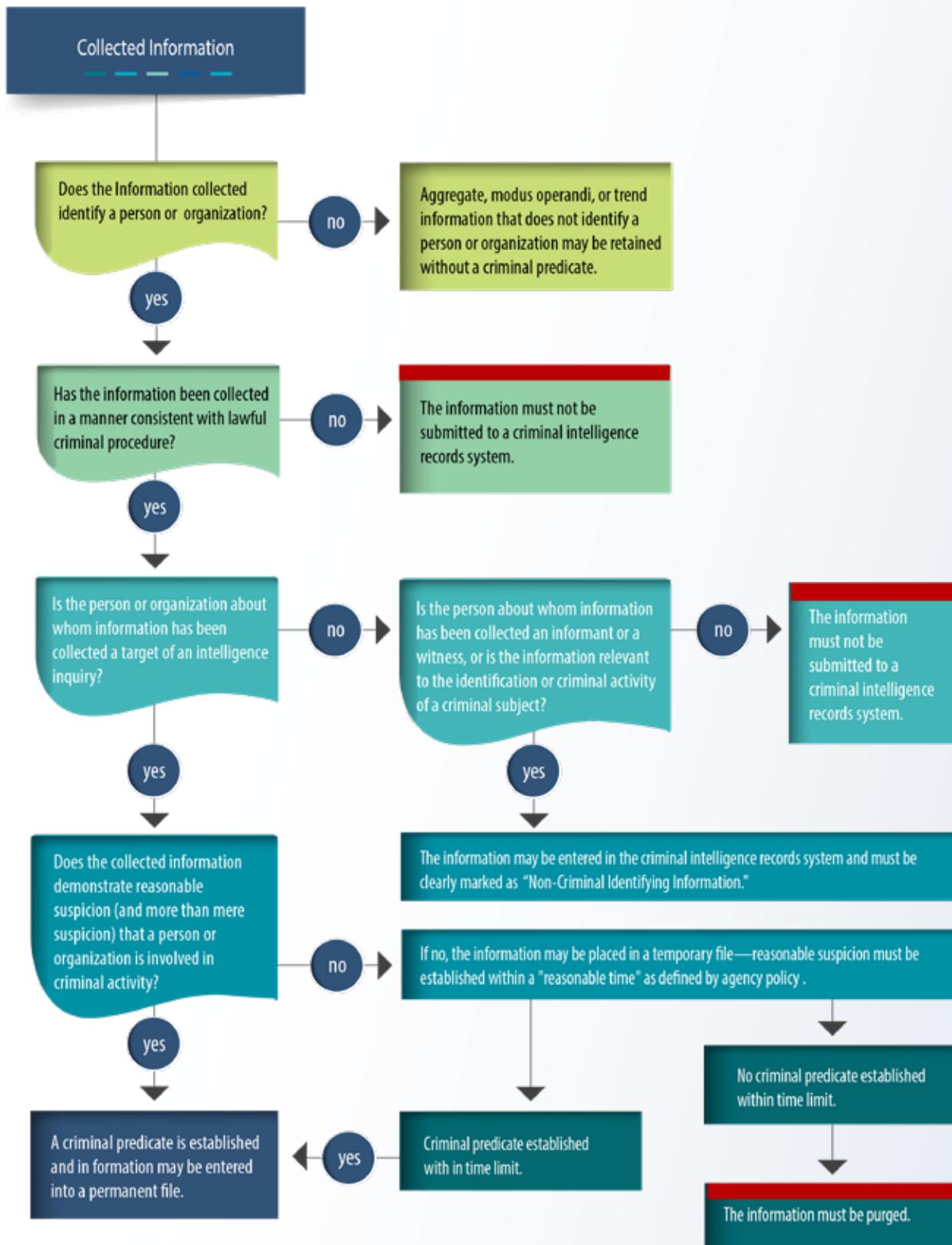
---

485 <http://www.leiu.org/>

486 <https://www.ialeia.org/>

487 The *LEIU File Guidelines* can be found at [http://it.ojp.gov/documents/LEIU\\_Crim\\_Intell\\_File\\_Guidelines.pdf](http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf).

FIGURE 7-1: INTELLIGENCE RECORDS SUBMISSION DECISION TREE



purpose, an identifiable organizational leadership structure, and a process or method for members to affiliate with the organization, albeit informal. Certain entities exist, such as sovereign citizen “collectives,” wherein people tend to affiliate with each other around a common ideology; however, such entities do not have the explicit characteristics defined above. In this illustration, the group is more of a movement than an organization. A movement that simply has a discernable ideology which people support, even as a collective, is not an organization.

A common question is why information that does not identify a person or organization can be retained in a criminal intelligence records system without establishing reasonable suspicion (i.e., a criminal predicate). Constitutional rights attach to individuals, not aggregate data, philosophical movements, criminal methods, or other information that is descriptive and useful for intelligence analysis but does not explicitly identify a person. Building on the concept from *Katz v. U.S.*<sup>488</sup> that the Fourth Amendment protects people, not places, the logic is extended that constitutional protections are afforded to individuals, not ideologies, aggregate behaviors, or other information not explicitly linked to individuals or organizations.

If the information does identify an individual or organization, the next step is to determine whether it was collected in a manner consistent with lawful criminal procedure. While this is not a requirement of 28 CFR Part 23, there is precedent in both criminal and civil law that suggests this is good practice for an agency to follow in deciding what information should be included in a criminal intelligence records system. There are several reasons: First, it is a constitutional protection that should be afforded to individuals, part of the fundamental fairness the American justice system affords to individuals under the due process clauses of the Fifth and Fourteenth Amendments. Second, the sole authority for law enforcement to have criminal intelligence and investigative functions is based on the statutory authority to enforce the criminal law. As such, there is a reasonable probability that criminal intelligence and investigative inquiries may lead to prosecution. If there are violations of criminal procedure, the evidence will likely be excluded from trial. Third, it strengthens the legal integrity of the intelligence or investigative inquiry, thereby reducing the probability of civil liability. Processes that carefully adhere to constitutional guarantees demonstrate good faith and, conversely, are an affirmative defense to negligence by the agency. Fourth, given the scrutiny of law enforcement intelligence and investigative practices by many in the civil rights community, having this step in the process reduces criticism of law enforcement activities. Finally, the practice is consistent with the Privacy Guidelines of the Information Sharing Environment (ISE), which state, in part:

- (i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and
- (ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.<sup>489</sup>

If information is collected about a person in the intelligence process and done in a manner consistent with constitutional standards, the agency needs to have a reason for collecting it. That reason is to further an inquiry about threats to the community in the hopes of preventing those threats from reaching fruition. As a result, information collected about individuals is based on the fact that they are either targets of an intelligence inquiry or have some type of information about a threat, even if they are not suspected of a crime. There is a need to lawfully retain both types of information in a criminal intelligence records system.

If a person is not the inquiry’s target but has critical information, “non-criminal identifying information” (NCI) may be entered into a criminal intelligence information file if it is relevant to the identification of the subject or the subject’s criminal activity, provided that: (1) appropriate disclaimers accompany the information noting that it is strictly

---

488 389 U.S. 347 (1967).

489 Program Manager for the Information Sharing Environment (September 4, 2006). *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment*. Washington, DC: PM-ISE, Office of the Director of National Intelligence, Guidelines 2.b.(i) and (ii).

identifying information carrying no criminal connotation; and that (2) if the information pertains to the political, religious, or social views, associations, or activities of the criminal subject, it must directly relate to criminal conduct or activity. For example, if a criminal subject is known to attend a particular church, synagogue, or mosque, inclusion of the religious affiliation in the system as NCI would be permitted only if it is directly related to the criminal conduct or activity, such as if the evidence indicates that the church, synagogue, or mosque is the site of the criminal activity. If an individual has material information about an acquaintance that supports the intelligence inquiry, this individual also may be entered into the criminal intelligence records system with a clear NCI identifier.

While 28 CFR Part 23 *does* allow the storage of NCI, the LEIU does not provide guidance for storing this information. Either approach is proper, but the *LEIU File Guidelines* are more restrictive.

If a person about whom information has been collected is the target of an inquiry, that information may only be retained if a *criminal predicate* is established. Determining a criminal predicate is a twofold process. First, there must be a nexus between a person's behavior and a crime or an organization's operations and involvement in criminal activity. Second, for information to be entered into a criminal intelligence records system as criminal intelligence information, the level of proof that must be met is reasonable suspicion. Under 28 CFR Part 23, "reasonable suspicion or criminal predicate" is established when information exists that establishes sufficient facts to give a trained law enforcement officer or an intelligence analyst a basis to believe that there is a reasonable possibility that an individual or organization is involved in or may become involved in a definable criminal activity or enterprise. Reasonable suspicion is more than mere suspicion. That is, a person's behavior may seem suspicious; however, that information must meet the criminal nexus and level-of-proof tests prior to being retained in a criminal intelligence records system.

Often, intelligence personnel receive a tip from the public or perhaps a suspicious activity report (SAR) from a patrol officer that a person is involved in a crime. Typically, there is no criminal predicate documented in such information. Practically speaking, an intelligence officer should not simply dismiss such information—indeed, the officer has the responsibility to determine the veracity of the information as it relates to community safety. The challenge to resolve is how the information can be lawfully retained if there is no criminal predicate. Since 28 CFR Part 23 does not address this circumstance, a practical interpretation of the regulation, which has been accepted by the courts, was created in the *LEIU File Guidelines*. The guidelines recommend establishing two types of intelligence files: "temporary" files and "permanent" files.

A *temporary file* is for information that does not rise to the level of reasonable suspicion but references an event or activity that indicates the possibility of criminal activity, such as a tip, a lead, or a SAR, none of which constitutes criminal intelligence information under 28 CFR Part 23. Since this information is not criminal intelligence information, it must be clearly labeled as such in a temporary file (and defined by policy), whether stored in the same database or accessed/disseminated with criminal intelligence information. The temporary file must have a policy-defined time limit for information to be retained (a generally accepted time limit is 60 days). The purpose of the temporary file is simply to have a place to store raw information while an inquiry is made to determine whether a criminal predicate can be established. If a criminal predicate is not established within the policy-defined time limit, the information should be purged.

Once a criminal predicate is established, the information is considered to be criminal intelligence information and may be stored in a *permanent file*. While it is commonly accepted phrasing, the term "permanent file" is somewhat misleading because the information in this file is subject to the 28 CFR Part 23 five-year, review-and-purge requirement.

**TABLE 7-2: QUESTIONS TO DETERMINE WHETHER RECORDS MUST COMPLY WITH 28 CFR PART 23 REGULATIONS**

<p>If the answer is “Yes” to any of the following questions, the records are considered criminal intelligence information and should be compliant with 28 CFR Part 23 regulations.</p>	<p>If the answer is “Yes” to any of the following questions, the records are most likely not criminal intelligence records for purposes of 28 CFR Part 23 regulations.</p>
<ol style="list-style-type: none"> <li>1. Are the records expressly called “intelligence records”?</li> <li>2. Are the records retained in the same records system as criminal intelligence records?</li> <li>3. Are the records kept primarily to assess threats with limited or no known criminal history of the intelligence targets?</li> <li>4. Are records being retained that identify individuals who or organizations that are suspected of criminal activity but are not the subjects of a current criminal investigation?</li> </ol>	<ol style="list-style-type: none"> <li>1. Are the records kept for investigative support of known crimes?</li> <li>2. Are the records kept in support of an active criminal investigation of a crime that has occurred and/or a known continuing criminal enterprise?</li> <li>3. Are the records kept to monitor the behavior of convicted criminal offenders (e.g., sex offenders), including persons on probation or parole, who are reasonably believed to pose a hazard to public safety?</li> <li>4. Are the records kept to identify individuals who are affiliated with a known crime group (e.g., persons who have tattoos known to be affiliated with a criminal gang)?</li> </ol>

It should be stressed that these processes and rules apply only to a criminal intelligence records system that is managed by a state, local, or tribal law enforcement agency. The guidelines of 28 CFR Part 23 do not apply either to a law enforcement agency’s investigative records or to a law enforcement agency’s records management system<sup>490</sup> (RMS). Often, there are questions about different types of records law enforcement agencies maintain that appear to be intelligence related but are often kept separately from the RMS. The most common questions are associated with field interview (FI) records and gang records. Because law enforcement agencies vary widely in these types of records, there are some general questions (Table 7-2) that can be asked to reasonably determine whether the records are criminal intelligence information for purposes of 28 CFR Part 23.

This discussion was intended to provide general information about the management and use of criminal intelligence records. Often, there are explicit questions about specific systems of a given agency. The best resource for these questions is the 28 CFR Part 23 Training and Technical Assistance program, funded by the Bureau of Justice Assistance.<sup>491</sup>

## FEDERAL CIVIL RIGHTS LIABILITY AND INTELLIGENCE<sup>492</sup>

As evidenced by a myriad of lawsuits—such as the New York and Denver cases—intelligence abuses have occurred. Unfortunately, critics often do not recognize the many changes that have occurred in law enforcement practices, coupled with the more specific professional direction of law enforcement intelligence. Higher educational standards, better training, adoption of ethical standards, and inculcation of law enforcement as a profession all indicate that

<sup>490</sup> The RMS typically stores information such as offense reports, arrest records, traffic accident records, miscellaneous investigations, and similar types of records kept in the daily operations of managing and responding to calls for service.

<sup>491</sup> For more information on this program, see <https://28cfr.ncirc.gov/>.

<sup>492</sup> Based in part on: Carter, D. L., & Martinelli, T. (2007). “Civil Rights and Law Enforcement Intelligence.” *The Police Chief*. (June).

the culture of law enforcement has changed, rejecting past practices that contributed to the previously mentioned abuses.

Beyond this history, the public generally has a misconception about the law enforcement intelligence function, envisioning it as involving community surveillance and acquisition of information by stealth. The public and the media need to be reassured that law enforcement intelligence processes will strictly subscribe to individual constitutional protections when information is collected, retained, and disseminated. Moreover, the public needs to understand that intelligence analysis is simply the scientific approach to problem solving, similar to the way analysis has been effectively used in evidence-based policing. The difference, however, is that evidence-based policing focuses on crime and community disorder, while intelligence focuses on threats and methods that may be used to prevent such threats from reaching fruition. In general, critics are not against using information gathering and analysis to prevent crimes and combat terrorism; rather, they simply demand that it be conducted pursuant to the constitutional parameters law enforcement officers are duty-bound to follow.

Because of the importance of protecting citizens' civil rights in all law enforcement activities, including intelligence operations, a remedy is available to citizens when an employee of a state, local, or, in some cases, tribal law enforcement agency violates individual civil rights guarantees under the color of law. As noted earlier, this remedy is Title 42 of the United States Code, Section 1983—*Civil Action for Deprivation of Civil Rights*<sup>493</sup> (frequently referred to as Section 1983).

Section 1983 lawsuits provide civil action for deprivation of constitutional and federal statutory rights by persons acting under the color of law. This statute was originally created as part of the Civil Rights Act of 1871, which was intended to curb oppressive conduct by government and private individuals participating in vigilante groups, such as the Ku Klux Klan. Section 1983 experienced a period of dormancy until 1961 and the landmark Supreme Court case, *Monroe v. Pape*, 365 U.S. 167 (1961), which gave individuals a federal court remedy as a first resort rather than only in default of (or after) state action. Today, Section 1983 lawsuits against

---

493 It should be noted that there are broad applications for Section 1983 lawsuits. The current discussion is limited to law enforcement intelligence issues. See <https://www.avvo.com/legal-guides/ugc/understanding-who-you-can-sue-under-section-1983>.

## HYPOTHETICAL ILLUSTRATION: FEDERAL CIVIL RIGHTS LIABILITY AND INTELLIGENCE RECORDS

How could a state or local law enforcement agency be held liable in a federal civil rights lawsuit (42 U.S.C 1983—Civil Action for Deprivation of Civil Rights) for improperly retaining personal identifying information in a criminal intelligence records system if the system's policies are 28 CFR Part 23- compliant?

- ◆ If the officers who were entering personal identifying information (PII) on “suspicious persons” in the criminal intelligence records system did not know that this information could not be entered because there was no criminal nexus, then there is potential negligence for failure to train.
- ◆ If a law enforcement employee did not understand that people involved in a protest were exercising their First Amendment right to expressive activity, then there is potential negligence for failure to train.
- ◆ If the training was not adequate to teach the officers to do the job properly, there could also be negligence for failure to train.
- ◆ If a supervisor did not monitor the information being entered into the system or did not take corrective action for improperly entered information, then there is potential negligence for failure to supervise.
- ◆ If a law enforcement employee clearly did not understand the policies of the intelligence unit or did not respect/follow the policies of the intelligence unit, or if the person was unable to adequately apply the policies, then there is potential negligence for negligent retention.
- ◆ If command-level personnel learned of improper information being collected and retained and did not take actions to correct the problem, then there is potential negligence for failure to direct.

law enforcement agencies most commonly involve First Amendment issues such as freedom of speech; Fourth Amendment issues such as search and seizure or use of force; and Fourteenth Amendment claims of due-process violations.

The key elements of the statute are as follows:

- ◆ Was the individual deprived of a constitutional or federally protected right?
- ◆ Did the law enforcement employee act under color of state law?
- ◆ Did the law enforcement employee fail to provide the standard of care owed to the individual?
- ◆ Was the law enforcement employee's conduct the cause of the individual's deprivation of constitutional right or federal statutory protection?
- ◆ Did the law enforcement agency fail to provide due diligence to ensure that agency policy and personnel practices protect civil rights?

For a successful civil rights case to occur, the plaintiffs must show that the law enforcement agency was negligent and that there was a pattern of misconduct associated with that negligence. This is typically achieved by providing evidence that the law enforcement agency repeatedly failed to provide due diligence in protecting individuals' civil rights. To accomplish this, the plaintiffs typically will attempt to demonstrate that the law enforcement agency showed deliberate indifference toward the protection of individuals' privacy and civil rights. In intelligence-related cases, this deliberate indifference may be a product of such things as:

- ◆ **Failure to train**—The agency does not provide intelligence training to all law enforcement personnel according to the recommendations of the *Minimum Criminal Intelligence Training Standards* promulgated by the Global Advisory Committee.
- ◆ **Failure to direct**—The agency does not provide clear policy and procedures on criminal intelligence information collection, retention, review, and dissemination.
- ◆ **Failure to supervise**—The agency does not adequately monitor the intelligence-related activities of personnel and/or does not enforce intelligence policy.
- ◆ **Failure to establish a privacy policy**—The agency does not articulate a clear policy to protect the privacy, civil rights, and civil liberties of persons as related to intelligence and records management activities.
- ◆ **Failure to adopt accepted professional standards of good practice**—The agency does not adopt the recommendations of the *National Criminal Intelligence Sharing Plan* or the *Intelligence Standards of the Commission on Accreditation for Law Enforcement Agencies*.

The resulting deliberate indifference is behaviors and processes that cause ongoing negligence in the protection of civil rights and civil liberties. Examples are:

- ◆ Retaining information that identifies people or organizations where there is no reasonable evidence supporting a criminal nexus.
- ◆ Profiling based solely on attributes such as race, religion, ethnicity, or country of origin rather than behaviors where there is a criminal nexus.
- ◆ Insinuating guilt by association or guilt based on mere suspicion.
- ◆ Inappropriate surveillance and information collection about an individual or organization.
- ◆ Knowingly keeping inaccurate information or information that should have been purged.
- ◆ Sharing information with other law enforcement agencies that identifies people or organizations with the

inference of a criminal involvement when a criminal predicate does not exist and/or without establishing the recipient's right to know and need to know the information.

As noted in the New York and Denver cases, the negative effects of a civil rights lawsuit can be costly, embarrassing, and disruptive of operations and can provide significant new restrictions on intelligence activities. As will be seen, this can be easily avoided with the proper policy, training, and supervision in place.

## STEPS TO ENSURE PROTECTION OF P/CRCL

An important tool for gaining citizen support for the intelligence function while minimizing accusations of impropriety is to ensure that the intelligence process is public and transparent. Providing some insight on the need for transparency was a press release by the ACLU of Massachusetts commenting on the opening of the Massachusetts Commonwealth Fusion Center. The statement expressed concern about the center's role and activities, specifically stating:

We need a lot more information about what precisely the fusion center will do, what information they will be collecting, who will have access to the information, and what safeguards will be put in place to prevent abuse.

These are reasonable and easily answerable questions. By simply providing this information to the community through a public information document or in town hall presentations, a great deal of conflict, criticism, and cynicism can be avoided. Uncertainty generates citizen anxiety, which translates into mistrust and allegations of impropriety. Educating the community about the intelligence process can reduce these tensions.

A wide range of issues have been discussed that represent legal flash points as related to law enforcement intelligence activities. A number of mechanisms may be easily implemented to ensure that civil rights protections remain intact while addressing the concerns of intelligence critics. (See Figure 7-2.)

1. **Policy Implementation.** Every law enforcement agency should implement a privacy policy, a security policy, and an accepted records management policy, such as the *LEIU File Guidelines*. Relying on policy models and policy development processes recommended by the Criminal Intelligence Coordinating Council (CICC) provides a solid foundation to demonstrate that the agency is following accepted national standards. This has a twofold advantage: First, it demonstrates to the community that the law enforcement agency has an intelligence policy foundation that is consistent with nationally recognized standards. Second, in case of a lawsuit, it can be used as an affirmative defense that the agency's policies are consistent with professionally recognized good practice.
2. **Training.** Training has three fundamental levels. First, every agency should follow the training recommendations of the NCISP and the *Minimum Criminal Intelligence Training Standards*,<sup>494</sup> which includes an intelligence awareness training program for all officers. Second, beyond these training standards, appropriate personnel within the agency need to receive training on agency policy and fusion center policy related to all aspects of the intelligence function. Special attention should be devoted to collection, retention, and dissemination of intelligence as well as special issues such as suspicious activity reports, intelligence related to juveniles, and other unique forms of information. Finally, as mentioned earlier, sworn personnel need to appreciate the gravity associated with constitutional rights violations as they pertain to intelligence gathering. Not unlike other critical issues in policing, a zero-tolerance policy toward such infractions is mandatory. This policy demonstrates to law enforcement personnel, as well as to the community, that civil rights violations will not be tolerated and that immediate disciplinary action will be taken.

---

494 <https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other>

3. **Supervision.** Good policy and training are only part of the equation. An agency must ensure that policies and procedures are being complied with as intended. If personnel are not following policy or are misinterpreting it, there will be a lack of systemic accountability and uniformity when it is time to mete out appropriate discipline. Street-level supervisors must be vigilant in their agencies' commitments to constitutional policing and must hold their subordinates to the highest standards of the profession, specifically when dealing with intelligence gathering. When patterns and practices of civil rights violations are uncovered over a period of time, plaintiffs' attorneys simply have to demonstrate to juries that street-level supervisors and their bosses knew or should have known of these violations and deliberately chose not to take disciplinary action. Deliberate indifference has proven to be very costly for law enforcement agencies that have opted to look the other way when citizens or fellow officers have reported possible civil rights violations.<sup>495</sup>
4. **Public Education.** A critical element of success for law enforcement intelligence is informing the public of law enforcement intelligence initiatives. Once again, there are two critical reasons. The first, as noted earlier regarding the ACLU's concerns, is to educate the public about the intelligence process. This eliminates erroneous assumptions and second guessing. Much of the lay public assumes that law enforcement agencies perform some type of widespread clandestine information collection and operate in a manner such as that of the intelligence community. Correcting this misperception can go a long way toward developing positive support for the intelligence process. The second benefit of public education is to inform citizens of the signs and symbols of terrorism to assist in the information collection process. For example, a trial program by the Regional Community Policing Institute (RCPI) at Wichita State University, in association with various police departments in Kansas, provided community training on terrorism and intelligence to educate the community about what to look for and how to report the information. Those attending the training were provided with a document called "Observe – Document – Report" and received instruction regarding indicators of behavior that were considered suspicious, what kinds of information needed to be documented, and how to report their observations to law enforcement. This model also helps citizens feel that they are contributing to the security of their own community and helps minimize the level of distrust toward their agency's efforts to combat crime and terrorism.
5. **Transparent Processes.** The intelligence function, like all other aspects of an American law enforcement agency, should have clearly understood and transparent processes. While certain information that is used in the intelligence function must be secured, the *process* that is used must be open. Critics of law enforcement intelligence argue that the intelligence process is secretive and that there is widespread spying on citizens.<sup>496</sup> This argument can be successfully countered by an agency that is open and transparent about how the intelligence process works, including relationships of an agency with other organizations, such as a fusion center. Without divulging the substance of intelligence records, an agency's efforts to educate its citizens on the procedural steps taken for information gathering and on its data storage policies can go a long way in achieving buy-in by the citizenry.
6. **Accountability Audits.** Periodic internal audits of the intelligence processes within any agency should be mandatory. A two-step process may be involved. First, a supervisor or manager must review and document the intelligence processes, following a recognized checklist of variables<sup>497</sup> written in the form of an inspection report. This would be followed by an external audit by a trustworthy, independent person such as a retired judge or other respected individual, who could review the report and ask challenging questions of both the auditor and the chief executive. Importantly, the audit should be viewed as a positive process designed to identify weaknesses or concerns that can be remedied. Taking proactive action such as an audit can ensure

---

495 Martinelli, T. J., & Pollock, J. M., "Law Enforcement Ethics, Lawsuits, and Liability: Defusing Deliberate Indifference," *The Police Chief* 67 (October, 2000) 10: 52–57.

496 As an illustration, the reader is urged to conduct an Internet search of the phrase "spy files." The results will provide insight on the breadth of concern about the intelligence process as well as the issues of concern to many citizens.

497 An example of an intelligence audit checklist can be found at [https://it.ojp.gov/documents/LEIU\\_audit\\_checklist.pdf](https://it.ojp.gov/documents/LEIU_audit_checklist.pdf).

that all aspects of the process are operating as constitutionally mandated. It can identify unforeseen problems and serve as affirmative evidence that the agency is operating in good faith and without malice.

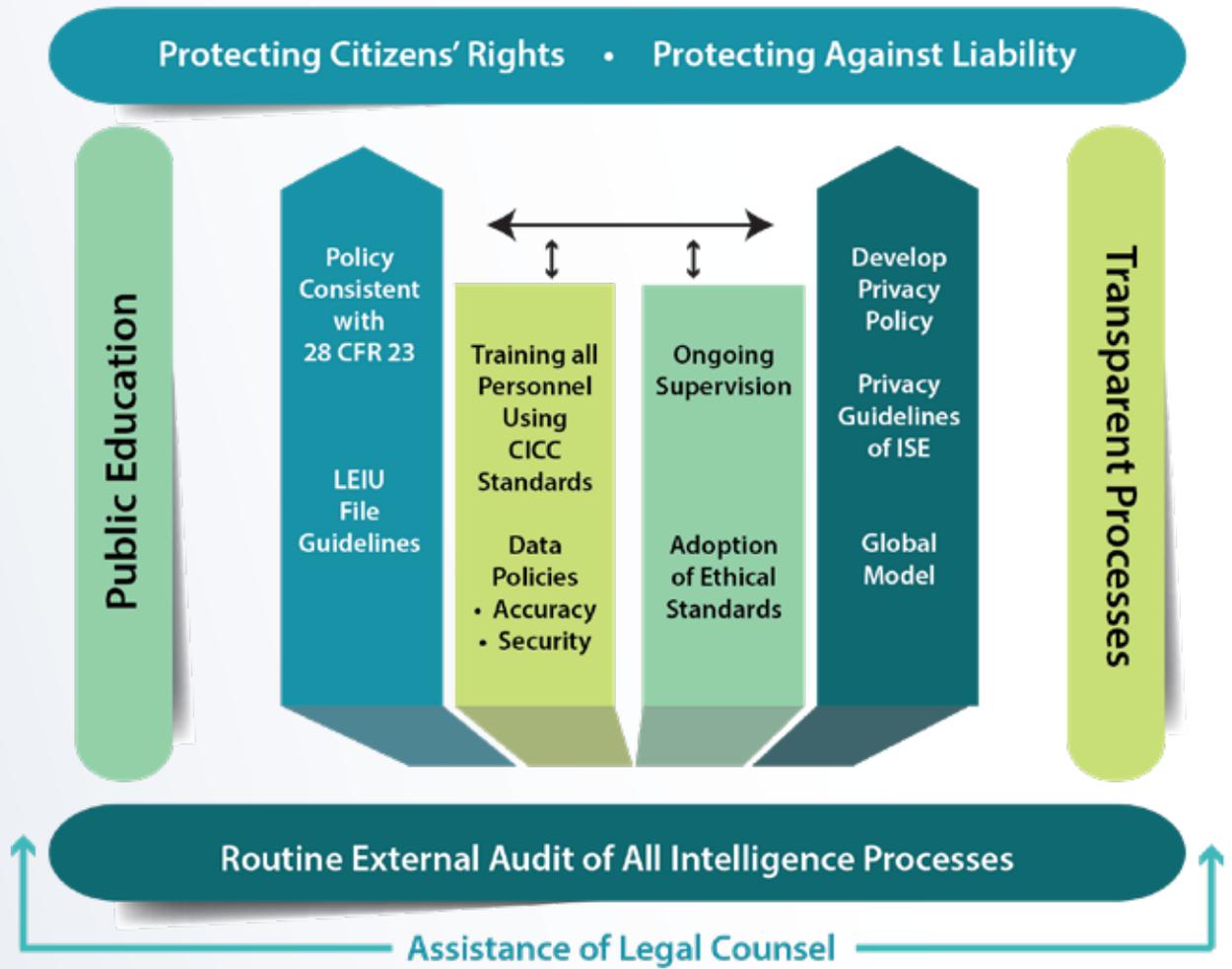
7. **Always Act in Good Faith.** All actions of the agency and its personnel should clearly demonstrate that the decisions made in the intelligence process are expressly intended to meet lawful standards. Good faith can be demonstrated in a variety of ways, including the implementation of policies and procedures, providing training to personnel, and ensuring that appropriate supervision is being performed. There are many areas of discretion in the intelligence process that often lack definitive legal guidance. If the framework is in place to aid personnel in making the best discretionary decision that protects individuals' rights while maintaining community safety, then the probability of negligence is reduced through these good-faith activities.
8. **Assistance of Legal Counsel.** The case law, as it pertains to police misconduct, relies on best police practice concepts such as good faith, reasonableness, and discretion without malice when judging an officer's conduct in hindsight. Juries typically do not want to find officers guilty for their alleged misdeeds or policy violations, and, more often than not, will give the officers the benefit of the doubt. But without clearly drafted policies, in-depth training scenarios, and evidence of an organization's strict compliance to constitutional law issues, an agency's legal counsel may find it difficult to defend one of its own against allegations of civil rights violations in a court of law. Competent legal counsel may be the best preventative measure agencies can use to prepare for litigation involving allegations of civil rights violations. Whether it be a sole practitioner or your insurance carrier's legal counsel, an attorney well-versed in municipal law, Section 1983 actions and police misconduct cases can assist in drafting your agency's privacy and security policies, as well as formulating the process for gathering and analyzing intelligence data.

With this approach, an agency can be assured that reasonable steps have been taken to comply with the latest Supreme Court rulings and the best police practices in accordance with society's increased need for vigilant police protection in this post-9/11 era.

## CONCLUSIONS

In the evolving world of information sharing that is increasingly being driven by intelligence fusion centers and technological development for information collection and analysis, law enforcement executives face new challenges in managing sensitive information and intelligence. Professional law enforcement accepts the responsibility for protecting citizens' civil rights while protecting the community. Moreover, this same environment will draw greater scrutiny from civil rights activists to ensure that the collection, retention, and dissemination of information by law enforcement agencies is done in a lawful manner. We have the knowledge and tools to protect both the community and citizens' rights. The intent of this discussion was to ensure that all of these tools are accounted for and placed in perspective.

FIGURE 7-2: STRATEGIES TO ENSURE CIVIL RIGHTS PROTECTIONS



## CHAPTER ANNEX 7-1: PROTECTING CIVIL RIGHTS AND IMMUNIZING AN AGENCY FROM LIABILITY IN THE LAW ENFORCEMENT INTELLIGENCE PROCESS

The following is a series of action steps and policy actions to ensure that law enforcement agencies protect privacy and civil rights. These same actions will also help protect agencies from civil rights lawsuits.

### PROTECTING CIVIL RIGHTS AND IMMUNIZING AN AGENCY FROM LIABILITY IN THE LAW ENFORCEMENT INTELLIGENCE PROCESS

Many citizens do not understand the law enforcement intelligence process and express concerns, often based on erroneous assumptions. As a foundation, a law enforcement agency should have a publicly available information document that answers these questions:

- ◆ What precisely does the intelligence unit or fusion center do?
- ◆ What types of information will be collected and retained in the intelligence records system by the law enforcement agency?
- ◆ Who will have access to the information?
- ◆ What safeguards are in place to ensure the proper and lawful use of the information?

Law enforcement agencies can take a number of actions to ensure the protection of citizens' civil rights. The application of some of these items will be dependent on the specific agency, its size, its jurisdiction, and whether it has a full-time intelligence unit or a part-time intelligence capacity. The items below provide a framework for ensuring that civil rights are protected and, consequently, limiting a law enforcement agency's civil liability.

- ☑ Adopt the *National Criminal Intelligence Sharing Plan* (NCISP).  
[https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/National%20Criminal%20Intelligence%20Sharing%20Plan%20version%202\\_0.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/National%20Criminal%20Intelligence%20Sharing%20Plan%20version%202_0.pdf)
- ☑ Adopt and adhere to the guidelines of 28 CFR Part 23.  
<https://28cfr.ncirc.gov/>
- ☑ Implement court-tested policies and procedures.  
<http://www.fas.org/jrp/agency/doj/lei/app.pdf>
- ☑ Provide a regular internal audit of the intelligence unit.  
[https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/leiu\\_audit\\_checklist.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/leiu_audit_checklist.pdf)
- ☑ Adopt a privacy policy.  
[http://it.ojp.gov/documents/Privacy\\_Civil\\_Rights\\_and\\_Civil\\_Liberties\\_Policy\\_Templates.pdf](http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf)
- ☑ Conduct a compliance review of the policy.  
<https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy%20civil%20rights%20and%20civil%20liberties%20compliance%20verification%20for%20the%20intelligence%20enterprise.pdf>
- ☑ Conduct an audit of the policy.  
<https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component>

- ☑ Adopt the *IACP Code of Ethics* and the *IACP Code of Conduct* as standards for ethical behavior.  
<https://www.theiacp.org/resources/law-enforcement-code-of-ethics>  
<https://www.theiacp.org/resources/policy-center-resource/standards-of-conduct>
- ☑ Appoint an external auditor to regularly review intelligence processes.
- ☑ Clearly identify lines of authority and responsibility for intelligence records management, including a two-stage review and approval process for records entry.
- ☑ Use the law of criminal evidence and procedure as a guideline for information management whenever in doubt.
- ☑ Have a documented process for a citizen's right to know and need to know.
- ☑ All personnel should sign a nondisclosure agreement related to information contained in the criminal intelligence records system.
- ☑ Always act in good faith. When a decision is made about information collection, retention, or dissemination wherein there is a lack of clarity due to unusual circumstances, write a justification for the decision and the rationale as part of the case file. This memo to the file ensures clarity of the facts and circumstances at the time for the decision in case that decision is challenged or reviewed.
- ☑ Review federal and state FOIA and privacy act guidelines and exemptions. Have a clear policy and procedure to handle FOIA requests, particularly as related to the intelligence function.
- ☑ Provide training for all of the above.

# CHAPTER 8

## THE INTELLIGENCE FUSION PROCESS



The intelligence fusion process represents an important chapter in the evolution of law enforcement intelligence. Fusion centers represent an intelligence structure for most state, local, and tribal law enforcement agencies to understand threats and share information. Contrary to intuition, the fusion process (developing intelligence from diverse resources) and the creation of fusion centers (the physical plant) are more involved than merely changing organizational functions of an existing law enforcement intelligence unit. Typically, they involve either the reengineering of the conceptual framework of the intelligence function in an agency or the creation of an entirely new entity. They require engaging a wide array of people and organizations to be partners as contributors and consumers of the intelligence function; they involve changing attitudes and processes of personnel; they require establishing new functional and information sharing processes among state, county, municipal, tribal, territorial, and federal law enforcement partners. Finally, they involve developing new agreements and functional relationships as well as new policies and processes and inculcating the intelligence-led policing (ILP)<sup>498</sup> philosophy.

As a result, the challenges are multifold, not the least of which is opening oneself and one's agency to organizational change. Most humans are dogmatic, resisting change. However, if incongruent past practices and erroneous assumptions are not eliminated from intelligence processes, the likelihood of success is diminished. The following discussion is intended to provide insight about different dimensions of the fusion process as well as concerns that have been expressed about intelligence fusion.

<sup>498</sup> See <https://www.policechiefmagazine.org/intelligence-led-policinga-strategic-framework/> and <https://leb.fbi.gov/articles/additional-articles/police-practice-intelligence-led-policing-connecting-urban-and-rural-operations>.

## HISTORICAL PERSPECTIVE

Initially, intelligence fusion centers were generally referred to as regional intelligence centers (RICs). They took different forms throughout the United States, with no single model for what an intelligence center did or how it should be organized. They evolved largely based on local initiatives as a response to perceived threats related to crime, drug trafficking, gangs, and/or terrorism within a geographic region. The intent was to marshal the resources and expertise of multiple agencies within that region to deal with cross-jurisdictional crime problems. In some cases, a region was defined as a county (e.g., Rockland County, New York Intelligence Center<sup>499</sup>); as a major urban area (e.g., Los Angeles Joint Regional Intelligence Center<sup>500</sup>); as a portion of a state (e.g., North Central Texas Fusion Center<sup>501</sup>); or it might encompass an entire state (e.g., Missouri Information Analysis Center<sup>502</sup>).

The earliest RICs began as the products of counterdrug initiatives starting in the 1980s. Indeed, the High Intensity Drug Trafficking Area (HIDTA) intelligence centers<sup>503</sup> served as models for successful structures and initiatives as well as identifying systemic issues that had to be overcome to make the intelligence centers functional. In the late 1990s, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) developed a number of programmatic activities to reduce gun violence. Emerging from these initiatives were ATF regional crime gun centers. In some cases, the centers were co-located with the HIDTA RIC and had a number of intelligence-related roles including analyzing trace data to identify gun traffickers, disseminating investigative leads, and coordinating with the HIDTA RIC to identify drug traffickers and their sources of guns.<sup>504</sup> In virtually all cases, both the HIDTA and ATF intelligence centers had a great deal of interaction with state, local, and tribal law enforcement agencies. The intent was to integrate—“fuse”—information from diverse sources to better understand and prevent multijurisdictional crime problems.

Hence the foundation was laid for intelligence centers. However, beyond idiosyncratic local crime issues, there was little incentive to expand the centers. Of course, this changed after September 11, 2001.

Because of their demonstrated successes and the information sharing challenges of counterterrorism, additional state and local entities embraced the concept and began developing their own centers. These centers were initially developed by state and local governments. However, the U.S. Department of Homeland Security (DHS) requested all states to develop a primary state fusion center that could help DHS fulfill one of its missions: to develop a two-way counterterrorism information sharing mechanism with state, local, and tribal law enforcement (SLTLE). While DHS provided grant funding to support the counterterrorism mission—and often assigned DHS intelligence analysts to many centers—the fusion center remained an entity of state or local government.

Recognizing that state and local fusion centers represent a critical source of local information about potential threats and a mechanism for providing terrorism-related information and intelligence from federal sources, the Program Manager for the Information Sharing Environment (PM-ISE), DHS, and the U.S. Department of Justice (DOJ) are taking steps to partner with and leverage fusion centers as part of the overall information sharing environment.<sup>505</sup>

Building on this observation, a report by the General Accountability Office (GAO) documented a number of federal efforts under way that were designed to support fusion centers and address challenges or obstacles identified by fusion center directors. These included the following:

499 <https://www.facebook.com/pg/Rockland-County-Intelligence-Center-556974424447741/about/>

500 <https://www.jric.org/>

501 [https://www.collincountytx.gov/sheriff/fusion\\_center/Pages/default.aspx](https://www.collincountytx.gov/sheriff/fusion_center/Pages/default.aspx)

502 <https://www.mshp.dps.missouri.gov/MSHPWeb/PatrolDivisions/MIAC/index.html>

503 <https://www.whitehouse.gov/ondcp/>

504 <https://crimegunintelcenters.org/atf/>

505 General Accountability Office. (October 2007). *Homeland Security: Federal Efforts are Helping Alleviate Some Challenges Encountered by State and Local Fusion Centers*. Washington, DC: General Accountability Office, GAO-08-35 Homeland Security, p. 2. <https://www.gao.gov/products/GAO-08-35>.

- ◆ DHS, FBI, and the PM-ISE have taken actions to assist fusion centers in gaining access to and managing multiple federal information systems, including classified systems.
- ◆ Both the DHS and FBI have committed to providing security clearances to state, local, and tribal fusion center personnel and reducing the time it takes for a clearance to be processed.
- ◆ DHS and FBI are assisting fusion centers in obtaining and retaining qualified personnel, both through assignments of federal employees to state fusion centers and through some DHS funding support.
- ◆ Federal funds in support of fusion centers have become more readily available and streamlined in operation to make grant awards faster and easier.
- ◆ Both DOJ and DHS have provided training and technical assistance in support of fusion center development and maturation.<sup>506</sup>

While significant progress had been made, many of the fusion centers and their governing officers believed that more development was needed for fusion centers to reach their full potential. While early development of procedures and processes was primarily coming from DHS and DOJ through the Criminal Intelligence Coordinating Council, in recent years the fusion center directors have been more proactive in developing their own training and processes through the National Fusion Center Association,<sup>507</sup> with advice and guidance from the CICC.

## REFINING THE FUSION CENTER CONCEPT

It was clear after the September 11, 2001 (9/11), terrorist attacks that there had been poor information sharing among and between all levels of law enforcement (and the Intelligence Community, as appropriate). As more information was learned about the terrorists and their minor encounters with state and local law enforcement in the weeks and months before the attacks, it was painfully evident that current information systems and processes were simply inadequate to deal with threats of this nature. It was also evident that if a diverse array of raw information was collected by different agencies, it would be essential to have a mechanism to provide data integration and analysis so its meaning would be of value to operational law enforcement personnel.

Increasingly, state and local law enforcement leaders recognized that the experiences of the HIDTAs and RICs could be applied to counterterrorism. Because of the need to have two-way information sharing directly with federal law enforcement and indirectly with the Intelligence Community, the fusion centers, the Federal Bureau of Investigation (FBI) and DHS reached out to each other to develop fusion centers more holistically. Indeed, “federal departments and agencies—including DHS, the FBI, and the U.S. Department of Defense (DoD)—launched efforts to develop strategies to incorporate these fusion centers into their information and intelligence activities.”<sup>508</sup>

The argument that fusion centers represent a vital part of our nation’s homeland security relies on at least four presumptions:

1. Intelligence, and the intelligence process, plays a vital role in preventing terrorist attacks.
2. It is essential to fuse a broader range of data, including nontraditional source data, to create a more comprehensive threat picture.
3. State, local, and tribal law enforcement and public sector agencies are in a unique position to make observations and collect information that may be central to the type of threat assessment referenced above.

<sup>506</sup> GAO, *Ibid.*, pp. 23–39.

<sup>507</sup> <https://nfcausa.org/?AspxAutoDetectCookieSupport=1>

<sup>508</sup> Program Manager-Information Sharing Environment (PM-ISE). (2006). *Information Sharing Environment Implementation Plan*. Washington, DC: PM-ISE, Office of the Director of National Intelligence, p. 18.

4. Having fusion activities take place at the subfederal level can benefit state and local communities and can possibly have national benefits as well.<sup>509</sup>

The initial focus of many new fusion centers was exclusively on terrorism, although most of the centers have broadened their focus to embrace all crimes and all threats. The reason was twofold: First, it was recognized that most terrorist acts have a nexus with other crimes. Hence, focusing exclusively on terrorism may cause us to miss some important indicators. Second, because there is a wide variety of crime, notably criminal enterprises, that is transjurisdictional and represents complex criminality,<sup>510</sup> it was recognized that the fusion process would be of value in dealing with these crimes as well.

Further evolution of fusion center responsibilities moved into the arena of an all-threats and all-hazards focus (in addition to all crimes). Inclusion of the all-threats and all-hazards approach came from two sources: One was recommendations from various organizations that fusion centers should focus on all threats and all hazards. The second source was from state or fusion center governing board mandates.

Recognizing that fusion centers were increasingly integrating the concepts of established law enforcement intelligence activities with the all-crimes, all-threats, all-hazards model of intelligence, the Homeland Security Advisory Council (HSAC) observed:

Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to State, tribal and local entities is that it will support ongoing efforts to address non-terrorism related issues by:

- Allowing State and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends;
- Supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and
- Improving the delivery of emergency and nonemergency services.<sup>511</sup>

There is no single model for a fusion center's structure or mission because of the diverse needs and environmental characteristics that affect the structure, processes, and products of a center. In states such as Texas and California, with their large land masses, large populations, and international borders, the structures and processes of fusion centers were necessarily different from those of predominantly landlocked rural states such as Wyoming or Nebraska.

A Congressional Research Service (CRS) report observed that questions have arisen regarding the current and/or potential efficacy of fusion centers. The report notes that in light of the growth of the fusion centers in state and local jurisdictions without a coordinated national plan, ". . . there appears to be no 'one-size-fits-all' structural or operational model for fusion centers."<sup>512</sup> From a centralized federal perspective—as reflected in the CRS report—the lack of a uniform model is assumed to be a significant flaw. However, the state and local perspective is somewhat different. Indeed, the ability to build a fusion center around grassroots needs is preferred. This permits state and local agencies to mold the fusion center into a model that best suits the needs and challenges that are idiosyncratic to each jurisdiction. As noted by Johnson and Dorn, describing the New York State Intelligence Center (NYSIC):

---

509 Masse, T., & Rollins, J. (September 19, 2007). "A Summary of Fusion Centers: Core Issues and Options for Congress." *CRS Report for Congress*. Washington, DC: Congressional Research Service, United States Congress, p. 3.

510 "Complex criminality" refers to criminal enterprises that are involved in a wide range of criminal activities in support of their core enterprises. For example, a drug trafficking organization may be involved in drug production, drug trafficking, money laundering, smuggling, corruption of public officials, fraud, and other offenses.

511 Homeland Security Advisory Council. (2005). *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Washington, DC: Department of Homeland Security, p. 2.

512 Masse, T., & Rollins, J., *Ibid.*, p. 18.

Creating one center for intelligence and terrorism information—to combine and distribute that information to law enforcement agencies statewide—prevents duplication of effort by multiple agencies. Additionally, one state fusion center serving the entire New York law enforcement community provides a comprehensive picture of criminal and terrorists networks, aids in the fight against future terrorists events and reduces crime.<sup>513</sup>

Within this same line of thought, fusion centers are also structured differently based on legislative or executive mandates. For example, Montana’s fusion center, Montana Analysis and Technical Information Center<sup>514</sup> (MATIC), focuses on all threats from homicide to Medicaid fraud; the New Jersey Regional Operations Intelligence Center (ROIC) includes emergency operations as well as intelligence fusion; the Massachusetts Commonwealth Fusion Center<sup>515</sup> (CFC) focuses on all crimes; and the Southern Nevada Counterterrorism Center<sup>516</sup> includes a focus on threats to the hotel and gaming industries. The variability of fusion center structures is broad because of functional necessity and the inherent nature of local control and states’ rights perspectives.

While the structure and operational processes of fusion centers may be different, national professional standards have nonetheless been articulated that outline good practice in critical administrative areas regardless of a center’s mission. That is the intent of the *Fusion Center Guidelines*.<sup>517</sup> (Table 8-1 shows the topics covered in the guidelines.)

Despite some criticisms, the fact that fusion centers are structured differently is not a weakness, but a strength. It exemplifies that each center is designed (a) to meet local and regional needs and (b) to best integrate the fusion center with existing organizational components (and priorities).

For example, the Michigan State Police (MSP) have widespread responsibility for both traffic and criminal law enforcement throughout the state. As such, the Michigan Intelligence Operations Center<sup>518</sup> (MIOC) is organizationally placed within the MSP. However, Florida has two predominant state law enforcement organizations: the Florida Highway Patrol, responsible for traffic law enforcement, and the Florida Department of Law Enforcement (FDLE), responsible for criminal law enforcement. As a result, the Florida Fusion Center<sup>519</sup> is organized as part of the FDLE Office of Statewide Intelligence. Hence, each state structured its fusion center in a manner that best fit existing organizational structures and functional responsibilities.

---

513 Johnson, B. R., & Dorn, S. (2008). “Fusion Centers: New York State Intelligence Strategy Unifies Law Enforcement.” *The Police Chief*. (February), p. 38.

514 <https://dojmt.gov/enforcement/investigations-bureau/>

515 <https://www.mass.gov/info-details/overview-of-the-department-of-state-polices-commonwealth-fusion-center>

516 <https://www.lvmpd.com/en-us/Pages/SouthernNevadaCounterTerrorismCenter.aspx>

517 The *Fusion Center Guidelines* are often referred to as “federal guidelines” because they are a product of the Global Intelligence Working Group (GIWG) of the Global Justice Information Sharing Initiative (Global), which is funded by and advisory to the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. However, it should be noted that the vast majority of GIWG members are from state, local, and tribal law enforcement agencies. Similarly, the group of subject-matter experts assembled to develop the *Fusion Center Guidelines* was predominantly composed of state, local, and tribal representatives. [https://it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)

518 [https://www.michigan.gov/msp/0,4643,7-123-72297\\_72370\\_72382---,00.html](https://www.michigan.gov/msp/0,4643,7-123-72297_72370_72382---,00.html)

519 <http://www.fdle.state.fl.us/FFC/FFC.aspx>

TABLE 8-1: TOPIC AREAS INCLUDED IN THE *FUSION CENTER GUIDELINES*

1. The *National Criminal Intelligence Sharing Plan* and the Intelligence Process
2. Mission statement and goals
3. Governance
4. Collaboration
5. Memoranda of understanding (MOUs)
6. Database resources
7. Interconnectivity
8. Privacy
9. Security
10. Facility, location, and physical infrastructure
11. Human resources
12. Training of center personnel
13. Multidisciplinary awareness and education
14. Intelligence services and products
15. Policies and procedures
16. Center performance measurement and evaluation
17. Funding

The point is that there are different operational and functional models of law enforcement throughout the United States. Fusion centers are no different, since they are an element of state or local government and have the responsibility to meet the unique needs of the jurisdictions they serve. As observed in one study:

Fusion centers [must identify] their mission and their customers, at what level of analytic product they will produce, and to whom. Not all fusion centers will need the same amount of strategic analysis or tactical analysis, but, in order to determine what to produce, they will have to understand their customers' needs and ensure they are educated so they understand the difference between the two products. Fusion centers will also need to determine how they will integrate the emergency responder community.<sup>520</sup>

It is, perhaps, this last point that will be the most challenging to define since "all-threats and all-hazards intelligence" and "meeting the needs of the emergency responder community" are not traditional roles for the law enforcement intelligence function. Some guidance to assist fusion centers in this area is being developed through the identification of baseline capabilities.

## BASELINE CAPABILITIES FOR FUSION CENTERS

As a result of national plans that seek to increase the efficiency and effectiveness of information sharing efforts, fusion centers serve as the interlink between SLTLE and the federal Information Sharing Environment (ISE) for the exchange of terrorism information.<sup>521</sup> As such, it was recognized that there was a need to define fundamental baseline operational capabilities that should be used by fusion centers, as well as major urban area intelligence units, to meet the information needs of all consumers of the various intelligence centers. Joint projects of the Global Justice Information Sharing Initiative, U.S. Department of Justice, and U.S. Department of Homeland Security have developed a wide range of resources and guidance documents to help develop and refine fusion centers' operations.<sup>522</sup> Baseline operational standards for the centers have received guidance provided in the *Fusion Center Guidelines*, the *National Criminal Intelligence Sharing Plan*, the Information Sharing Environment Implementation Plan, and the U.S. Department of Homeland Security's *National Preparedness Guidelines* and *Target Capabilities List*<sup>523</sup> (TCL). Relying on the guidance of these national standards, the baseline capabilities for fusion centers are also guided by the requirements of the National Strategy for Information Sharing and the Justice Department's information sharing philosophy and resources.<sup>524</sup>

520 Nenneman, M. (2008). *An Examination of State and Local Fusion Centers and Data Collection Methods*. Monterey, CA: A thesis prepared for the Naval Post Graduate School, p. 109.

521 See the White House policy for federal interaction with fusion centers and criteria for federal recognition of fusion centers: [https://www.dni.gov/files/ISE/documents/DocumentLibrary/RAC\\_final.pdf](https://www.dni.gov/files/ISE/documents/DocumentLibrary/RAC_final.pdf).

522 <https://it.ojp.gov/initiatives/fusion-centers>

523 <https://www.fema.gov/pdf/government/training/tcl.pdf>

524 <https://www.justice.gov/otj/information-sharing>

The baseline capabilities follow the structure of the *Fusion Center Guidelines* and represent a comprehensive articulation of functional standards and performance expectations. As a supplement to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*, baseline capabilities have been prepared for critical infrastructure and key resources<sup>525</sup> (CIKR). In addition, efforts have been made to integrate portions of the fire service with the intelligence function.<sup>526</sup> Each of these additional documents supports the all-threats and all-hazards responsibilities of fusion centers. The reader should monitor the Justice Information Sharing website<sup>527</sup> and/or the National Criminal Intelligence Resource Center<sup>528</sup> for related and newly developed resources.

## WHAT IS INTELLIGENCE FUSION?

According to the *Fusion Center Guidelines*, a fusion center is:

—defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The intelligence component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be “fused” with law enforcement data to provide meaningful information and intelligence about threats and criminal activity.<sup>529</sup>

The fusion process is an overarching methodology of managing the flow of information and intelligence across levels and sectors of government to integrate information for analysis.<sup>530</sup> That is, the process relies on active involvement of state, local, tribal, and federal law enforcement agencies—and sometimes non-law enforcement agencies and the private sector—to provide the input of raw information for intelligence analysis. As the array of diverse information sources increases, there will be more accurate and robust analysis that can be disseminated as intelligence products. Information fusion utilizes the intelligence process<sup>531</sup> for information management and analysis. The fusion center is the physical location where the fusion process occurs.<sup>532</sup>

While the term “fusion center” has been used widely, often there are misconceptions about the function of the center. Perhaps the most common of these is that a fusion center is a large room full of work stations where the staff is constantly responding to inquiries from officers, investigators, and agents. This vision is more accurately that of a watch center or investigative support center—not an intelligence fusion center. Another common misconception is that a fusion center is minimally staffed until there is some type of crisis wherein representatives from different public safety agencies converge to staff workstations to manage the crisis. This is an emergency operations center, not an intelligence fusion center.

---

525 [https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/baseline\\_capabilities\\_for\\_state\\_and\\_major\\_urban\\_area\\_fusion\\_centers0.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/baseline_capabilities_for_state_and_major_urban_area_fusion_centers0.pdf)

526 [https://swdiafc.files.wordpress.com/2015/09/terr\\_homelandseintelguide4firechiefs.pdf](https://swdiafc.files.wordpress.com/2015/09/terr_homelandseintelguide4firechiefs.pdf) All baseline capability annexes are listed at <https://www.dhs.gov/fusion-center-foundational-guidance>.

527 <https://it.ojp.gov/>

528 <https://www.ncirc.gov/>

529 Global Intelligence Working Group. (2005). *Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level*. Washington, DC: U.S. Department of Justice and U.S. Department of Homeland Security, p. 8.

530 *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview*. (2005) Lessons Learned Information Sharing, U.S. Department of Homeland Security. <https://www.hsdl.org/?view&did=765456>.

531 The intelligence process—also known as the intelligence cycle—involves the systemic steps used to collect, assess, analyze, and disseminate intelligence.

532 *Executive Summary: Fusion Center Guidelines*. (2005) Global Intelligence Working Group. [https://it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf).

In the purest sense, a fusion center is not an operational center, but a support center. It is *analysis*-driven. The fusion process proactively seeks to identify criminal and homeland security threats and stop them before they occur—prevention is the essence of the intelligence process. The distinction, however, is that the fusion center is typically organized by amalgamating representatives from different federal, state, local, and tribal law enforcement agencies (and, in some cases, the private sector) into one physical location. Each representative is intended to be a conduit of raw information from his or her agency who can infuse that agency-specific information into the collective body of information for analysis. Conversely, when a fusion center has intelligence requirements,<sup>533</sup> the representative is the conduit to the agency to communicate, monitor, and process the new information needs. Similarly, the agency representative ensures that analytic products and threat information are directed to the parent agency for proper dissemination. Agency representatives may be physically assigned to the center; however, a more common arrangement is that the agency representative—often called a fusion liaison officer<sup>534</sup> (FLO), terrorism liaison officer<sup>535</sup> (TLO), or intelligence liaison officer<sup>536</sup> (ILO)—performs his or her fusion center responsibilities along with other assignments at the home agency. The approach varies significantly depending on the characteristics of the jurisdictions, their threats, and, frankly, the commitment of an agency to be part of the fusion process.

In short, an intelligence fusion center must be able to: (1) access and explore all government databases, including intelligence, regulatory, and law enforcement; (2) integrate the information found in those databases; (3) make independent judgments about that information; and (4) provide warning.<sup>537</sup>

Obviously, not every law enforcement agency can contribute a person to work in the fusion center. Therefore, the centers must develop mechanisms for two-way information sharing that captures information from nontraditional collectors and provides threat-based intelligence and intelligence requirements back to those who have a need to know. As a result, multiple strategies and technologies need to be developed for diverse two-way information sharing.

For example, electronic two-way information sharing via the various secure electronic information systems—RISSNET,<sup>538</sup> LEEP,<sup>539</sup> HSIN,<sup>540</sup> NLETS<sup>541</sup>—can be very effective. In some systems, individuals beyond the law enforcement community who have a demonstrated need—including some private sector persons—may also have access to the system and use it for secure two-way information sharing. Another example is the New York Police Department’s Operation Nexus:

The New York City Police Department’s Operation Nexus is a nationwide network of businesses and enterprises joined in an effort to prevent another terrorist attack against our citizens. Our detectives [visit] firms that have joined us in this mutual effort. Members of Operation Nexus are committed to reporting suspicious business encounters that they believe may have possible links to terrorism. The NYPD believes terrorists may portray themselves as legitimate customers in order to purchase or lease certain materials or equipment, or to undergo certain formalized training to acquire important skills

---

533 “Intelligence requirements” consist of information that is needed to help make a comprehensive and accurate analysis of a threat. See Global Intelligence Working Group, Intelligence Requirements Subcommittee Report. *Recommendations for Intelligence Requirements for State, Local and Tribal Law Enforcement Agencies*. (October 2005).

534 Saupp, K. (February 2010). “Fusion Liaison Officer Programs: Effective Sharing of Information to Prevent Crime and Terrorism.” *Police Chief Magazine*. <https://www.policechiefmagazine.org/fusion-liaison-officer-programs/>

535 For example, see Orange County Intelligence Assessment Center’s description of its TLO program at <https://ociac.ca.gov/default.aspx?menuitemid=307&AspxAutoDetectCookieSupport=1>.

536 <https://cfix.ocso.com/ILOProgram/tabid/537/Default.aspx>

537 Wortzel, L. (2002). “Creating an Intelligent Department of Homeland Security.” *Executive Memorandum 828*. Washington, DC: Heritage Foundation. <https://www.heritage.org/homeland-security/report/creating-intelligent-department-homeland-security>.

538 Regional Information Sharing Systems Secure Cloud, <https://www.riss.net/>.

539 Law Enforcement Enterprise Portal (operated by the FBI), <https://www.fbi.gov/services/cjis/leep>.

540 Homeland Security Information Network, <https://www.dhs.gov/homeland-security-information-network-hsin>.

541 International Justice and Public Safety Network, <http://www.nlets.org/>.

or licenses. . . . Through Operation Nexus, the NYPD actively encourages business owners, operators, and their employees to apply their particular business and industry knowledge and experience against each customer transaction or encounter to discern anything unusual or suspicious and to report such instances to authorities.<sup>542</sup>

Another model has been adopted throughout the United States. Developed in Los Angeles, California, the Terrorism Early Warning (TEW) group has multiple functions, including supporting the intelligence fusion center.

The Los Angeles TEW includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-, and post attack) specifically tailored to the user's operational role and requirements. The TEW bridges criminal and operational intelligence to support strategic and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies.<sup>543</sup>

Regardless of the method of information sharing, the key factors are that: (1) There must be diverse raw input; (2) it must be analyzed; and (3) actionable intelligence output must be shared with appropriate consumers.

## WHY FUSION CENTERS?

The heart of good intelligence analysis is to have a diverse array of valid and reliable raw information. The more robust the raw information, the more accurate the analytic output (i.e., intelligence) will be. If one thinks of information input in terms of bandwidth, the typical law enforcement intelligence unit has a narrow bandwidth. That is, information is gathered from a fairly narrow array of sources, thereby limiting both the quality of the analysis and the ability to see the “big picture” of a criminal enterprise. Quite simply, the more limited the input of raw information, the more limited the quality of intelligence. However, if the number of sources is broadened to include a wide range of agencies representing much broader geographic and jurisdictional parameters, then the bandwidth is much wider. With wider bandwidth, there is a greater (and more diverse) information flow. Therefore, with greater information flow, the analysis becomes more accurate and utilitarian. As the quality of analysis increases, the ability to prevent or mitigate the threats of a terrorist or criminal organization increases exponentially.

Analyses of both law enforcement and national security intelligence operations found a problem that has been referred to as the “stovepipe” of information in agencies.<sup>544</sup> That is, each agency would develop a large body of information and analytic products that would be retained within the agency and rarely shared with other agencies. Analysis was generally limited to the information that came from internal sources, and dissemination of information was also largely internal. As a result, while agencies were developing information, it was simply being stacked and stored in isolation, as in a stovepipe. Current thought recognizes that far more value can be derived from information that is widely shared for analysis—information from one agency may be a key in learning about a threat when integrated with information another agency. Hence, there was a need to “fuse” as much information as possible.

---

542 <https://www.nypdshield.org/public/nexus.aspx>

543 Sullivan, J. P. (2005). *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence*. A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada, p. 1.

544 As an illustration, see Kindsvater, L. C. (2003). “The Need to Reorganize the Intelligence Community.” *Studies in Intelligence*. Vol. 47, No. 1, <https://www.cia.gov/static/178addc9e60e41310b05c2024fdbb5b1/Need-Reorganize-Intel-Community.pdf>.

As noted in a report from the Heritage Foundation, a fusion center would not simply duplicate the activities of existing agencies but would enhance and improve their efforts by providing a service that is not available elsewhere.<sup>545</sup>

Another perspective on the development of fusion centers observed that:

Conceptually, fusion centers differ from [state police intelligence units] in that they are intended to broaden sources of data for analysis and integration beyond criminal intelligence, to include federal intelligence as well as public and private sector data. Furthermore, fusion centers broaden the scope of state and local analysis to include homeland security and counterterrorism issues.

Despite being an expansion of existing sub-federal intelligence/information activities, fusion centers represent a fundamental change in the philosophy toward homeland defense and law enforcement. The rise of fusion centers is representative of a recognition that non-traditional actors— state and local law enforcement and public safety agencies—have an important role to play in homeland defense and security.<sup>546</sup>

In exploring the need and structure of fusion centers, a project by the Police Executive Research Forum (PERF) identified five critical questions:<sup>547</sup>

1. Why do we need a fusion center? Fusion centers embody the core function of collaboration, and as demands increase and resources decrease, fusion centers serve as effective tools to maximize available resources and build trusted relationships. What distinguishes fusion centers from intelligence units within local law enforcement agencies is that fusion centers synthesize data gathered from multiple sources and disciplines.
2. What is a fusion center’s mission? While opinions on the topic vary, many in the law enforcement community believe it makes more sense to establish a fusion center with a broader mission and scope, i.e., implement an all-crimes or all-hazards approach, while still maintaining the unique capability to monitor terrorist activity. The value of an all-crimes center is that it increases the ability of law enforcement to detect the traditional crimes that ultimately may be precursors of terrorist activity. The underlying purpose and goal of a fusion center is to provide law enforcement agencies with analysis of local, state, and regional activities. Local law enforcement agencies, however, must do their part by feeding information to the center.
3. Who governs the fusion centers? Most fusion centers established memoranda of understanding with participating agencies and appointed a governing board of representatives from these agencies to provide oversight and ensure adherence to policies, according to the recommendations put forth in the *Fusion Center Guidelines*.
4. What are the major functions and services fusion centers perform? Fusion centers are intended to be analytical support centers for law enforcement and other public safety agencies. A fusion center serves as a repository for all information available from open source and law enforcement agencies throughout the state or region. Fusion centers and the agencies they serve work together to determine the best method for dissemination of center analysis and products.
5. How does law enforcement define value in its relationship with fusion centers?
  - Providing daily information to law enforcement agencies
  - Interpreting diverse threat information from a local perspective
  - Providing timely actionable intelligence
  - “Connecting the dots” from diverse jurisdictions that affect a local area

---

545 Dillon, D. R. (2002). “Breaking Down Intelligence Barriers for Homeland Security.” *Backgrounder #1536*. Washington, DC: Heritage Foundation. <https://www.heritage.org/homeland-security/report/breaking-down-intelligence-barriers-homeland-security>.

546 Masse, T., & Rollins, J., *Ibid.*, p. 2.

547 *What is a Fusion Center?* (2008). Washington, DC: Police Executive Research Forum.

- Serving as a “one-stop shop” for threat information
- Managing diverse pieces of information in a coherent form for local law enforcement agencies

## FUSION CENTERS AND THE CRIME LABORATORY: AN ANALOGY

The relationship between a fusion center and a law enforcement agency may be seen in a somewhat familiar analogy: the crime laboratory. The vast majority of law enforcement agencies do not have a crime lab—just as they do not have an intelligence unit—however, they frequently need forensic analysis of evidence for cases. To use the crime lab effectively, each agency must have some type of forensic capacity so that physical evidence can be collected properly (i.e., to prevent contamination and maintain the integrity of the chain of custody). The agency also must have established a relationship with the crime lab and know the processes for submitting evidence for analysis.

For most agencies, a state crime lab is used. While a small agency may only use the laboratory periodically, in those few instances in which forensic analysis is needed, it is essential that the local agency have trained personnel and have access to appropriate resources to use the crime lab’s services expeditiously and effectively. Table 8-2 provides a comparative series of factors that are analogous between crime laboratories and fusion centers.

The purpose of this analogy is to illustrate that there is a precedent for many organizational processes and practices that are required for fusion centers. Building on these experiences can make integration of the fusion center into law enforcement agency operations much easier.

TABLE 8-2: ANALOGY OF CRIME LAB AND FUSION CENTER

CRIME LABORATORY	FUSION CENTER
<ul style="list-style-type: none"> <li>◆ Central laboratory operated by the state.</li> <li>◆ Each law enforcement agency must have a capacity to collect physical evidence to prevent contamination.</li> <li>◆ Retain physical evidence to meet chain-of-custody requirements.</li> <li>◆ Certified agency participant with crime laboratory to submit evidence for analysis.</li> <li>◆ Forensic analysis is performed by specially trained analysts.</li> <li>◆ Crime lab provides analytic results of physical evidence.</li> </ul>	<ul style="list-style-type: none"> <li>◆ Fusion center operated by the state.</li> <li>◆ Each law enforcement agency must have a capacity to lawfully collect raw information, building on the criminal predicate.</li> <li>◆ Retain information to meet 28 CFR Part 23 guidelines.</li> <li>◆ Certified as a fusion center participant to establish the right to know and the need to know to receive intelligence products.</li> <li>◆ Intelligence analysis is performed by specially trained analysts.</li> <li>◆ Fusion center provides intelligence products.</li> </ul>

## FUSION CENTERS AND THE INFORMATION SHARING ENVIRONMENT (ISE)

In the fusion center development process, the *ISE Implementation Plan* embraced the growth of fusion centers as a critical linchpin to serve as information clearinghouses among federal entities (both federal law enforcement and the Intelligence Community), nonfederal law enforcement, and the private sector.

[M]any States and localities emphatically moved to create and invest in fusion centers in the post-9/11 environment. These fusion centers now play a prominent role in collecting, analyzing, and sharing terrorism information. Individually, these centers represent vital assets for collecting terrorism-related information. Collectively, their collaboration with the Federal government, with one another (State-to-State, State-to-Locality), and with the private sector represents a tremendous increase in both the

nation’s overall analytic capacity and the multi-directional flow of information. It is important to note that these centers are not homogenous—considerable variations exist in terms of operations and mission focus (e.g., homeland security, law enforcement, emergency response). To date, more than [70] such centers have been established across the United States, and significant effort has gone into developing and adopting standards to facilitate easier information access, sharing, and use.<sup>548</sup>

To further this plan, the PM-ISE helped establish a National Fusion Center Coordination Group, led by DHS and DOJ, to identify federal resources to support the development of a national, integrated network of fusion centers.<sup>549</sup> Moreover, the ISE. . .

. . . recognizes the “all-crimes and all-hazards” nature of State and local sharing, where SLT organizations may share and fuse together multiple types of information to address a variety of needs including law enforcement, preparedness, and response and recovery. In many instances, this information may not initially be recognized as terrorism information, but may be information that could ultimately prove crucial in preventing, preparing for, or responding to terrorism. The ISE focus on terrorism information will not impede or interrupt these additional fusion center functions.<sup>550</sup>

When created, the National Fusion Center Coordination Group served a critical role for development of fusion centers; however, its efforts have largely been taken over by the National Fusion Center Association.<sup>551</sup>

## OPERATIONALIZING THE FUSION PROCESS

As depicted in Figure 8-1, there are three critical focal areas to make the integrated information sharing strategy functional. While all of the factors are essential, the fusion center plays a uniquely critical role.

The process begins with the fundamental step, noted earlier, of developing an intelligence capacity in all state, local, and tribal law enforcement agencies, regardless of agency size. The intelligence capacity must be integrated with a law enforcement agency’s proactive participation with the fusion center. The more agencies that participate as fusion center partners, the greater the value of the center. As noted by the PM-ISE, “state and major urban area fusion centers will be central to implementation at the State and local levels. . . .”<sup>552</sup> Hence, creation of the fusion center is only one ingredient—it is essential to have widespread participation.

The outer band of Figure 8-1 is the federal ISE, which consists of both the Intelligence Community and federal law enforcement. Both deal with national security and homeland security, from a broad perspective and typically at a classified level. The challenge is to share appropriate threat information with local law enforcement. Similarly, when local law enforcement discovers information that is valuable to the ISE, there must be a mechanism to effectively share the information. The primary state fusion center is intended to fulfill these roles.

---

548 PM-ISE, (2006). Ibid., pp. 7–8.

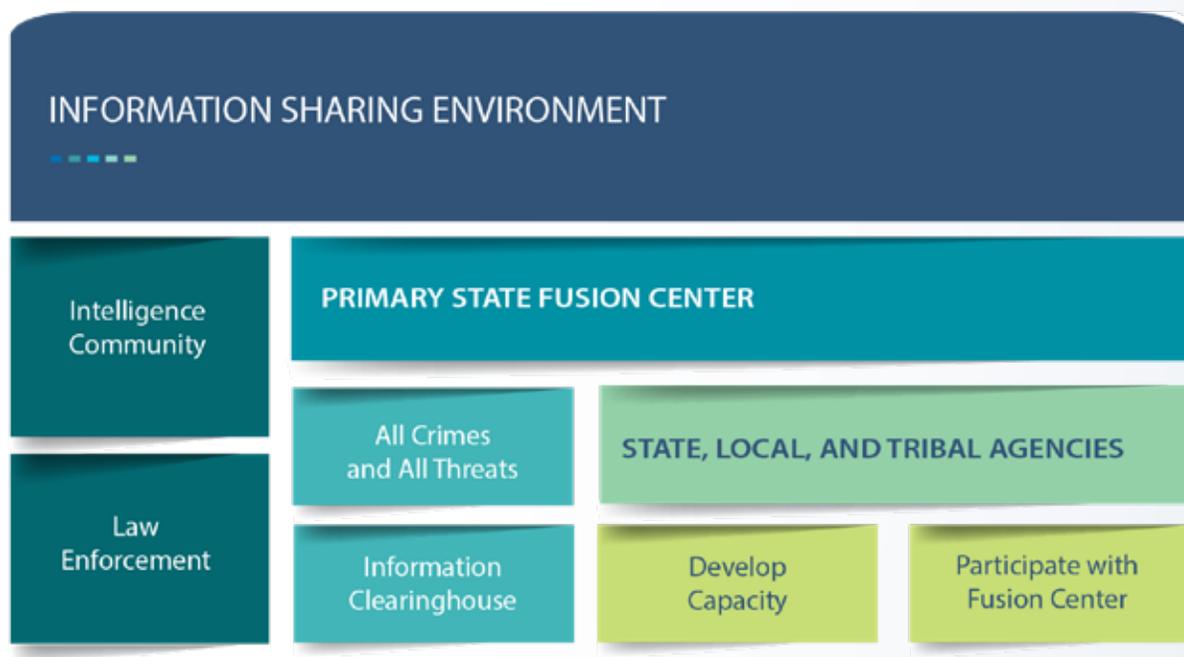
549 GAO, Ibid., p. 12.

550 PM-ISE, (2006). Ibid., p. 11.

551 <https://nfcausa.org/>

552 Program Manager-Information Sharing Environment. (2007). *Common Terrorism Information Sharing Standards (CTISS) Program Manual*. Washington, DC: PM-ISE, p. 18.

FIGURE 8-1: ORGANIZATIONAL INTERRELATIONSHIPS AND RESPONSIBILITIES FOR THE FUSION PROCESS AND ISE



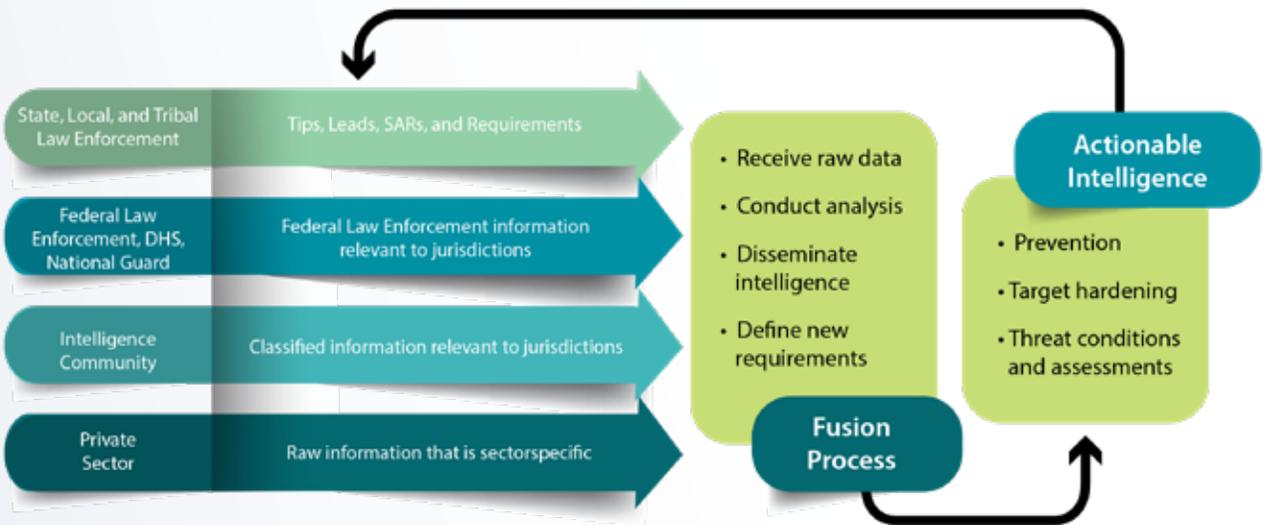
The fusion center is envisioned to serve as an information clearinghouse between all levels of law enforcement intelligence. Typically, the center will have representatives from all levels of government, experienced analysts, personnel with federal security clearances, and access to a wide range of information systems, including classified systems at most primary state fusion centers. With this foundation, the fusion center can disseminate critical intelligence to local and tribal partners as well as pass critical raw information to federal agencies that is collected at the local, tribal, and private levels.

A simplified version of the fusion information sharing process to accomplish these objectives is depicted in Figure 8-2. A fundamental objective is to gain buy-in by all critical sectors within a state: law enforcement, federal partners within the state, and the Intelligence Community,<sup>553</sup> as applicable to each state and the private sector. Hence, the fusion process receives input (both raw data and intelligence, as indicated in the block arrows of Figure 8-2) from a variety of agencies. The analysts then integrate this diverse data and provide analytic output that may include information for prevention, target hardening, or threat assessment. In addition, the analysts may define further intelligence requirements. After analyzing and redefining intelligence requirements, the fusion center disseminates relevant information and intelligence to its participants in the form of actionable intelligence.

It cannot be overemphasized that for intelligence fusion to be successful, as many law enforcement agencies as possible must participate in the process. Every nonparticipating agency represents a weakness in the ability to identify and prevent threats.

<sup>553</sup> The 17-member Intelligence Community (IC)—which includes the FBI and the Drug Enforcement Administration (DEA)—has a presence in every state; however, the specific IC agencies represented in each state, and consequently each fusion center, vary widely. States with large international ports of entry or military bases, for example, have a greater IC presence. See [https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/061222\\_DNIHandbook\\_Final.pdf](https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/061222_DNIHandbook_Final.pdf).

FIGURE 8-2: THE FUSION PROCESS



## IS THERE A ROLE FOR THE PRIVATE SECTOR?

Often overlooked, the private sector can be a rich resource of information that adds a broadened dimension to information collection. Many large corporations have sophisticated security operations that monitor global threats to their facilities, products, supply chain, and personnel posed by organized crime and criminal extremists as well as predatory criminals. This type of information is often different from that collected by law enforcement organizations and can add a unique and more insightful component to the body of information being analyzed by the fusion center.

Similarly, the private sector is often a legitimate consumer of law enforcement intelligence meeting the right-to-know and need-to-know information sharing standards. For example, 85 percent of the U.S. critical infrastructure is owned by the private sector. Moreover, the private sector has a large personnel force which, if given the proper information, can significantly increase the “eyes and ears on the street” to observe individuals and behaviors that pose threats. As noted in a “Best Practices” paper produced by DHS, “a jurisdiction’s analysis and synthesis entity [such as a fusion center], should also establish processes for sharing information with the local private sector.”<sup>554</sup>

Of course, there are information sharing issues that need to be resolved. For example, certain types of personal identifiable information<sup>555</sup> (PII) may be inappropriate for law enforcement to release to the private sector. Conversely, the private sector will be reluctant to share proprietary information related to intellectual property, corporate products, and processes. Despite these limitations, there is a legitimate role for the private sector in fusion centers. Just as in the case of law enforcement partners, memoranda of agreement (MOAs) need to be in place that include provisions on information sharing processes and restrictions. DHS has provided guidance on how to facilitate private sector engagement with fusion centers that can be quite helpful.<sup>556</sup> (Chapter 9 significantly expands on the discussion of private sector involvement in the law enforcement intelligence process.)

## CONCERNS ABOUT FUSION CENTERS

As might be expected, centralized intelligence fusion centers have heightened concerns of some citizens and critics who fear that the centers will collect, retain, and disseminate information that will further erode the privacy and free speech of people who express support for unpopular or controversial causes. In some cases, a dialogue with

554 Lessons Learned Information Sharing Best Practices. (2006). *Local Anti-Terrorism Information and Intelligence Sharing: Dissemination*. <https://www.hsd.org/?view&did=765561>.

555 <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>

556 <https://www.dhs.gov/sites/default/files/publications/Facilitating%20Private%20Sector%20Engagement%20with%20Fusion%20Centers.pdf>

the community will reduce the concerns; in other cases, it will not. It is nonetheless important to understand these points of conflict. The following discussion presents the most common concerns expressed about fusion centers, followed by the law enforcement response. The intent is to provide insight and communication between fusion centers and those who are skeptical about the centers.

**CONCERN:** “THERE IS A LACK OF AN UNDERLYING PHILOSOPHY. IN THE ABSENCE OF A COMMON UNDERSTANDING ABOUT WHAT CONSTITUTES INTELLIGENCE, FUSION CENTER DEVELOPMENT AND PROGRESS MAY BE IMPEDED.”<sup>557</sup>

**Response:** The purpose of a philosophy is to establish the underlying purpose, processes, and parameters in the execution of an enterprise. The philosophy of law enforcement intelligence, and, by extension, intelligence fusion centers, has never been clearer than it is today. The philosophy has been molded quite effectively, with a clear articulation of roles and responsibilities as found in the *National Criminal Intelligence Sharing Plan* (NCISP), with further support provided by the *Information Sharing Environment Implementation Plan* and the *DHS Target Capabilities List*. Indeed, *Fusion Center Guideline 1* states, “Adhere to the National Criminal Intelligence Sharing Plan and perform all steps of the intelligence process.”<sup>558</sup> The *Guidelines* established the NCISP and the standards contained therein as an unequivocal philosophy.

**CONCERN:** “. . . ARGUABLY, THE 2006 *FUSION CENTER GUIDELINES* HAVE THE FOLLOWING LIMITATIONS: (1) THEY ARE VOLUNTARY; (2) THE PHILOSOPHY OUTLINED IN THEM IS GENERIC AND DOES NOT TRANSLATE THEORY INTO PRACTICE; AND (3) THEY ARE ORIENTED TOWARD THE MECHANICS OF FUSION CENTER ESTABLISHMENT.”<sup>559</sup>

**Response:** The *Fusion Center Guidelines* cannot be viewed in isolation but must be viewed in the context of the other national standards described above. While they are voluntary—the federal government has no authority to mandate all state and local fusion centers to follow the guidelines—the guidelines nonetheless represent accepted national professional standards that are adopted for two reasons. The first, a philosophical reason, is to ensure ongoing professional practice. The second, more pragmatic, reason is that adoption of the *Guidelines* represents good faith and a component of due diligence that helps protect the fusion center from civil liability. While voluntary, the *Fusion Center Guidelines* represent the de facto national standard for state, local, and tribal law enforcement.

With respect to the philosophy, the *Guidelines* state: “. . . a fusion center is defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.”<sup>560</sup> These are explicit, practical objectives, not generic ones.

Finally, the criticism that the *Guidelines* “. . . are oriented toward the mechanics of fusion center establishment” is puzzling. The philosophy has been clearly established as described above: It is a responsible, proactive, and effective fact that national standards for the “mechanics” of fusion centers have been established to help ensure consistency, efficiency, and effectiveness.

---

557 Masse, T., & Rollins, J., *Ibid.*, p. 4.

558 Global Intelligence Working Group (2005), *Ibid.*, p. 25.

559 Masse, T., & Rollins, J., *Ibid.*

560 Global Intelligence Working Group. (2005). *Fusion Center Guidelines*. Washington, DC: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, p. 5.

Indeed, the *Guidelines* represent important control mechanisms for fusion centers to help ensure adherence to the rule of law.

**CONCERN:** “ARGUMENTS AGAINST FUSION CENTERS OFTEN CENTER ON THE IDEA THAT SUCH CENTERS ARE ESSENTIALLY PREEMPTIVE LAW ENFORCEMENT—THAT INTELLIGENCE GATHERED IN THE ABSENCE OF A CRIMINAL PREDICATE IS UNLAWFULLY GATHERED INTELLIGENCE.”<sup>561</sup>

**Response:** The fallacy of this argument rests on erroneous or misinformed assumptions about the law enforcement intelligence function. The first is that *information* is collected—*intelligence* is the output of the analytic process. This is an important distinction.

Certainly, intelligence is preemptive—the intent of intelligence is to *prevent* crime. All crime prevention programs are a form of preemptive law enforcement—the rationale of the criticism is inherently illogical. A cornerstone of law enforcement for decades has been a preemptive approach toward crime whenever possible. Indeed, this preemptive philosophy is the reason the National Crime Prevention Council (NCPC) was created. Law enforcement intelligence is simply another dimension of prevention.

With respect to the concern about unlawfully gathering information, law enforcement personnel at all levels of government are acutely aware of the criminal predicate standard for criminal intelligence records systems. They adhere to privacy and civil rights standards in the intelligence process just as they adhere to constitutional standards of criminal procedure in the course of criminal investigations. Law enforcement organizations have privacy policies, intelligence records, policies, and training, all of which meet constitutional and regulatory requirements. Law enforcement understands these obligations and fulfills them.

**CONCERN:** “AMBIGUOUS LINES OF AUTHORITY ALLOW FOR ‘POLICY SHOPPING. . .’ FUSION CENTERS. . .EXIST IN A NO-MAN’S LAND BETWEEN THE FEDERAL GOVERNMENT AND THE STATES, WHERE POLICY AND OVERSIGHT IS OFTEN UNCERTAIN AND OPEN TO MANIPULATION.”<sup>562</sup>

**Response:** All state and regional fusion centers are a part of a state or local government. Hence, they all have a chain of command and accountability to their parent governmental authorities. All fusion centers have policy manuals that establish, among other things, authority and responsibility; some also have oversight boards. In some cases, fusion centers may be co-located with federal agencies, most notably the FBI; however, there are clear lines of authority and responsibility for the management and accountability of a fusion center to the state or local government. Some fusion centers have governing boards, while others have direct lines of command to a state or local law enforcement organization or a state office of homeland security. While there are different organizational configurations of fusion centers, the lines of authority are unequivocally clear. The practice of “policy shopping” simply does not occur.

There is a long history of state and local law enforcement working in operational capacities with federal agencies on both federal task forces<sup>563</sup> and the Joint Terrorism Task Forces<sup>564</sup> (JTTF). Clear lines of authority, responsibility, and operational policy are for all task force participants

---

561 Masse, T., & Rollins, J., *Ibid.*, p. 5.

562 German, M., & Stanley, J. (2007). *What’s Wrong with Fusion Centers?* New York, NY: American Civil Liberties Union, p. 9. <https://www.aclu.org/report/report-whats-wrong-fusion-centers>

563 <https://www.justice.gov/usao-wdpa/task-forces>

564 <https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces>

are stipulated and have functioned effectively without policy shopping. Fusion centers are no different.

**CONCERN:** “PRIVATE SECTOR PARTICIPATION IN FUSION CENTERS RISKS PRIVACY AND SECURITY. FUSION CENTERS ARE POISED TO BECOME PART OF A WIDE-RANGING TREND OF RECENT YEARS IN THE UNITED STATES: THE CREATION OF A ‘SURVEILLANCE-INDUSTRIAL COMPLEX’ IN WHICH SECURITY AGENCIES AND THE CORPORATE SECTOR JOIN TOGETHER IN A FRENZY OF MASS INFORMATION GATHERING, TRACKING, AND ROUTINE SURVEILLANCE.”<sup>565</sup>

**Response:** All non-law enforcement personnel in fusion centers, including public and private partners, must pass background investigations before they are given access to information—many have security clearances, which make them subject to federal laws governing the handling of classified and sensitive information and state and local privacy protection laws. In addition, private sector representatives typically do not represent a single company, but an entire sector.

Information collection for the intelligence process is a product of explicit procedures that are dictated by law and the scientific approach to problem solving—it is not collected in a frenzy. Indeed, “mass information gathering” is typically avoided because it makes the intelligence process more difficult: A greater mass of information would have to be sorted through to identify a threat. Indeed, the purpose of *intelligence requirements* is to identify and collect only that information which is needed for analysis.

The NCISP and the *Fusion Center Guidelines* describe the importance of private sector involvement in law enforcement intelligence. Certainly, there is sensitivity to the types of information to which the private sector participants have access. As a result, each fusion center has a privacy policy,<sup>566</sup> to which private sector participants agree to adhere. Moreover, private sector partners must sign a memorandum of understanding (MOU) and a nondisclosure agreement (NDA), both of which help to protect individual privacy.

**CONCERN:** “MILITARY PARTICIPATION IN FUSION CENTERS VIOLATES FUNDAMENTAL TENETS OF LIBERTY. OFFICIALS WHO REGARD AMERICAN COMMUNITIES AS BATTLEFIELDS IN A ‘WAR’ CAN BE TEMPTED TO DISPENSE WITH ‘INCONVENIENT’ CHECKS AND BALANCES.”<sup>567</sup>

**Response:** While typically not seen by the public, there is hypersensitivity by both law enforcement agencies and military representatives in the law enforcement intelligence arena. Both recognize the sensitivity to these issues.

Law enforcement does not have this war perspective, nor is law enforcement influenced by the military. The only military personnel in some fusion centers are members of the National Guard, who are responsible to the state governor, not to DoD, and who work on narrowly defined drug trafficking cases, typically as analysts. A few fusion centers also have representatives from the U.S. Coast Guard, notably in support of drug enforcement. As an organizational entity of DHS, rather than DoD, the U.S. Coast Guard is not considered military except in time of war.

---

565 Ibid., p. 11.

566 [https://it.ojp.gov/documents/d/Fusion\\_Center\\_Privacy\\_Policy\\_Development\\_508compliant.pdf](https://it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf)

567 Ibid., p. 15.

**CONCERN:** “DATA FUSION = DATA MINING, WHICH IS BAD FOR PRIVACY AND BAD FOR SECURITY.”<sup>568</sup>

**Response:** These two forms of research and analysis are not the same. Data mining (also known as knowledge discovery) has been defined as “the nontrivial extraction of implicit, previously unknown and potentially useful information from data”.<sup>569</sup> It uses artificial intelligence, machine learning, and statistical and visualization techniques to discover and present knowledge in a form that is easily comprehensible to humans.<sup>570</sup>

The greatest use of data mining is for marketing and advertising—industries that have far more information about individuals than fusion centers have. Data fusion is the analytic process of integrating information obtained from many heterogeneous sources into a single composite picture of the environment.<sup>571</sup>

Data mining is a proactive process using sophisticated software and algorithms to develop new knowledge about an entity. Data fusion is an integration and analytic technique that increases the accuracy of analysis by relying on a wide array of diverse information sources. In general, law enforcement agencies and fusion centers have neither the resources nor the expertise for data mining activities. However, the inclusion of different agencies from different levels of government establishes the heterogeneous information sources characteristic of data fusion. Analysis is performed on this diverse data using the scientific approach to problem solving, as is characteristic of all types of intelligence analysis.

From an intelligence perspective, data mining is somewhat like a fishing expedition, examining massive amounts of data in the hope of finding something potentially criminal. While technology enhances the ability to data mine for this purpose, it is still inherently inefficient and ineffective.

**CONCERN:** “EXCESSIVE SECRECY UNDERMINES THE MISSION OF FUSION CENTERS.”<sup>572</sup>

**Response:** Fusion centers operated by state and local law enforcement should have transparent *processes*; however, the content of much of their work must remain largely secret both to protect privacy and to protect the integrity of inquiries. Some levels of secrecy increase when the fusion center is accredited as a sensitive compartmented formation facility (SCIF).<sup>573</sup> In these cases, there will be more secrecy, as a matter of federal law, because the facility will contain classified information. Although there are instances of excessive secrecy, the fundamental issue is that “excessive” will be interpreted differently depending on one’s position and perspective. Fusion centers are a component of public law enforcement organizations: While the content of their work largely needs to remain secret, their processes should be transparent.

For many people, the past abuse of law enforcement intelligence will be the lens through which all future law enforcement intelligence activities are judged. The ongoing skepticism, while frustrating, is a reminder of the need to remain vigilant in training, supervising, and managing the intelligence process.

---

568 Ibid., p. 15.

569 Frawley, W., Piatetsky-Shapiro, G., & Matheus, C. (1992). “Knowledge Discovery in Databases: An Overview.” *Artificial Intelligence Magazine* (Fall), pp. 213–228.

570 <http://www.the-data-mine.com/bin/view/Misc/IntroductionToDataMining>

571 <https://www.hindawi.com/journals/tswj/2013/704504/>

572 German, M., & Stanley, J., Ibid., p. 9.

573 For more information on SCIFs, see <https://fas.org/irp/offdocs/dcid6-9.pdf>.

Similarly, critics need to realize the radical changes that have occurred in law enforcement organizations over the past generation. Officers are significantly better educated; training has increased dramatically; and professional leadership has embraced modern management techniques, values, and responsibilities. This underlying fabric serves as an important foundation for the law enforcement intelligence function.

## FUSION CENTERS AND CIVIL RIGHTS ISSUES

There is a concern among many privacy advocates that the growth of fusion centers will increase the jeopardy to citizens' civil rights and privacy. As noted in a National Governors Association "Best Practices" paper, "The risks to individuals' privacy begin when personal information of any kind is entered into criminal justice information systems."<sup>574</sup> Criminal intelligence records systems are certainly included in this description and warrant special attention because of the low level of "proof"—i.e., "reasonable suspicion"—required to enter PII into the system.

Complicating this issue is the fact that, not understanding the concept of the fusion process, many privacy advocates fear that the centers are the next iteration of centralized surveillance of citizens.

Perhaps the greatest concern about fusion centers in this regard is participation of federal law enforcement agencies whose jurisdictions for information collection and retention differ from those of state, local, and tribal law enforcement agencies. Certainly, when a state, local, or tribal law enforcement agency is the custodian of an intelligence records system, care must be taken to exclude information from the fusion center that does not meet the standards of 28 CFR Part 23.

Fundamentally, the privacy and civil rights issues of citizens related to fusion centers are the same as for any other aspect of the intelligence process. Those relevant standards of the NCISP apply in the same manner and should be fully adhered to. Further, *Guideline 8* of the *Fusion Center Guidelines* states that the management of the fusion center should "[d]evelop, publish, and adhere to a privacy and civil rights policy."<sup>575</sup> Commentary on this *Guideline* goes on to note that:

. . .one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals' privacy and constitutional rights through the use of intelligence sharing systems. In order to balance law enforcement's ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place.<sup>576</sup>

As a consequence, civil rights issues for fusion centers have components related to policy, training, supervision, and public information that must be addressed in the development and implementation stages. Over the past two decades, the author has participated in countless meetings, training programs, and discussions related to the intelligence process and fusion centers. It has been unquestionable that contemporary law enforcement leaders and personnel place a priority on intelligence processes that operate to protect civil rights and privacy.

---

574 MacLellan, T. (2006). *Protecting Privacy in Integrated Justice Systems*. Washington, DC: National Governors Association Center for Best Practices, p. 4.

575 *Fusion Center Guidelines*, *Ibid.*, p. 49.

576 *Ibid.*

## 10 WAYS TO ENGAGE AND SUPPORT YOUR FUSION CENTER

1. **Recognize the importance of information sharing.** Encourage the practice of sharing information with other law enforcement and public safety agencies. Use the guidelines and action steps of the NCISP to implement or enhance your organization’s intelligence function.
2. **Improve information flow.** Ensure that channels of communication exist to efficiently share information and intelligence, including suspicious activity reports (SARs). Work with the fusion center to agree on a common lexicon and the most effective and efficient methods for the transfer of this information.
3. **Support an information sharing culture through training initiatives.** Provide training programs for everyone by explaining intelligence, why it is valuable, and how it benefits the department.
4. **Train new recruits.** Provide training to new recruits on the role of fusion centers, why the mission is important, how to send information to the fusion center, and what information to collect.
5. **Communicate your needs to the fusion center or governing board.** Constantly communicate your information needs and requirements to the fusion center and offer definitions for actionable information. Ensure that your agency provides feedback on the value of products disseminated and offers recommendations for improvement when necessary.
6. **Assign personnel to the fusion center.** Depending on the center, officers, investigators, and analysts may all be assigned and have skills and knowledge to contribute. There are many models for assignment. Some agencies choose to assign personnel on a part-time basis (e.g., one day a week), while others serve full-time for three- or six-month rotations.
7. **Establish or participate in a terrorism liaison officer (TLO) program.** Departments that cannot afford to loan personnel to a center can participate in a TLO program or an intelligence liaison officer (ILO) program. The purpose of these programs is to disseminate information distributed by a center to the “boots on the ground” and ensure that all appropriate information collected by a particular agency is effectively shared with the fusion center.
8. **Educate political leaders.** Educating political leaders about fusion centers—their value and their needs—may encourage them to demonstrate commitment to the fusion center concept and thus to support their agencies, and that commitment, through appropriate funding.
9. **Join the governing board of the fusion center, if one exists.** Participating on an interagency governing board will demonstrate the importance of collaborating with the fusion center and allow for a greater understanding of the capabilities and products the center has to offer law enforcement.
10. **Hire analysts, if possible.** Both intelligence analysts and crime analysts require different skill sets than those required for patrol officers and investigators. Analysts can make officers “work smarter,” providing for both increased efficiency and effectiveness.

Based on: 10 Ways to Engage and Support Your Fusion Center. (2008). Washington, DC: Police Executive Research Forum.

## CAN FEDERAL CRIMINAL INTELLIGENCE BE SHARED WITH FUSION CENTERS?

From the materials presented throughout this guide on information sharing, the intuitive response to this question would be “yes.” However, the issue emerged surrounding intelligence associated with the January 6, 2021 insurrection of the U.S. Capitol. The FBI had intelligence concerning the insurrectionists but did not believe it could be shared with the fusion center serving the District of Columbia, the National Capital Region Threat Intelligence Consortium<sup>577</sup> (NTIC). The rationale was that the NTIC was not a part of the Metropolitan Police Department but was instead organized as part of the District of Columbia Homeland Security and Emergency Management Agency. As such, the NTIC was not a law enforcement agency and NTIC employees were not sworn law enforcement officers.

While the intelligence was eventually shared, it may have slowed some operational responses, while bringing to the forefront a question that could not be readily answered with certainty. However, many believed the information could be shared, particularly after intelligence reform from the Intelligence Reform and Terrorism Prevention Act of 2004. It appears IRPTA may not have directly addressed this issue.

Ironically, this issue had nonetheless actually been addressed around 15 years earlier, when the Office of General Counsel (OGC) of the U.S. Department of Justice issued an opinion on the matter. The OGC stated,

The Department of Justice Office of Justice Programs (DOJ OJP) understands that professionals at “fusion centers” under 6 U.S.C. Section 124h(k)(1) engage in activity that facilitates the detection, prevention, investigation, apprehension, and response to criminal or terrorist activity. Given that fact, in advising one of our OJP client offices, it appears likely that we would understand such engagement to constitute “law enforcement activity” within the meaning of 28 C.F.R. Section 23.20(e) that would provide a proper basis to disseminate criminal intelligence information under (and pursuant to the requirements of) 28 C.F.R. Part 23 (“Part 23”).

Accordingly, it seems to us that such fusion centers may appropriately be provided, under Part 23, with access to Part 23 criminal intelligence information on a right-to-know and need-to-know basis, regardless as to whether a particular fusion center happened to bear the title of “law enforcement agency” or its professionals bear the title of “law enforcement officers.”<sup>578</sup>

This opinion was in response to specific inquiries and apparently not widely disseminated. Moreover, the opinion—likely because it was stated in letters in response to inquiries—appears not to have been included in training programs or other policy documents. Regardless of the source of uncertainty and decisions made under these unclear circumstances, it is now clear that federal criminal intelligence may be shared with fusion centers not functionally organized as law enforcement agencies and with professionals working in those fusion centers, even though they are nonsworn employees.

---

<sup>577</sup> <https://hsema.dc.gov/NTIC>

<sup>578</sup> Based on opinions from the DOJ Office of General Counsel in letters sent to Colonel Tommy Davis, Director, Texas Department of Public Safety (April 7, 2004) and Brigadier General Matthew Broderick, USMC (Ret.), Director, Homeland Security Operations Center (March 31, 2005). (Copies on file.)

## DEVELOPING THE FUSION CENTER

As noted previously, a fusion center's operations should be consistent with the recommendations of the *National Criminal Intelligence Sharing Plan* (NCISP)<sup>579</sup> and the *Fusion Center Guidelines*<sup>580</sup> of the Criminal Intelligence Coordinating Council. The NCISP provides standards for all aspects of the intelligence function to ensure best practices, effective operations, and adherence to civil rights. The *Fusion Center Guidelines* are designed to ensure that:

Information and intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center utilizes a common set of guidelines. The complete support of public safety leaders at all levels is critical to the successful implementation and operation of fusion centers.<sup>581</sup>

Adherence to established national standards will increase the quality of information sharing within the fusion center's participants' jurisdictions, with intelligence entities outside of the region, and with the Information Sharing Environment. Further, the standards will institutionalize a consistent approach to information collection, retention, analysis, and dissemination that represent recognized and accepted processes as defined by the consensus of intelligence subject-matter experts (SMEs) who helped design the standards.

Beyond relying on national standards, consideration must be given to defining who the center's stakeholders are and determining what it will take to get the stakeholders' buy-in to the center's operations. It is this simple: There is a direct correlation between stakeholder (or consumer) participation in the fusion center and the success of the center. Similarly, stakeholders will not participate in the center unless the products they receive are useful.

To assist in the development and utility of fusion centers, the following common themes, and, more important, common questions, should be examined:

- ◆ Do fusion centers solve the pre-9/11 information sharing barriers, and, as such, make Americans safer?
- ◆ Can fusion centers work if they are not part of an integrated philosophy of intelligence and security?
- ◆ Who are the customers of the fusion center's products?
- ◆ What agency should staff, fund, and oversee the center?
- ◆ What role should federal agencies play in fusion centers, to include funding?
- ◆ What is the role of fusion centers in balancing the security versus civil liberties pendulum?
- ◆ How active and proactive, if at all, should fusion centers be in the collection of intelligence that is not directly tied to a specific and identifiable criminal act (i.e., threats)?
- ◆ Is the current approach to creating, authorizing, funding, and supporting fusion centers sustainable?
- ◆ What are the risks to the fusion center concept, and how have those risks been specifically weighed and balanced against the stated goals of fusion center operations?<sup>582</sup>
- ◆ How should fusion center outcomes be evaluated, including the variables for evaluation?

---

579 See <https://it.ojp.gov/gist/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>.

580 See [https://it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf).

581 Global Intelligence Working Group. (2005). *Ibid.*, p. ii.

582 Adapted from Masse, T., and Rollins, J., *Ibid.*, pp. 3–4.

The answers to these questions provide the foundation for shaping the Guiding Principles related to the creation and management of fusion centers:

1. Adhere to the tenets contained in the *National Criminal Intelligence Sharing Plan*.
2. Collaboratively develop and embrace a mission statement.
3. Create a representative governance structure.
4. Use an MOU, NDAs, and other types of agreements as appropriate.
5. Integrate state, local, tribal, and federal law enforcement agencies.
6. Create an environment in which participants can seamlessly communicate.
7. Develop, publish, and adhere to a policies and procedures manual.
8. Develop, publish, and adhere to a privacy policy.
9. Ensure that appropriate security measures are in place for the facility, data, and personnel.
10. Integrate sworn and nonsworn personnel and ensure that all personnel are properly trained.
11. Leverage existing systems and databases and allow for future connectivity.
12. Offer a variety of intelligence services and monitor outputs and outcomes.<sup>583</sup>

From an *operational* perspective, the North Central Texas Fusion Center has defined five Guiding Principles in support of the fusion center's performance:

- |                      |  |
|----------------------|--|
| Guiding Principle 1: | Processing tools and the aggregation of data across jurisdictions and across disciplines are required to achieve the benefits of fusion. |
| Guiding Principle 2: | Visualization and analysis tools are essential for "connecting the dots."  |
| Guiding Principle 3: | The most important objective is disaster prevention, early warning, and mitigation.  |
| Guiding Principle 4: | The more data, the better.   |
| Guiding Principle 5: | Cross-disciplinary analyst(s) need to be assigned to constantly explore the data and test hypotheses. <sup>584</sup>                     |

Building on these principles, three broad phases, each with specific focal areas, are envisioned to accomplish the fusion center's development.

---

583 Modafferi, P., & Bouche, K. (2005). "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards." *The Police Chief*. (February). Vol. 72., No. 2.

584 Stone, K. (2006). *Deploying and Operating an Effective Regional Fusion System: Lessons Learned from the North Central Texas Fusion System*. Unpublished policy paper prepared by the North Central Texas Fusion System, McKinney, Texas, p. 5.

Phase

1

THIS IS THE FOUNDATION PHASE. IT INCLUDES THESE COMPONENTS:

- ◆ **Re-education.** Stakeholders must understand the contemporary role of law enforcement intelligence and the capabilities of the fusion center. Just as important, stakeholders must understand their role in making the intelligence function a success at preventing acts of terrorism, preventing the occurrence of organized crime, and managing homeland security threats that may affect public safety. As recommended by the NCISP and the *Minimum Criminal Intelligence Training Standards*, personnel at all levels of the organization—from executives to line personnel—must receive awareness training as intelligence relates to their roles.
- ◆ **Developing a mission, goals, and objectives.** What is the fusion center to do? How will it operate? What crimes will be addressed? What will it produce? What is its role and its relationship to its consumers? What are the priorities of the fusion center? These are questions that must be resolved and articulated in the mission, goals, and objectives. This is a laborious process requiring input from everyone, including executives and stakeholders. The process cannot be effectively accomplished, however, until after the training component is completed because all personnel must understand the contemporary law enforcement intelligence function and ensure that their vision of the fusion center is consistent with contemporary standards.
- ◆ **What the fusion center will not do.** Just as important as what the fusion center will do is some discussion of what the fusion center will *not* do. There will likely be changes in the historic intelligence activities of agencies that will not be continued in the fusion center. For example, many activities of state police intelligence units tended to be more akin to investigative support rather than to intelligence activities. For the center to function most effectively, these factors must be clear. Similarly, stakeholders and consumers must understand what the fusion center will not do to avoid erroneous expectations.

Phase

2

PROACTIVE DEVELOPMENTAL ACTIVITIES THAT MUST BE OVERTLY ADDRESSED IN THIS PHASE INCLUDE THE FOLLOWING:

- ◆ **Developing relationships.** Two critical elements of the success of any intelligence activity are information collection and information dissemination. Both must have detailed elements to ensure that everyone does his or her job with respect to intelligence activities. The fusion center must rely on management support from partnering agencies. It must also rely on personnel to collect needed information, document it, and forward it to the fusion center. Similarly, to be successful, the fusion center must effectively disseminate information and products in a manner that is easily accessible by consumers, in a format that is easy to use, and containing information on a consistent basis that is useful. To accomplish these things, there must be overt initiatives to develop relationships among stakeholders within the fusion center and with its external constituency. Developing these relationships must involve developing commitments to participate in the center's activities.
- ◆ **Outputs/products.** The fusion center must identify specific outputs and products that will be produced on a regular basis. Will both tactical and strategic reports be produced? Will bulletins and advisories be produced? Will summaries be produced? What is the schedule for outputs? How will responses to specific inquiries be produced? What is the process for determining right-to-know and need-to-know standards for products and outputs? These are among the questions that need to be addressed and articulated as the fusion center's development process moves forward.

Phase

3

THIS PHASE INVOLVES MOVING ALL PHASE 1 AND PHASE 2 ACTIVITIES INTO OPERATIONAL FORM.

It includes everything from facilities and staffing to developing MOAs (see Chapter Annex 8-1) to the actual implementation of the fusion center's operations. This phase can consume a massive amount of time and logistics, particularly when the intelligence function is not just being revised, but reengineered.

Among other activities in this phase are melding agencies and their data, protecting each agency's data, standardizing data for incorporation into a single system, ensuring quality control (i.e., accuracy) of data, protecting the security of the data, and establishing processes for auditing and accountability.

## OUTPUTS OF THE FUSION CENTER

Typically, fusion centers are not designed to respond to ongoing calls or inquiries about individuals or threats (this is the role of investigative support centers and dispatch centers). While such inquiries will, no doubt, occasionally occur, if they occur too frequently, staff members will be overwhelmed and unable to perform their analytic responsibility. The most important output of the intelligence fusion center is *actionable* intelligence. This means that the intelligence produced by the center drives operational responses and strategic awareness of threats.

An operational response occurs when analysis determines that there is a threat against a specific type of target. Operationally, a law enforcement agency may then take necessary actions to harden the target or intercept the threat. Strategic awareness is broader information that provides information on threats and methodologies—or indicators—of terrorists and criminals.

The specific kinds of output from a fusion center are not universal. Different regions of the country, the character of targets in a region, and the unique character of threats must be taken into consideration when output is being designed. For example, in a given geographic region, there may be a large presence of active right-wing extremists. As a result, a significant amount of attention from the fusion center would be focused on their activities. Similarly, a fusion center in a state on the U.S. border with Mexico would have significant attention devoted to drug smuggling and human trafficking. Thus, while all fusion centers should have an all-crimes approach, there should be appropriate strategic priorities within those crime categories.

In light of this, a fusion center's substantive outputs should be based on three basic factors:

- ◆ Defined threats based on comprehensive—and ongoing—threat assessments within the jurisdiction of the fusion center.
- ◆ Information and intelligence needs defined by stakeholders.
- ◆ National priorities—including those of external funding—such as the National Preparedness Goal<sup>585</sup> or FBI intelligence requirements.

Beyond the substantive content, the format and frequency of outputs need to be identified, specifically in light of the types of analysis and products that are produced and the frequency with which they are produced. In some cases, the format of the output may be dependent on unique characteristics of the fusion center's jurisdiction. Types of output may include any or all of the following:

585 <https://www.fema.gov/national-preparedness-goal>

- ◆ **Summary briefs**—incidents and activities, globally or locally, that may have some correlation to threats, particularly if the incidents reflect a trend.
- ◆ **Threat assessment**—a detailed description of threats, targets, the likelihood of an attack against a defined target, and the potential methods of attack.
- ◆ **Situational awareness reports**—the current status of known threats or changes in the status of known threats.
- ◆ **Information bulletins**—information on new or emerging threats, including threat indicators and methodologies.
- ◆ **Intelligence assessments**—comprehensive analysis, usually of a strategic nature, about a threat.
- ◆ **Raw intelligence**—information that is derived from a source deemed to be reliable but not yet corroborated or analyzed. Typically, the threat is time critical and potentially severe; hence the dissemination of the information.

In addition to these intelligence products, the fusion center will produce case or investigative intelligence. This is intelligence related to specific threats, targets, and suspects. Case intelligence is produced and disseminated on a timely basis as facts warrant, rather than on a fixed schedule. Dissemination is narrower and goes only to those persons who have a demonstrable right to know and need to know the information.

The different intelligence outputs may employ a variety of analytic techniques: link analysis, financial analysis, association matrices, visual investigative analysis, threat profiling, and pattern analysis are illustrations. Typically, a fusion center is also involved in other processes that enhance the criminal inquiries of intelligence targets, such as deconfliction, case correlation (particularly between jurisdictions), and intelligence support of investigations related to criminal enterprises and terrorism.

## RESEARCH AND FUSION CENTERS

Perhaps one of the most common questions about fusion centers is whether they are effective. What appears to be an easy question is surprisingly complex—the simple answer is that some are and some are not. Effectiveness depends on accomplishing stated goals, which varies widely among the centers. Threats identified, threats prevented, facilitation of productive investigations, identification of targets and facilitation of target hardening, identification of new and emerging crime trends, and provision of information to law enforcement decision makers to help with crime priorities and resource allocations could all be measures of effectiveness. To effectively fulfill its mission, the fusion center must have sufficient capacity—to include staffing, facilities, equipment, connectivity, and funding—and the expertise of analysts and management. One researcher observed that:

Fusion center outcomes vary because the paths to effectiveness vary based on organizational factors like capacity, the skills and abilities of analysts, and the relationships that analysts maintain with communities of practice internal and external to the network. While strong ties may be able to better leverage capacity, it does not appear from the cases that ties alone compensate for a lack of capacity. Based on the sample analyzed in this research, the most highly effective organizations have high capacities and strong ties. Analysts in these fusion centers were also very skilled. On the other hand, less effective organizations lacked both in capacity and relationships, and analysts prioritized fewer skills.<sup>586</sup>

The research suggests that fusion centers can be effective on virtually any of the variables identified above: Their structure, staffing, resources, and organization are all critical variables that will influence their success. While some

---

<sup>586</sup> Coffey, A. F. (2015). *Measuring Effectiveness in the Domestic Intelligence Community: Taking a Configurational Approach to Explain Organizational Outcomes in the National Network of Fusion Centers*. A dissertation submitted to the Virginia Polytechnic Institute and State University.

have argued the need to ensure uniformity—or as close to it as possible—across all fusion centers,<sup>587</sup> this is not a feasible alternative because the centers are entities of state and local governments and must operate within the mandates, structures, and resources of their parent governments. Some critics have accused fusion centers of “mission creep,”<sup>588</sup> arguing that they are not effective because they have gone beyond counterterrorism and are focusing on various types of crime. This is a mischaracterization because the missions of different fusion centers are whatever their governance structure defines, including all crimes, all threats, and all hazards. Their missions are not limited to counterterrorism.

Another key component of fusion center effectiveness is successful information sharing. Researchers have examined information sharing practices of fusion centers to assess whether they enhance information sharing to produce quality intelligence as clearinghouses to support homeland security, ILP, and community safety.<sup>589</sup> The core need for fusion centers to enhance analysis and information sharing comes from the fact that U.S. law enforcement agencies are fragmented, most with no analytic capacity and many with limited information sharing experience. Thus, establishing fusion centers that can share critical threat information will ideally produce more actionable intelligence.<sup>590</sup> This has prompted some empirical research on how fusion centers operate. Specifically, it is not sufficient to simply produce intelligence products and disseminate them. Rather, intelligence products must meet the needs of consumers, since they must be disseminated to the persons who can use the information to identify and prevent criminal threats.

Research has shown that despite major initiatives in the post-9/11 environment, some police agencies still are not fully engaged in information sharing.<sup>591</sup> Moreover, the autonomy of traditional police agencies and the limited interagency experience beyond often superficial contact may hinder the quality of information shared across agencies.<sup>592</sup> Essentially, to enable effective information sharing, police agencies’ organizational cultures must change; although this has occurred at some levels, the problem is not fully resolved. Further research has found that interagency information sharing has often not occurred in a formal fashion, such as via fusion centers. Rather, officers overly rely on informal methods of information sharing.<sup>593</sup> That is, officers tend not to engage fusion centers for information sharing. They view the formal process of fusion center information sharing as awkward or time-consuming. Hence there is a need to ensure that officers are informed of information sharing processes, have the appropriate connectivity, and learn how using fusion centers will benefit their work. This suggests that there is both a need for fusion center outreach and for police management that proactively promotes information sharing through fusion centers, which requires training, policy development, and establishment of an information sharing culture within the agency.

---

587 Ladich, S. (2018.) *Asserting Collective State Sovereignty to Strengthen the National Network of Fusion Centers*. A thesis submitted to the Naval Postgraduate School.

588 <https://privacysos.org/blog/its-time-to-pull-the-plug-on-fusion-centers/>

589 Chermak, S., Carter, J., Carter, D., McGarrell, E., & Drew, J. (2013). “Law Enforcement’s Information Sharing Infrastructure: A National Assessment.” *Police Quarterly*, 16(2), 211–244.

590 Carter, J. (2015). “Inter-Organizational Relationships and Law Enforcement Information Sharing Post September 11, 2001.” *Journal of Crime and Justice*, 38, 522–542.

591 Joyal, R. (2012). “How Far Have We Come? Information Sharing, Inter-agency Collaboration, and Trust Within the Law Enforcement Community.” *Criminal Justice Studies*, 25(4), 357–370.

592 Taylor, R., & Russell, A. (2012). “The Failure of Police Fusion Centers and the Concept of National Intelligence Sharing Plan.” *Police Practice and Research*, 13(2), 184–200.

593 Carter, J. (2015), *Ibid*.

Another study found that:

—the intelligence products [from fusion centers are] read daily and perceived to be moderately useful by recipients. End users are primarily concerned with jurisdiction-specific and officer safety-related information. Upper-level administrators are the organizational lynchpins for funneling information to patrol officers.<sup>594</sup>

This gets back to the issue of developing user-specific intelligence products and, in some cases, educating end users on why the intelligence product is important, such as when new crime trends emerge. Thus, writing intelligence products sometimes needs to go beyond simply providing the results of an analysis to providing context to enable the end user to fully understand the information. Of course, the challenge is providing the information concisely in easily consumable forms.

The problem with relying on the chain of command or specialty assignments to funnel intelligence products to patrol officers is that this adds filtering—and sometimes barriers—to effective information sharing to line level officers. Direct distribution of intelligence products can increase efficiency and effectiveness. Moreover, modern information systems can ensure that intelligence products that are electronically pushed<sup>595</sup> to line officers meet the needs self-identified by officers as well as meeting right-to-know and need-to-know standards.

Despite the fact that fusion centers have been in place for well over a decade, some research has shown that many officers did not know what a fusion center actually does or had misconceptions about a fusion center's function.<sup>596</sup> Indeed, many officers did not know that they had access to fusion center information. Officers who were familiar with fusion centers often saw themselves solely as consumers of the information provided, not as having any responsibility for pushing raw information to the centers. Further, lack of specificity of the analytic product, or lack of specificity of the intelligence, dissatisfied some officers, which led to uncertainty about the utility of information produced by the centers.<sup>597</sup>

The lesson learned was that to develop and maintain a trusting relationship between a fusion center and the officers, the fusion center must, on a consistent basis, proactively reach out to law enforcement agencies and officers to inform them of the fusion center's resources and intelligence capabilities, helping them learn about the local law enforcement's specific intelligence needs and develop methods for more efficient two-way information sharing. Fusion centers and officers who view and practice their relationships as partnerships will be the most productive.

In the end, an important key to a fusion center's success is the law enforcement agency's attitude toward the fusion center<sup>598</sup> and the information sharing infrastructure as an organization.<sup>599</sup> In an ethnographic study of how officers make sense of ILP, researchers concluded that it was dependent on the organizational culture and situational context of policing. That is, they asserted that upper-level police managers rhetorically adopted ILP,<sup>600</sup> translating it into ways that were favorable to them. For example, they used the ILP philosophy for demonstrating accountability and to quantify police practice and as a risk analysis tool for the allocation of resources.<sup>601</sup> Thus, fusion centers can serve

---

594 Lewandowski, C., & Carter, J. G. (2017). "End-User Perceptions of Intelligence Dissemination From a State Fusion Center." *Security Journal*, 30(2), 467–486.

595 Wongthongtham, P., et al. (2018). "State-of-the-Art Ontology Annotation for Personalized Teaching and Learning and Prospects for Smart Learning Recommender Based on Multiple Intelligence and Fuzzy Ontology." *International Journal of Fuzzy Systems*. Vol. 20, No. 4, pp. 1357–1372.

596 Carter, D., et al. (2016), *Ibid.*

597 Lewandowski, C., & Carter, J. (2017).

598 Sanders, C., Weston, C., & Schott, N. (2015). Police Innovations, "Secret Squirrels" And Accountability: Empirically Studying Intelligence-Led Policing In Canada. *British Journal of Criminology*, 55(4), 711–729.

599 Chermak, S., et al., 2013, *Ibid.*

600 Sanders C., et al., 2015, *Ibid.*

601 *Ibid.*

as linchpins of information sharing both vertically, within law enforcement agencies, and horizontally, across law enforcement agencies, to help facilitate ILP as well as to understand the threat environment. In many cases, it is upper-level managers or specialty units in police agencies who share information across departments horizontally; they are also the ones who disseminate the obtained information to officers vertically.

There is variation among fusion centers across the country, and it should not be surprising that major-urban-area fusion centers are reportedly more responsive to line officers than are primary state fusion centers because of their local mandates. Nonetheless, research suggests that a strong customer-oriented approach and an education effort by primary state fusion centers would enhance both their effectiveness and the receipt of more raw information for analysis.

## CONCLUSIONS

The intelligence fusion process holds a great deal of promise for effective intelligence operations. In many ways, fusion centers are still a work in progress. This is particularly true given the multijurisdictional character of terrorist operations and criminal enterprises as well as hazards that require public safety operations. The four greatest challenges for a fusion center are: (1) to develop a cooperative and committed relationship among all stakeholders; (2) to ensure the privacy and protection of personal identifiable information; (3) to establish policies and processes that support efficient, effective, and lawful intelligence operations; and (4) to ensure that the center stays on message as an analytic center.

# CHAPTER ANNEX 8-1: DEVELOPING A MEMORANDUM OF UNDERSTANDING

## DEVELOPING A MEMORANDUM OF UNDERSTANDING (MOU)<sup>602</sup>

Fusion centers inherently require the sharing of information and, often, resources between law enforcement agencies. In either case, there are important obligations on the part of the fusion center and each agency that enters into an agreement with it. As a result, a formal agreement needs to be in place that serves to *formalize and institutionalize* obligations and responsibilities of all parties involved. These agreements have different names: memorandum of understanding (MOU), memorandum of agreement (MOA), letter of understanding (LOU), or statement of understanding (SOU). Regardless of the name, they all refer to a written agreement between two or more parties that articulates a specific relationship.

Because the nature of the agreements varies widely, the description below focuses on the basic principles and types of content that should be included in an MOU.

### GUIDING PRINCIPLES OF AN MOU:

- ◆ **The MOU is a statement of commitment**—The MOU defines the actual agreements and responsibilities in the relationship. The commitment statement can set the context, quality, or sentiment behind the relationship.
- ◆ **The MOU requires explicit statements of expectations and obligations**—Specific activities, expertise, and resources need to be articulated in the agreement in as much detail as possible.
- ◆ **The MOU must state what is not intended to be covered**—If there are specific activities and responsibilities that might be assumed to be covered by the MOU but are not intended to be covered by the agreement, these should be spelled out.

### CONTENTS OF THE MOU:

#### I. Introduction

- b. What is the intent, capability, or resource for which the MOU is being created?
- c. Specify the agencies that are participating in the MOU. An MOU may be between two entities—such as the fusion center and a single law enforcement agency—or it may include multiple parties.
- d. Provide a statement on why the MOU is necessary. This is essentially the “spirit of the agreement,” which can be useful if questions of interpretation later arise about certain provisions in the agreement.
- e. What agreements are set forth by this MOU?

#### II. Purpose

- a. To what capability does the MOU apply? When answering this question, consider the questions that follow.
  - ii. What is the intended level of commitment?
  - iii. What is the command structure that will make decisions about and enforce components of the agreement?

#### III. Scope

- a. What are the public safety, public service, and other governmental and nongovernmental agencies that will use the capability/resource?
- b. Are there organizations or agencies that must be excluded whose members would otherwise be participants?

---

602 For further information, see <https://www.justice.gov/archives/ovw/page/file/910376/download>.

#### IV. Definitions

- a. What are the technical and operational aspects of responsibilities, capabilities, and resources? Consider including definitions for each.
- b. Be certain to define/explain acronyms that may be commonly used.

#### V. Policy

- a. Specify the circumstances for use of fusion center resources, including special requests.
- b. Specify authorization required for contacting and use of the fusion center.
- c. Specify the operating procedures associated with the fusion center as related to the parties of the MOU.

#### VI. User Procedure Requirements

- a. What are the training, exercise, and equipment requirements associated with participating in this MOU?

#### VII. Financial Relations

- a. If the MOU includes a fee-for-service arrangement or other financial obligations, a method for determining financial payments should be clearly established. Any and all financial commitments should be spelled out clearly, with appropriate approvals and monitoring systems in place.
- b. Articulate any financial obligations that must be considered.
  - iii. What is going to be done?
  - iv. Who is going to do it?
  - v. Under what conditions/when will it happen?
  - vi. Who pays for what?

#### VIII. Maintenance

- a. What are the maintenance requirements associated with participating in this MOU?
- b. If any licenses are required for activities (e.g., software licensing), who will own the licenses?
- c. Who will maintain the equipment?

#### IX. Oversight

- a. What governance structure oversees the fusion center?
- b. What is the relationship of the governance structure to the parties of the MOU?
- c. What are the participation requirements in the governance structure of agencies entering this MOU?
- d. How are issues affecting policy, recommendations, and/or subsequent change implemented by the governance structure?

#### X. Responsibility for Standard Operating Procedure (SOP) Compliance

- a. Who is responsible for ensuring that the SOPs associated with this capability/resource are followed and that individual agency personnel are trained appropriately?
- b. How will compliance be carried out?

#### XI. Updates to the MOU

- a. Who has the authority to update/modify this MOU?
- b. How will this MOU be updated/modified?
- c. Will updates/modifications require this MOU to have a new signature page verifying the understanding of changes by each participating agency?

#### XII. Separation from the MOU

- a. Under what circumstances may a signatory agency withdraw from the MOU?
- b. What are the penalties or obligations (both funding and other resources), if any, for separation prior to the termination date of the MOU?

#### XIV. Authorized Signatures and Dates

- a. All parties to the MOU must have a signature of agreement and commitment by an individual who has the authority to make such commitments.
- b. Explicit dates should be specified as to when the MOU goes into effect.



# CHAPTER 9

## DEVELOPING PUBLIC-PRIVATE PARTNERSHIPS FOR LAW ENFORCEMENT INTELLIGENCE (P3I)



It could be argued that the idea for public-private partnerships (PPPs) in law enforcement dates back to one of the most fundamental principles of policing, articulated by Sir Robert Peel in 1829 in the United Kingdom. Peel noted that the government alone could not perform all policing duties—assistance was needed by members of the public, and by extension the private business sector, to help keep communities safe from crime. Indeed, Peel argued that in a democratic society, the police derived their authority from the public; hence the public had an *obligation* to assist the police on matters of public safety. His principle, “The police are the people and the people are the police,” infers a reciprocal responsibility.<sup>603</sup> In the 21st century, this may be inferred to include two-way information sharing and joint public safety initiatives—responsibilities that both law enforcement and the private sector should embrace.

Reinforcing this notion was an observation reported in a study by the Vera Institute, which concluded:

The police depend on citizens to assist in almost every aspect of crime prevention and investigation. Mobilizing that public support is essential to the core mission.<sup>604</sup>

Traditionally, the relationship between law enforcement and the private sector concerning crime control and community safety initiatives has been relatively superficial. Typically, such initiatives have been related to crime issues which were largely idiosyncratic to a given community. In some cases, the law enforcement-private sector

603 Carter, D. L. (2000). *The Police and the Community*. 7th ed. Englewood Cliffs, NJ: Prentice-Hall, Inc.

604 Bhanu, C., & Stone, C., op. cit., p. 3.

relationship has even been contentious. For example, alarm companies and law enforcement agencies have often had problems related to responses to false alarms just as law enforcement and private investigators or security guards have been at professional odds, often with law enforcement viewing these two groups disparagingly as “police wannabes.” From another perspective, in some instances private companies have asked state and local law enforcement for assistance in enforcing laws where counterfeit products—such as T-shirts—were being sold, with law enforcement largely dismissing the requests because it had to focus on “real crime.”

In other cases, new law enforcement-private sector relationships have been derailed by legitimate obstacles such as civil rights and privacy concerns by law enforcement or concerns about the potential to undermine profit and investments by private entities. To keep a perspective, public safety and security is part of a law enforcement agency’s core mission, whereas in the private sector, safety and security are an expense that draws from the bottom-line profit. While accommodating these different perspectives is not an insurmountable challenge, it requires creativity and innovation, both of which are often labor-intensive. All too often, a potential relationship has dwindled away, with both groups saying “we tried” rather than forging forward to resolve the barriers. In some cases, it was just perceived that the potential outcomes were not worth the time and resource investment needed to make the initiative work. These perspectives began to be reshaped in the post-September 11, 2001 (post-9/11), era, albeit slowly.

Working cooperatively with the private sector to accomplish functional goals can be highly productive. As observed by the Vera Institute:

Perhaps the most promising but least studied source of external support for police reform is the private business community. Not only do private sector companies command political attention, they hold talent, dynamism, creativity, and a wealth of resources that can be useful to reformers within police agencies.<sup>605</sup>

Similarly, a study by the RAND Corporation found that:

Private organizations also have proved to be a good source of information for local police. Private security officers, reservation and store clerks, and baggage handlers are good examples of private sources with helpful information; they are much more likely than an officer to see or sense something suspicious. Some agencies are trying to develop such relationships by creating seminars to teach businesses about the kinds of information that are most helpful. These seminars have the twofold objective of easing the anxiety of participants while enhancing the likelihood that they will call the police with information.<sup>606</sup>

As law enforcement continues to reengineer its intelligence initiatives to support real-time crime centers, homeland security, targeted violence, cybercrime, and other threats, it has become obvious that the need for effective public-private partnerships is more important than ever. Even something that seems as simple as sharing private video surveillance footage with law enforcement can have obstacles. Furthermore, partnerships need to be configured in an array of different models depending on the threat picture within a region. The obstacles remain; however, increasingly it is understood that the value derived from such relationships is indeed worth the time and resource investment. While there are many programmatic approaches related to the private sector associated with prevention, disaster preparedness, incident management, and response, the current discussion will be limited to public-private partnerships for intelligence (P3I).

---

605 Bhanu, C., & Stone, C. (2004). *Public-Private Partnerships for Police Reform*. New York, NY: Vera Institute of Justice, p. 1.

606 Riley, K. J., Treverton, G., Wilson, J., & Davis, L. (2005). *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation, p. 40.

## BACKGROUND AND PERSPECTIVE

Much of the current thought on PPPs has been shaped by initiatives related to the development of the European Union. A brief look at this history provides some perspective.

As a means to increase their economic strength on a global basis, 13 Western European countries developed an agreement originally known as the European Economic Commonwealth, which evolved into the European Community and, as it is known today, the European Union.<sup>607</sup> One of the foundations of developing a viable and economically strong union of diverse, multilingual governments was to embrace PPPs. The conceptual framework developed by the European Union has broad applicability to the United States (U.S.). Paraphrasing, a PPP is an agreement of cooperation between autonomous private and public parties working together to achieve joint objectives, on the basis of a clear division of responsibilities, tasks, and authority, and with no hierarchy among the parties. The most important preconditions for the success of a PPP are mutual trust and recognition of the possibilities for the future.<sup>608</sup>

In expanding the concept of PPPs to public safety and security issues, there is a recognition in Western societies that security—or safety—is a fundamental right, meaning that the government bears responsibility for the preservation of this right. Four notions are important in this respect:

1. The government cannot solve security problems in society alone.
2. When there is a specific threat, government leaders have the obligation to take the necessary measures to prevent or mitigate the threat.
3. Repression is not the solution in a free society; there is a need to develop prevention.
4. Threats and security problems at the local level must be addressed by a common strategy that can often be enhanced and supported by the private sector.

Three conditions for effective partnerships have been articulated for PPPs to be functional:

1. Effective cooperation, which includes the willingness to listen, to get to know each other, to respect each other, to recognize the limits of each partner, and to share useful information, leading to discretion, confidentiality, and the willingness to share information.
2. Working methodically, which means not waiting for a crisis before working together, to meet regularly, to plan processes of meeting, and to use tools agreed on by all the partners to collect information.
3. Developing programs and initiatives adapted to the history of the community and to its administrative and social reality.

On the last point, for P3I in the United States, this would include consideration of civil rights and privacy issues, protection of corporate proprietary information, and adherence to national standards for security of sensitive information and participation in the Information Sharing Environment (ISE).

---

<sup>607</sup> The current European Union membership is 27 countries (since the exit of the UK). The history of the European Union (EU) is too complex and unnecessary for the current discussion. A good history of the EU, including milestone events, can be found at [https://europa.eu/european-union/about-eu/history\\_en](https://europa.eu/european-union/about-eu/history_en).

<sup>608</sup> <https://ec.europa.eu/digital-single-market/en/public-private-partnerships>

## U.S. NATIONAL STANDARDS AND RECOMMENDATIONS FOR PUBLIC-PRIVATE PARTNERSHIPS

In the United States, the need to proactively incorporate the private sector as a functional partner in the information/intelligence sharing process has been consistently recognized by a wide range of inquiries. The *9/11 Commission Final Report* noted that:

The mandate of the Department of Homeland Security does not end with the government; the department is also responsible for working with the private sector to ensure preparedness. This is entirely appropriate, for the private sector controls 85% of the critical infrastructure in the nation. Indeed, unless a terrorist's target is a military or other secure governmental facility, the "first" responders will almost certainly be civilians. Homeland security and national preparedness therefore often begins with the private sector.<sup>609</sup>

There is a critical need for information sharing with the private sector to develop intelligence to prevent terrorists' attacks from touching U.S. soil. The 9/11 Commission goes on to observe, on the matter of public-private information sharing, that:

The necessary technology already exists. What does not [already exist] are the rules for acquiring, accessing, sharing, and using the vast stores of public and private data that may be available. When information sharing works, it is a powerful tool.<sup>610</sup>

Moreover, that information sharing need has grown even more as law enforcement deals with radicalization on social media, growth of transjurisdictional trafficking of illegal goods and services via darknet marketplaces, and access to smartphones and personal devices with biometric security and encryption.

In examining the successes of government information sharing, the General Accountability Office observed that:

One of the challenges in securing our homeland is ensuring that critical information collected and analyzed by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) is shared in a timely and secure manner with a variety of parties within federal, state, and local governments, as well as the private sector.<sup>611</sup>

To deal with these issues, the *National Strategy for Homeland Security* stated, "Government at the federal, state, and local level must actively collaborate and partner with the private sector. . ."<sup>612</sup> Similarly, the *National Strategy for Information Sharing* observed, "Private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks."<sup>613</sup>

Specifically, for law enforcement, recommendations have been made by the Criminal Intelligence Coordinating Council to include the private sector in the law enforcement intelligence mission. For example, Recommendation 7 of the *National Criminal Intelligence Sharing Plan, Version 2.0*, states that:

To sustain effective information sharing, it is imperative that law enforcement agencies continue to develop and enhance partnerships with each other, as well as with the private sector, other public safety

---

609 National Commission on Terrorist Attacks upon the United States. (2004). *9/11 Commission Final Report*. Washington: pp. 397–398.

610 Ibid., p. 419.

611 General Accountability Office. (2007). *TECHNOLOGY: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*. Washington, DC: GAO, p. 9.

612 *National Strategy for Homeland Security*. (2002). Washington, DC: Executive Office of the President, p. 33.

613 *National Strategy for Information Sharing*. (2007). Washington, DC: Executive Office of the President, p. 4.

disciplines, privacy advocates, and community groups, to foster collaboration and coordination that provide for improved public relations and may also support criminal intelligence development.<sup>614</sup>

Similarly, the *Fusion Center Guidelines* observed that:

The public safety and private sector components are integral in the fusion process because they provide fusion centers with crime-related information, including risk and threat assessments, and subject-matter experts who can aid in threat identification.<sup>615</sup>

As evidenced by the various reports cited thus far, it is clear that public-private information sharing is critical for protecting communities from terrorism and complex criminality. It is recommended in virtually every inquiry and assessment of intelligence effectiveness. Yet, in the years since the 9/11 attacks, these partnerships have not reached the magnitude that was envisioned. As noted by the Bureau of Justice Assistance (BJA) in a report exclusively devoted to public-private relationships, “Barriers to information sharing between law enforcement and private security clearly exist.”<sup>616</sup> The report goes on to conclude:

The lifeblood of any policing agency is information; thus, information sharing (and its analyzed counterpart, intelligence sharing) should be a central component of any law enforcement-private security partnership.<sup>617</sup>

Not only has the U.S. Department of Justice noted the importance of public-private information sharing, an array of DHS inquiries has also emphasized the importance of this relationship. For example, one of the objectives of the *DHS Intelligence Enterprise Strategic Plan* is:

*Objective 1.4: Reporting:* Manage Homeland Security intelligence-related information reporting, seamlessly linking all levels of government and the private sector.<sup>618</sup>

Similarly, in one of the DHS “Best Practices” papers, it is stated that:

A jurisdiction’s analysis and synthesis entity should also establish processes for sharing information with the local private sector. Private businesses and public safety agencies can provide each other with valuable threat and vulnerability information. However, public and private entities often have restrictions on information sharing with each other because of concerns over the release of sensitive or proprietary information.<sup>619</sup>

Yet another DHS “Lessons Learned” document recommends that “[l]ocal businesses and industries should also be incorporated into any local information sharing network.”<sup>620</sup> One of the caveats, however, is that “[p]ublic safety and private security officials should cooperatively establish guidelines that strike a balance between the need to

---

614 Criminal Intelligence Coordinating Council. (2013). *National Criminal Intelligence Sharing Plan, Version 2.0*. Washington, DC: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, p. 17.

615 Global Intelligence Working Group. (2004). *Fusion Center Guidelines*. Washington, DC: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, p. 2.

616 Morabito, A., & Greenberg, S. (2005). *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: Bureau of Justice Assistance, p. 4.

617 *Ibid.*, p. 7.

618 Office of the Chief Intelligence Officer. (2006). *DHS Intelligence Enterprise Strategic Plan*. Washington, DC: U.S. Department of Homeland Security, p. 7.

619 Lessons Learned Information Sharing Best Practices. (2006). *Local Anti-Terrorism Information and Intelligence Sharing: Dissemination*. <https://www.hsdl.org/?abstract&did=765515>

620 Lessons Learned Information Sharing Best Practices. (2006). *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Networks*. <https://www.hsdl.org/?abstract&did=765561>

inform the private sector of potential threats and the need to ensure that proprietary information is not improperly disseminated.”<sup>621</sup> Another report addressed this issue, noting:

Currently, no formal process exists for state, local, tribal, and private sector entities to task federal agencies with specific intelligence requirements. Failing to understand these entities’ requirements inhibits the federal government’s ability to understand the threats facing the Nation, much less provide actionable, timely, preferably UNCLASSIFIED, and frequently updated homeland security information and intelligence to those on the front lines of the domestic War on Terrorism.<sup>622</sup>

More recently, recognizing the value of private sector expertise, DHS has urged “innovative” PPPs to fight online extremism.<sup>623</sup>

Active collaboration with private sector technology specialists, non-governmental organizations, and academics is key to Countering Violent Extremism (CVE) communications efforts. The private sector generally best understands emerging online trends and how to foster dialogue about the intersection of technology and important issues such as violent extremism. The United States Government best understands broad trends regarding the ways violent extremists use online platforms and the relevant policy and law enforcement implications. Bringing these competencies together will ensure our national approach to CVE appropriately incorporates modern technologies and is informed by accurate information regarding violent extremists’ use of the Internet. The CVE Task Force will work to ensure engagements with the non-governmental stakeholders on this topic are consistent with protections for civil rights and civil liberties and are strategic and coordinated in order to avoid burden and to produce mutual benefit.<sup>624</sup>

For the purposes of monitoring online extremism, developing partnerships can not only bring unique expertise to the table that may not exist in the government; it can also provide unique access and review of information—in this case, social media posts and messaging—to which the government may not have ready access.<sup>625</sup>

With respect to online extremism, one useful source is the Global Internet Forum to Counter Terrorism, whose mission it is to bring together the technology industry, government, civil society, and academia to foster collaboration and information sharing to counter terrorist and violent extremist activity online.<sup>626</sup>

The FBI has also recognized the value of P3I by establishing the Office of Private Sector (OPS), which:

...provides an organized, coordinated, and horizontal approach to how the FBI engages with the private sector. It serves as the entity within the FBI that has a 360-degree understanding of the FBI’s engagement with the private sector—enterprise-wide. Part of the Intelligence Branch, OPS allows for one “FBI voice” and connects private industry with who they need to connect with—whatever the concern. Among other activities, OPS works to enhance the FBI’s understanding of the private sector’s risks and needs, increases collaboration and information-sharing between the Bureau and the private sector, and mitigates threats through longstanding, mutually beneficial partnerships between the private sector and the FBI.<sup>627</sup>

---

621 Ibid.

622 Lessons Learned Information Sharing Best Practices. (2006). *Homeland Security Intelligence Requirements Process*. [https://www.dhs.gov/xlibrary/assets/Final\\_LLIS\\_Intel\\_Reqs\\_Report\\_Dec05.pdf](https://www.dhs.gov/xlibrary/assets/Final_LLIS_Intel_Reqs_Report_Dec05.pdf)

623 <https://www.fedscoop.com/dhs-advocates-innovative-public-private-partnerships-fight-online-extremism/>

624 <https://www.dhs.gov/cve/task-force#digital-strategies>

625 The privacy and civil liberties issue is significant in these types of operations and must be addressed. However, this illustration is limited to demonstrating the value of PPPs.

626 <https://gifct.org/>

627 <https://www.fbi.gov/about/partnerships/office-of-private-sector>

DHS I&A also has initiatives to work with the private sector through the Private Sector Engagement initiative.<sup>628</sup> While both the FBI and DHS private sector programs have limited daily application to SLTLE operations, they demonstrate that both the DBI and DHS recognize the importance of private sector relationships.

As an illustration at the local level, “the City and County of Denver and Denver Police Department (DPD), in collaboration with the Downtown Denver Partnership and the Downtown Denver Business Improvement District, are expanding the city’s gunfire detection system. . . .”<sup>629</sup> All parties recognized the threat of firearms violence and that solving the problem would be most effective with a partnership. While the police goal was to expressly reduce violent crime, the businesses recognized that making downtown safer would bring in more customers for businesses. While their core motives were different, all parties wanted the same outcome leading to the partnership.

It is clear from these recommendations and assessments that the private sector must be integrated into information sharing partnerships. Despite this plethora of recommendations, integration has been surprisingly limited. Moreover, the economic lifeblood of many communities lies in the corporate sector. Many corporations and industries—beyond those that are part of the critical infrastructure—have been identified as targets of terrorist attacks, ransomware attacks, and theft of proprietary information by hackers. Information sharing between public and private entities simply has not evolved as recommended and expected—it is incumbent upon law enforcement leaders to develop a process and training to remedy the information gap.

## P3I AND THE INTELLIGENCE PROCESS

The reader should recall that the current model of intelligence addresses all crimes, all hazards, and all threats. From this perspective, the private sector can be particularly valuable in addressing threats to the community from terrorism, targeted violence, criminal extremism, and cybercrime.

As a brief review, law enforcement (LE) intelligence is the analytic output of raw information that describes threats to a community that have a nexus with crime. This traditional form of intelligence focuses on criminal behaviors such as those related to terrorism or criminal enterprises. The less traditional homeland security (HS) intelligence is the analytic output of raw information that describes noncriminal threats to critical infrastructure, public health, or community safety for which a law enforcement agency will have some type of public order, public safety, and/or order maintenance responsibility. For example, if pandemic strikes a community—such as the coronavirus of 2020—law enforcement agencies will likely have to assist with victims; aid in quarantines; and assist in expediting and protecting medical supplies, food, water, and the supply chain. As another illustration, HS intelligence may determine that as a result of new industry, larger barges will travel a major waterway near a community which, in turn, increases the likelihood of a barge striking a major bridge. As a result, law enforcement strategic planning will have to deal with rescue and recovery plans, traffic control plans, and security of the accident scene.

Linking both types of intelligence into a “targeted capability outcome,” the DHS *Target Capabilities List* states that:

Effective and timely sharing of information and intelligence occurs across Federal, State, local, tribal, territorial, regional, and private sector entities to achieve coordinated awareness of, prevention of, protection against, and response to a threatened or actual domestic terrorist attack, major disaster, or other emergency.<sup>630</sup>

---

628 <https://www.dhs.gov/private-sector-engagement>

629 <https://www.denvergov.org/content/denvergov/en/police-department/news/2019/city-and-county-of-denver-and-downtown-denver-partnership-make-s.html>

630 National Preparedness Directorate. (2007). *Targeted Capabilities List*. Washington, DC: U.S. Department of Homeland Security, p. 69.

Some challenges for P3I may occur for health professionals with unique types of personal identifying information (such as information on public health and the Health Insurance Portability and Accountability Act of 2006<sup>631</sup> [HIPAA]). Plans and processes for lawfully dealing with sharing this type of information and avoiding barriers, should a public health threat emerge, are much easier to resolve before a crisis than during a crisis. For example, if a public health emergency occurs, it would be essential for health care professionals to identify individuals to law enforcement who pose a risk or who are at risk. If processes are put in place with both law enforcement and public health professionals trained on these procedures, conflict resolution and service delivery will be expedited.

Moreover, suspicious banking transactions, threatening rhetoric on social media, or suspicious activities at hotels that may indicate human trafficking are all examples in which the private sector can have an important role in protecting the community.

The intent of this discussion has been to place in context some basic definitions and concepts to provide perspective for the P3I. A transitional issue is the relationship of PPPs to the Information Sharing Environment from the context of state, local, and tribal law enforcement agencies.

## THE INFORMATION SHARING ENVIRONMENT AND THE PRIVATE SECTOR

A challenge for both law enforcement and the private sector results from the creation of the Information Sharing Environment (ISE). This is a formal set of guidelines and processes to enhance the sharing of intelligence across five critical sectors: (1) the Intelligence Community; (2) federal law enforcement; (3) state, local, and tribal law enforcement; (4) the private sector; and (5) selected foreign partners.

Recognizing the need to go beyond individual solutions to create an environment—the aggregation of legal, policy, cultural, organizational, and technological conditions—for improving information sharing, Congress passed, and the President signed the landmark *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). The Act requires the President to establish an Information Sharing Environment (ISE), “for the sharing of terrorism information in a manner consistent with national *security* and with applicable legal standards relating to privacy and civil liberties.”<sup>632</sup>

Based on this legislative mandate, the Program Manager for the ISE (PM-ISE) guided the development of an *Implementation Plan* to provide the mechanism by which the ISE would accomplish its legislative mandate. A critical starting point was defining a vision that has essentially become the ISE’s ultimate goal:

We envision a future ISE that represents a *trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America.*<sup>633</sup> (Emphasis in original.)

Key to realizing this vision was to create a “culture of information sharing” among the Intelligence Community, law enforcement agencies, and the private sector. This ambitious plan includes developing the willingness among all entities to proactively be involved in two-way information sharing, increasing technological connectivity between the entities to appropriately and lawfully share information and to develop a common lexicon to increase information quality while maintaining security.

---

631 See the Office of Civil Rights, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/hipaa/> for more information.

632 Program Manager–Information Sharing Environment. (2006). *Implementation Plan for the Information Sharing Environment*. Washington, DC: PM-ISE, Office of the Director of National Intelligence, p. xiii.

633 Ibid.

As part of this challenge, the *ISE Implementation Plan* stated that the private sector should be part of “. . . a coordinated [information sharing] source. . . for access to terrorism information, alerts, warnings, and situational awareness.”<sup>634</sup> The *Plan* went on to note that private sector information represents a crucial element in both understanding the current threat environment and preventing the nation’s critical infrastructure from being the target of attacks.

Protecting the interconnected and interdependent U.S. infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, as well as protects private sector information in such a way that the private sector is willing to share it with government partners.<sup>635</sup>

While going beyond the needs of the intelligence process, the primary conduits for sharing threat information currently are the Sector Coordinating Councils<sup>636</sup> (SCCs) and sector-specific Information Sharing and Analysis Centers<sup>637</sup> (ISAOs) established by the National Infrastructure Protection Plan (NIPP) and the Cybersecurity and Infrastructure Security Agency.<sup>638</sup> To date, however, sharing through these mechanisms has yielded mixed results. One of the reasons stems from the ambiguity inherent in public-private relationships. Another important factor is that private sector participants report that the demand from federal, state, and local governments for critical infrastructure and other information since 9/11 has multiplied many times over, imposing more demands on industry to collect information and report it. Added to the complexity of these factors is that requests for private sector information are rarely coordinated or consistent, resulting in duplicative requests.<sup>639</sup> If P3I is going to be successful, a consistent collection plan needs to be established. The NIPP<sup>640</sup> articulated six objectives that can serve as guideposts for the collection plan:

1. Sharing information to manage risks to business enterprises and in a manner that protects the information privacy and other legal rights of Americans
2. Creating a national framework and culture for sharing information that rationalizes requests for terrorism information to the private sector and that adequately protects the risks and proprietary interests of corporations
3. Creating an integrated, trusted environment in which information can be shared, maintained, and protected
4. Ensuring access to the integration and analysis of data from multiple sources to provide industry with indicators of impending threats or current attacks
5. Receiving actionable alerts and warnings concerning specific industries that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations
6. Implementing policies and mechanisms that provide liability and antitrust protections to the private sector in connection with sharing information in good faith<sup>641</sup>

Private sector participation in the Information Sharing Environment continues to mature as existing organizations and information sharing protocols within ODNI, DHS, and the FBI develop and mature. The Domestic Security Alliance Council<sup>642</sup> (DSAC), led by the FBI, is a strategic partnership between the U.S. government and U.S. private industry to

634 Ibid., p. 12.

635 Ibid., p. 19.

636 <https://www.dhs.gov/cisa/sector-coordinating-councils>

637 <https://www.dhs.gov/cisa/information-sharing-and-analysis-organizations-isaos>

638 <https://www.cisa.gov/>

639 <https://www.dhs.gov/hsin-critical-infrastructure>

640 The NIPP can be downloaded at [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

641 Ibid., p. 20.

642 <https://www.dsac.gov/>

enhance information sharing and the timely and effective exchange of security and intelligence information between the federal government and the private sector. The DSAC promotes efforts to advance the FBI's mission of detecting, preventing, and deterring criminal acts by facilitating strong, enduring relationships among its private sector member companies, FBI headquarters, FBI field offices, DHS headquarters and fusion centers, and other federal government entities. DHS's National Protection and Programs Directorate<sup>643</sup> (NPPD) shares responsibility for coordinating private sector participation in the information sharing environment. Specifically, NPPD is responsible for the protection of the nation's physical and cybercritical infrastructure from terrorist attacks, natural disasters, and other catastrophic incidents. NPPD also works with private sector partners to integrate both government and private sector information into the ISE.<sup>644</sup>

A number of federal initiatives in different departments of government, along with relevant federal regulations, support PPPs.<sup>645</sup> These initiatives demonstrate that partnerships can work and provide models for consideration in the intelligence enterprise.

The challenge is to understand the complete character of P3I, defining the critical issues that must be resolved and achieving these objectives in a manner that protects the critical interests of both private entities and law enforcement organizations. These are often competing interests; however, there are some principles which can be relied on to guide both types of organizations through this territory that, despite many recommendations, remains largely uncharted.

## FUNDAMENTAL PRINCIPLES OF P3I

The Public-Private Partnership for Intelligence (P3I) is intended to prevent or mitigate criminal and homeland security threats to a community through a two-way flow of raw information and intelligence. In its *Homeland Security Policy Statement*, the National Governors Association (NGA) observed that:

... private sector partners play a key role in providing experts, technology, and infrastructure resources to establish and maintain our nation's security. The role of the business community and the impact on the economic viability of a community when faced with [the prospect of] a terrorist attack must be considered.<sup>646</sup>

One perspective of understanding private sector targets within a community is to use the framework on which DHS relies on: Identifying "critical infrastructure" (CI).

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. The 16 critical infrastructure sectors are as follows:

- ◆ Commercial Facilities Sector
- ◆ Communications Sector
- ◆ Critical Manufacturing Sector
- ◆ Dams Sector
- ◆ Defense Industrial Base Sector
- ◆ Emergency Service Sector

---

643 <https://www.dhs.gov/publication/nppd-glance>

644 *Information Sharing Environment Annual Report to Congress*. (2019). Washington, DC: Office of the Director of National Intelligence, p. 9. [https://www.dni.gov/files/documents/FOIA/2017\\_Information\\_Sharing\\_Environment\\_Annual\\_Report.pdf](https://www.dni.gov/files/documents/FOIA/2017_Information_Sharing_Environment_Annual_Report.pdf)

645 <https://www.acus.gov/research-projects/public-private-partnerships>

646 National Governors Association. (2007). "Section 5.5—Coordination with the Private Sector." *Policy Position: EC-05. Homeland Security Policy*. Washington, DC: NGA.

- ◆ Energy Sector
- ◆ Financial Service Sector
- ◆ Government Facilities Sector
- ◆ Food and Agriculture Sector
- ◆ Healthcare and Public Health Sector
- ◆ Information Technology Sector
- ◆ Nuclear Reactors, Materials and Waste Sector
- ◆ Transportation Systems Sector
- ◆ Water and Wastewater Systems Sector<sup>647</sup>

These elements of critical infrastructure affect every community in the United States and are therefore of primary national concern.

As noted previously, while there are many roles the private sector may fulfill in homeland security, the current discussion is focusing solely on the intelligence role for prevention. As such, private critical infrastructures should be identified based on their likelihood to be targets in light of the reasonable threats within the region.

One might also consider the non-law enforcement public sector within the same framework as “private” because much of its information processing and roles are more like the private sector than law enforcement. Moreover, these organizations have access to unique types of information. For example, public housing, code enforcement, traffic engineering and maintenance, corrections, tax collections, occupational licensing, and waste management possess unique information that could provide value to the domestic intelligence enterprise.

Intelligence relies on raw information. From this perspective, an important element to consider is that the private sector has access to raw information not readily available to law enforcement that can be important to respond to intelligence requirements related to threats within a community or a region. This information may come from independent sources (domestically or internationally) that a corporate security organization has developed through its own sources. For example:

- ◆ An auto manufacturer’s corporate security division learns through an investigation of transshipment thefts from an overseas parts supplier that the same criminals are smuggling stolen art and antiquities to locations within the United States.
- ◆ Corporate security from a multinational banking firm learns of financial transactions originating in your city in which funds are transferred to a bank in Venezuela suspected of hosting bank accounts of persons suspected of drug trafficking.
- ◆ Corporate security of a large retail company discovers that illicit opioids are being smuggled from China to your community hidden in legitimate shipments of merchandise.

Information from the private sector may also be developed as the result of a request from law enforcement to “be on the lookout” (BOLO) for certain terrorism or criminal indicators. As an example:

- ◆ Law enforcement intelligence provides training on criminal indicators to freight or package delivery companies and asks their delivery persons to report suspicious activities based on those indicators.

---

<sup>647</sup> <https://www.dhs.gov/cisa/critical-infrastructure-sectors>

- ◆ Law enforcement intelligence officials ask a retailer to notify them if certain commodities known to be used in terrorism financing or part of another type of criminal enterprise are being sold or stolen from the retailer's store.
- ◆ Law enforcement intelligence asks a representative of large corporate retailers of certain chemicals to report unusual purchases of selected products that could be used to commit a terrorist attack.

“Business leaders often ask what—other than extra funds—they can contribute to effective police reform. One answer is skills.”<sup>648</sup> The private sector has a range of expertise and technology not readily available to law enforcement. This includes expertise with unique technologies, such as artificial intelligence; international audio and video communications; social media analysis; and the ability to assess hazardous materials; as well as access to a wide array of technological equipment, ranging from chemical detectors to satellites.

## TYPES OF PARTNERSHIPS

Partnerships may be developed in different forms based on resources, threats, and information needs. These will be determined by such factors as the nature of threats within a community; the types of critical infrastructure in a region and their vulnerability; and the willingness of public and private organizational leaders to enter into information sharing partnerships.

**Full partnerships through personnel assignment.** Full partnerships occur when a person from the private sector is assigned full-time to a fusion center or intelligence unit. Typically, the individual will represent a business sector, not just the company where he or she is employed. For example, the Boeing Corporation assigned an analyst to the Washington fusion center as a sector liaison for the aircraft manufacturing industry.<sup>649</sup>

Having the private sector employee represent an entire sector, with the approval of the fusion center command structure, avoids allegations of playing favorites to any specific company. Moreover, it is simply more efficient and effective to have one sector representative rather than multiple representatives from one sector. Of course, a challenge is to ensure that the sector representative has an agreement with other members of the sector to share needed information.

A full partnership assignment should include, at the minimum, (1) a background investigation of the person being assigned; (2) a memorandum of agreement (MOA) between the public and private entities that spells out duties, responsibilities, and processes of both parties as related to the employee's assignment; and (3) a signed nondisclosure agreement.

The law enforcement intelligence entity needs to assess the sectors in its region (which may be more explicit than the DHS list of critical infrastructures) to determine the most critical to be represented in the fusion center or unit; for example, the gaming and hotel industry in Las Vegas, Nevada, or the tourism industry in Orlando, Florida. Table 9-1 lists the range of sectors that may provide value to an intelligence unit.

648 Bhanu, C., & Stone, C., op. cit., p. 3.

649 <https://www.upi.com/Defense-News/2007/06/06/Boeing-plans-analyst-in-fusion-center/44181181166359/>

TABLE: 9-1: SECTORS OF PRIVATE INDUSTRY

◆ Agriculture, food, water, environment	◆ Postal and shipping
◆ Banking and finance	◆ Private security
◆ Chemical industry and hazardous materials	◆ Public works
◆ Criminal justice (non-law enforcement)	◆ Real estate
◆ Education	◆ Retail
◆ Emergency services (non-law enforcement)	◆ Transportation – aviation (all commercial)
◆ Energy	◆ Transportation – aviation (general)
◆ Government	◆ Transportation – buses and light rail
◆ Health and public health	◆ Transportation – maritime
◆ Hospitality and lodging	◆ Transportation – rail
◆ Information and telecommunications	◆ Transportation – roads and bridges
◆ Military facilities and defense industrial base	

**Full-time information sharing partnership.** Under this arrangement, there is two-way information sharing between law enforcement and private sector partners that occurs on an ongoing basis, just as the agency does with law enforcement partners. The distinction between this and the “full partnership” is that in the current case, a person is not assigned to a fusion center or intelligence unit—he or she physically remains at the place of employment. This is particularly valuable when there are standing intelligence requirements related to the private sector. The most commonly used instance in which this is used is when an intelligence liaison officer<sup>650</sup> (ILO) program is established.<sup>651</sup>

The ILO concept establishes a formal relationship with the private sector organization designating an individual who will be the contact point on all two-way information sharing. Typically, the ILO is vetted for security purposes; receives training along with law enforcement officers on intelligence, counterterrorism, and homeland security intelligence issues; is given defined areas of responsibility for information sharing; and is often given access to a secure email system. ILOs should also meet regularly with the intelligence group to discuss issues and processes to maximize effectiveness as well as to maintain a strong relationship that is essential for sustaining the ILO program. As was the case with the full partnership, all participating organizations should sign a MOA, and the ILO should sign a nondisclosure agreement.

Since the ILO will physically remain at his/her place of employment, information security becomes a greater issue for both parties. As a result, information security processes should be outlined in the MOA.

The ILO program is a functional option when the private sector does not have sufficient personnel to assign a person to the law enforcement agency, yet this information is critical for community safety.

<sup>650</sup> It should be noted that this role is used in a variety of different agencies and has different names: fusion liaison officer (FLO), terrorism liaison officer (TLO), and intelligence liaison officer (ILO) are common examples. Regardless of the name of the role, the concept is the same. Similarly, the concept is not limited to the private sector. A state fusion center, for example, may designate intelligence liaison officers from different law enforcement agencies from throughout the state.

<sup>651</sup> There are many illustrations of ILO programs, most notably in fusion centers. As an example, see <https://publicsafety.ohio.gov/wps/portal/gov/odps/what-we-do/our-programs-new/ilo-program/ilo-program>.

The ILO fulfills a number of important roles which include, but are not limited to:<sup>652</sup>

- ◆ Collecting, reporting, retrieving, and sharing training materials related to threats faced by the sector.
- ◆ Serving as a source person for internal and external inquiries from the fusion center or intelligence unit.
- ◆ Collecting, reporting, retrieving, and sharing of information and intelligence related to potential threats to the sector.
- ◆ Identifying, communicating, and serving as a liaison with stakeholders in the sector.
- ◆ Serving as the contact person for persons in the sector who have questions about or information to share about a threat.
- ◆ Conducting, coordinating, and/or facilitating training with regard to threats in the sector. The training should be for law enforcement and/or the sector.
- ◆ Serving as the designated sector representative for meetings, associations, task forces, or any other entity related to sector threats.
- ◆ Monitoring and sharing information with the fusion center or intelligence unit about the existence and/or changes of sector critical infrastructure.
- ◆ Conducting and maintaining threat and vulnerability assessments for the sector.
- ◆ Keeping up to date on terrorist and criminal threats to the sector by monitoring all sources, including open sources.
- ◆ Being familiar with all law and national standards related to the intelligence function.
- ◆ Serving as a sector subject-matter expert on all technical and industry-specific language, equipment, and processes for the sector.

**Ad hoc partnerships.** The ad hoc partnership is used on an as-needed basis. This is a particularly viable alternative when there are no standing intelligence requirements needed from a particular industry or event in the private sector, for example, in a major event such as the Super Bowl. When threat circumstances arise relating to the sector or organization, a mechanism is in place for rapid information sharing. In extreme cases, a private sector representative may be placed on a temporary duty (TDY) assignment to the law enforcement agency. Similar vetting processes should be used in the case of the ILO as well as for the MOU and the nondisclosure agreement.

## OBSTACLES TO LAW ENFORCEMENT-PRIVATE PARTNERSHIPS

The inherent nature of P3I requires the open two-way exchange of threat-based information and intelligence between law enforcement agencies and the private sector for both law enforcement and homeland security purposes. As such, processes need to ensure that the exchange is open and that both law enforcement and the private sector receive the information they need. Unfortunately, this is not easy. In exploring the law enforcement-private sector relationship, the Bureau of Justice Assistance (BJA) identified three key obstacles that must be overcome in order to establish effective partnerships.<sup>653</sup>

**Obstacle 1: Barriers to Information Sharing.** There are a number of information sharing barriers that must be overcome by both law enforcement and the private sector if effective information sharing is to take place.

The barriers emanating from a law enforcement agency to the private sector include:

---

652 Based on the Arizona Counterterrorism Information Center bulletin on the Terrorism Liaison Officer (TLO) program.

653 Bureau of Justice Assistance. (2005). *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: Office of Justice Programs, U.S. Department of Justice, p. 4.

- ◆ Uncertainty on what types of information may be shared with the private sector because of privacy and civil rights concerns.
- ◆ Uncertainty on how to share information designated for law enforcement distribution only. In this regard, one question to resolve is whether the assignment of a private sector representative in a formal arrangement under the authority of an MOU establishes that person as an agent for the law enforcement organization. In many cases, this will be largely influenced by state law.
- ◆ Determination of an acceptable method to share sensitive information and intelligence.
- ◆ Ethical issues to ensure that an agency is not sharing information that favors one competitor over another.

Conversely, private sector barriers to law enforcement include the following:

- ◆ The reluctance to share proprietary information even if related to a potential threat.
- ◆ Foreign-owned companies are reticent to share any information with governments in the United States.
- ◆ As a rule, the private sector does not want to risk information becoming public that could harm profit.

While these information sharing barriers are not insurmountable, they require nontraditional and creative resolution to address legal controls, information security concerns, and legitimate corporate interests.

**TABLE 9-2: SAMPLE COMPONENTS OF A RELEASE AND NONDISCLOSURE AGREEMENT REGARDING PROPRIETARY INFORMATION**

- ◆ Identify the specific type of proprietary information needed.
- ◆ Provide a clear rationale for why the information is needed to prevent or mitigate terrorism or criminal offense or to meet a public safety need.
- ◆ Define the conditions under which the private sector entity would release the information.
- ◆ Articulate any unique stipulations to the distribution of the information.
- ◆ Define the information security requirements to be used to protect the proprietary information.
- ◆ Describe the time frame, if any, for which the information release is authorized.
- ◆ Describe how the information is to be handled after the threat requiring the information has passed.
- ◆ Stipulate sanctions, processes, or other remedies to be imposed should the information be inappropriately disclosed or disseminated.
- ◆ Ensure that the agreement is signed and dated by both the public sector and private sector authorizing agents.

**Obstacle 2: Lack of Trust.** Surveys by DOJ<sup>654</sup> have consistently found the level of trust between law enforcement and private sector security to be quite low. The two sectors often view each other as having separate goals and different constituencies. For example, the law enforcement agency's constituency is the community it serves, whereas the constituency of the private sector includes not only a broader community but also its investors, who go far beyond the local community. There is also an often-unstated belief by both law enforcement and the private sector that if one cooperates, the other may not reciprocate. Contributing to the distrust is that in some instances, private security is seen as not being equal to sworn law enforcement. Of course, private security capability is quite broad, ranging from security guards to sophisticated investigators and analysts.

<sup>654</sup> Ibid.



BJA noted that to develop trust, law enforcement executives and their staff members must:

- ◆ Create a vision and passion that brings workers together.
- ◆ Deliver what is promised.
- ◆ Ensure consistency. Constant change or change that is not understood destroys credibility.
- ◆ Communicate.
- ◆ Draw out and address past suspicions and concerns.
- ◆ Pay attention to detail.
- ◆ Train law enforcement personnel and private sector partners together.
- ◆ Ensure equity and equality. Both sides must produce their share of work and be recognized for it.
- ◆ Reinforce the importance of the partnership (with an emphasis on sharing the credit for successes).
- ◆ Admit mistakes and learn from them. Both sides will make errors.

**Obstacle 3: Misinformation and Misunderstanding.** One of the major causes of lack of trust is misinformation and misunderstanding. Often, neither law enforcement nor the private sector has a complete understanding of what the other does or can do. Collectively, these have often been viewed as insurmountable barriers by both parties. Successful partnerships demonstrate that the barriers can be overcome; however, leadership, commitment, and work are required to resolve the barriers.

How can these obstacles be overcome? BJA recommends using the “4 C’s”:<sup>655</sup>

**Communication**—Goals, plans, the types of information to be shared, and concerns should be clearly and unequivocally stated by both parties.

- ◆ **Cooperation**—Overt efforts must be made to reach out to the other—each party will have “wins and losses,” the need to develop creative ways to share information should be paramount to establish a trusting relationship.
- ◆ **Coordination**—Be certain that the actions and responsibilities of each party are clearly articulated to ensure that there is no duplication and that all activities mesh well in a seamless public-private information sharing environment.

<sup>655</sup> BJA, *Ibid.*, p. 5.

- ◆ **Collaboration**—Not only work together, but plan together—each should rely on the expertise and strengths of the other.

## TWO CRITICAL ISSUES TO RESOLVE: SHARING CRIMINAL INFORMATION AND PRIVATE PROPRIETARY INFORMATION/INTELLECTUAL PROPERTY

The sharing of criminal information with a private partner has concerns and restrictions related to civil rights, state law, criminal intelligence records regulations and policy, and operational security issues. Most issues can be resolved; however, they will require carefully crafted policies, MOU provisions, and training. A critical issue for law enforcement is the sharing of information when individuals or organizations are identified—this is the point where constitutional protections attach.

Perhaps the easiest issue is how to share information related to criminal intelligence when individuals and organizations are *not* identified. This may be information about threat conditions, threat indicators, and advisories related to unspecified threats. In these cases, the information sharing restrictions essentially focus on the right-to-know and need-to-know requirements. The MOA between both parties should be written in such a manner that the private sector representative becomes an agent of the law enforcement entity, thereby giving the representative the right to know. Need to know is determined on a case-by-case basis, just as it should be for law enforcement personnel.

The greater challenge is how to lawfully share information with private sector partners that identifies individuals and organizations. When a person or organization is identified, constitutional rights and more stringent restrictions attach to the information and information sharing process. The ability to share this information with private sector personnel hinges on two important issues. The first is how state law deals with privacy issues and, in particular, whether a private sector partner is deemed to be an agent of the law enforcement agency. The second issue is the right-to-know and need-to-know standards, which apply in the same manner as described above. Essential to success are careful crafting of the MOA, training for all parties, and a secure information sharing process.

Just as there are legal and operational restrictions on sharing criminal information, there are corporate restrictions on sharing proprietary information that belongs to businesses.

Proprietary information is patented, copyrighted, and/or trademarked information that describes a product, a process, a design, and/or a formula that was developed or purchased by a private organization and is part of that organization's business processes. This includes, but is not limited to, financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and "know-how" clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information.

To be proprietary, the information must have been developed by the private entity and not be available to the government or to the public without restriction from another source; for example, the formula for a soft drink, a software code, the business plan

## DEVELOPING THE MESSAGE TO PRIVATE SECTOR PARTNERS

- ◆ There should be a consistent message to private sector partners.
- ◆ However, recognize that:
  - Different types of substantive information may be disseminated to different partners; and
  - Somewhat different information will be sought from different partners.
- ◆ The message should emphasize the law enforcement agency's responsibility to contribute to community safety.
  - This is somewhat parallel to a neighborhood watch or a business watch.
- ◆ Key components of the message:
  - We need your help to protect our community by reporting suspicious activity that you observe.
  - We will provide you information on what to look for.
  - We will provide you with details on the reporting process.
  - The process is designed to protect the rights of innocent persons.
- ◆ Goal: To convey to partners their obligation to community safety through a structured process that protects citizens' civil rights.

of a company, a business marketing list, or the components of a computing device are all examples of proprietary information. The nature of proprietary information can range on a very broad spectrum—essentially, for every product and every business in the world, there is conceivably some form of proprietary information that is typically not shared because of concern over aiding competitors or undermining one’s success in the marketplace.

In some cases, proprietary information may be relevant to the prevention or mitigation of a criminal incident or emergency. For example, the design of a production or shipping facility, the location of storage and backup sites, the compounds in a chemical product, or the process to disable some type of device. In such a circumstance, it is hoped that the private entity would share proprietary information with law enforcement. To accomplish this, the law enforcement agency must recognize the magnitude that such a request holds—disclosure of the information could undermine the success of the company. While the law enforcement agency sees the value of learning such information, it must also be cognizant of the risk that the information poses to its private sector partner. It is good practice to have a procedure for the release of proprietary information and a statement of release and nondisclosure signed by both parties. Examples of components of such a document are listed in Table 9-3.

## DEVELOPING A SUCCESSFUL P3I

Successes in P3I require a collaborative effort and effective plan. In its study of public-private relationships, BJA identified 12 essential components to be developed. These components can be used as a road map to create a PPP. To begin, the law enforcement agency must articulate its vision and responsibilities for each of the factors below (see Figure 9-1). The response to each factor is then reviewed and refined by those responsible for establishing and managing the partnership. The final implementation plan, including commitments of personnel and resources is reviewed, refined (as necessary), and affirmed by the chief executive. The critical factors to be addressed in this process are as follows:

- ◆ Negotiate and develop common goals.
- ◆ Identify and develop common tasks for both law enforcement and private sector personnel.
- ◆ Develop knowledge of the capabilities and goals of participating agencies and businesses.
- ◆ Articulate well-defined projected outcomes.
- ◆ Establish a reasonable timetable for implementation.
- ◆ Provide training on the concepts, purpose, and tasks for all involved.
- ◆ Clearly identify the tangible purposes of the partnership.
- ◆ Clearly identify leaders and those responsible for tasks and goals.
- ◆ Create an operational guide on how the partnership will function after it is implemented.
- ◆ Secure an agreement by all partners as to how the partnership will proceed, including resources and responsibilities.
- ◆ Articulate a mutual commitment to providing necessary resources.
- ◆ Establish an assessment and reporting process.<sup>656</sup>

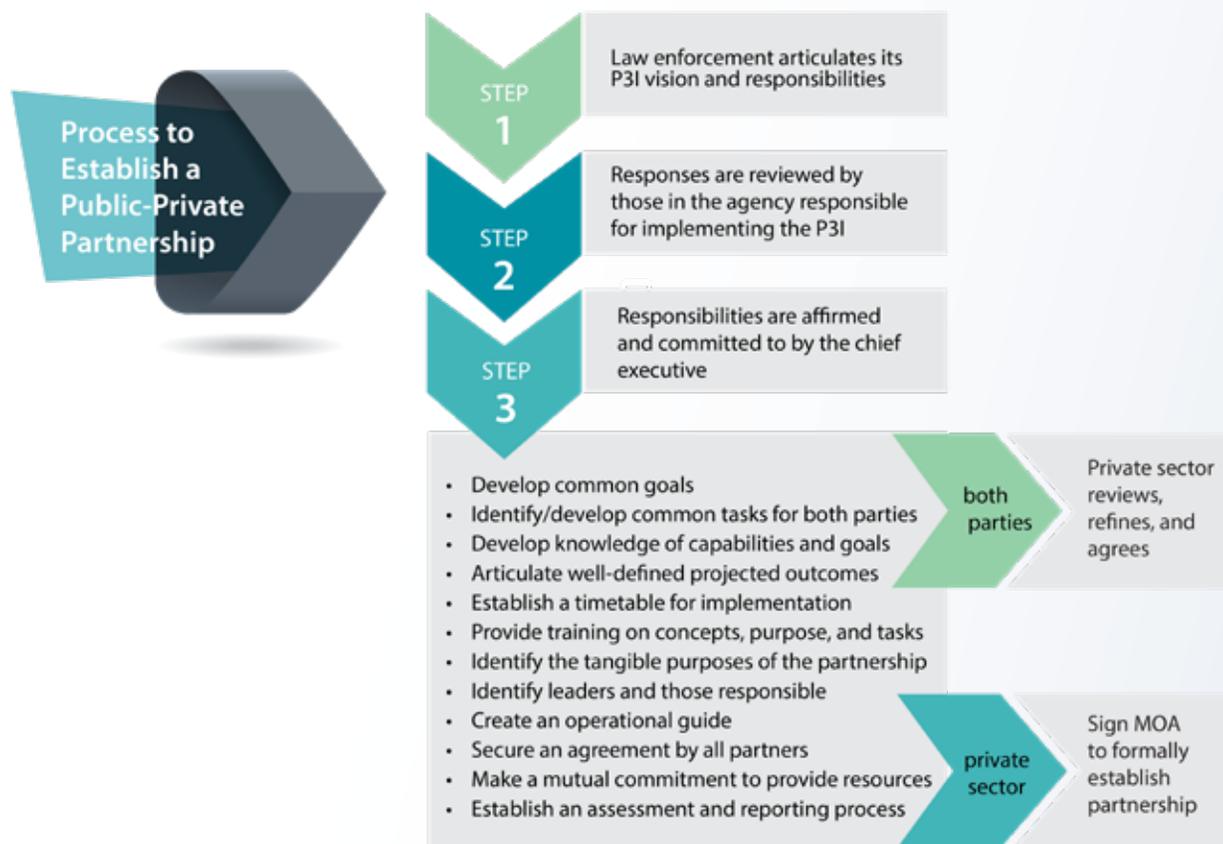
Following this process provides a solid foundation and a clear purpose for the partnership, with a demonstration of support and commitment by the chief executive. Collectively, this represents an explicit development plan that may be submitted to potential private sector partners. If the partnership is going to move forward, the private sector must agree to its responsibilities associated with the above factors. There may need to be a negotiation process on certain elements of the plan, which the law enforcement agency must reasonably consider. In the end, each

---

<sup>656</sup> Adapted from: BJA, *Ibid.*, pp. 5–6.

party must agree to its responsibilities and commitments before the partnership is finalized. The development and implementation plan should then move into a joint operational plan with a signed MOA as appropriate.

FIGURE 9-1: ESTABLISHING A PUBLIC-PRIVATE PARTNERSHIP FOR INTELLIGENCE



Attempting to implement critical factors without input from the other party, whether it is the law enforcement agency or the private entity, is a recipe for failure. Remember that in many cases, the private partner will have to “sell” the partnership to a larger corporate structure. As such, demonstrating substantive input into the partnership development process by the private entity can be an important factor in securing corporate commitments.

In developing a PPP in support of the intelligence function, Matthew Simeone of the Nassau County, New York, Police Department identified several key factors executives should consider:

- ◆ **First who, then what:** Make sure the right people were in the right positions in the organization before they decided on strategy.
- ◆ **Tipping-point leadership:** Within every organization, there are people, acts, and activities that exert a disproportionate amount of influence on performance. Consequently, focusing efforts on identifying and then leveraging these factors can enable great change.
- ◆ **Instilling a need for change:** An initiative involving the private sector and information sharing is likely to bring about debate within the agency regarding the type of information that will be shared. Preparing an internal campaign that addresses the anticipated concerns of officers and the value they will receive from the partnership is essential for the partnership to be effective.
- ◆ **Committing the resource:** As has been discussed on previous issues, the failure to commit resources to the partnership is essentially condemning the partnership to failure.

- ◆ **Leveraging the natural leaders:** The person responsible for developing and implementing the PPP must believe in the concept, understand the concept, have the interpersonal and intellectual skills to move the partnership forward, and be respected within the agency as an “informal leader.”
- ◆ **Be open to innovation:** Agencies should be open to user innovation and should encourage creativity and sharing within the agreed-upon guidelines. Just because something has not been done before does not mean it is a bad idea or that it will not work.
- ◆ **Build on established experiences:** While PPPs for intelligence may be new, the agency may have previous public-private experiences related to crime prevention or community policing that can serve as a springboard for the intelligence initiative.<sup>657</sup>

In illustrating the “power of public-private partnerships,” *The Police Chief* provides concrete methods to establishing them.<sup>658</sup> Similarly, the British office of Her Majesty’s Inspectorate of Constabulary (HMIC), which reviews British police forces for the effectiveness of their operations, created a practical guide titled “Private Sector Partnering with the Police Service” that has applications to U.S. policing.<sup>659</sup> Along the same theme, a publication by the START consortium identified 14 field principles across two broad categories for PPPs to be successful.<sup>660</sup>

#### PRINCIPLES FOR GOVERNMENT ACTORS TO FACILITATE PPPS

1. Identify the division of labor.
2. Reduce barriers to entry for nongovernmental partners.
3. Foster an organizational culture that makes partnering a top priority.
4. Act as an “innovation catalyst.”

#### PRINCIPLES FOR DEVELOPING, IMPLEMENTING, AND SUSTAINING SUCCESSFUL PPPS

1. Have clear goals.
2. Focus on results and measure progress.
3. Involve consumers in developing programs.
4. Involve diverse stakeholders from the start.
5. Identify and utilize champions for support.
6. Establish clear governance structures.
7. Adapt to changing conditions.
8. Enable all partners to benefit.
9. Work to maintain momentum and sustain efforts.
10. Balance transparency and confidentiality.

Some examples of different law enforcement-private partnership models will provide additional insight.

657 Adapted from: Simeone, M. J. (2007). *The Integration of Virtual Public-Private Partnerships in Law Enforcement to Achieve Enhanced Intelligence-Led Policing*. Monterey, CA: A thesis prepared for the Naval Postgraduate School, pp. 103–108.

658 <https://www.policechiefmagazine.org/the-power-of-public-private-partnerships-p3-networks-in-policing/>

659 [https://www.nao.org.uk/wp-content/uploads/2013/07/10127\\_Private-sector-partnering-in-the-police-service\\_NEW.pdf](https://www.nao.org.uk/wp-content/uploads/2013/07/10127_Private-sector-partnering-in-the-police-service_NEW.pdf)

660 Beutel, A., & Weinberger, P. (2016). “Public-Private Partnerships to Counter Violent Extremism: Field Principles for Action,” *Final Report to the U.S. Department of State*. College Park, MD: START. [https://www.start.umd.edu/pubs/START\\_State\\_PublicPrivatePartnershipstoCounterViolentExtremismFieldPrinciplesforAction\\_June2016.pdf](https://www.start.umd.edu/pubs/START_State_PublicPrivatePartnershipstoCounterViolentExtremismFieldPrinciplesforAction_June2016.pdf)

## INFRAGARD<sup>661</sup>

In the 1990s, with the rapid growth of computer networking and reliance on computerization for managing many aspects of government and commerce, it was recognized that the U.S. cyber-infrastructure responsible for sustaining the fundamental elements of American life was increasingly vulnerable to terrorist attacks, criminal incursions, and natural disasters. To address this issue, a new initiative in “critical infrastructure protection” was developed by the FBI with the expressed purpose to understand potential threats and develop ways to prevent or mitigate threats. The greatest emphasis was focused on cyberthreats and cybersecurity.

As this initiative developed, it became apparent that a significant portion of the critical infrastructure was owned by the private sector. As such, it was concluded that critical infrastructure could be adequately protected only by developing a two-way information sharing partnership between the government and private sector. It was in this environment that InfraGard was developed.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. It is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI field office territories, each with an FBI special agent coordinator assigned to it. The FBI coordinator works closely with program managers in the Cyber Division at FBI Headquarters.

In its early development, InfraGard was under the direction of the National Infrastructure Protection Center (NIPC), with its focus on cyber infrastructure protection. After September 11, 2001, NIPC expanded its efforts to include physical as well as cyberthreats to critical infrastructures. InfraGard’s mission expanded accordingly.

In March 2003, the NIPC was transferred to DHS, which now has responsibility for critical infrastructure protection (CIP). The FBI retained InfraGard as an FBI-sponsored program and works with DHS in support of its CIP mission, facilitating InfraGard’s continuing role in CIP activities. In addition, the FBI has further developed InfraGard’s ability to support the FBI’s investigative mission, especially as it pertains to counterterrorism and cybercrimes.

The goal of InfraGard is to have ongoing, two-way, substantive information sharing between the FBI and its private sector critical infrastructure partners. InfraGard members gain access to information that enables them to protect their assets and, in turn, give information to the government that facilitates its responsibilities to prevent and address terrorism and other crimes. This information exchange occurs at both the national and local levels for a more comprehensive approach to infrastructure protection.

To accomplish its goal, the FBI established the following objectives:

- ◆ Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cybercrime, and other major crime programs.
- ◆ Increase interaction and information sharing among InfraGard members and the FBI regarding threats to critical infrastructures, vulnerabilities, and interdependencies.
- ◆ Provide members with value-added threat advisories, alerts, and warnings.
- ◆ Promote effective liaison with local, state, and federal agencies, to include DHS.
- ◆ Provide members with a forum for education and training on counterterrorism, counterintelligence cybercrime, and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

---

661 For more information in InfraGard, see <https://www.infragard.org/>.

## JANI-KING JANITORIAL SERVICES TERRORISM AWARENESS PROGRAM

Dallas-based Jani-King International, Inc., the world's largest commercial cleaning franchisor, has announced a training program for its franchisees and employees to provide an additional level of security to the more than 50,000 buildings that Jani-King cleans. Some 10,000 franchisees will be trained to assess potential building and workplace security threats and report them to authorities.

Jani-King believes that an aggressive and proactive approach to terrorism prevention is critical and of benefit to everyone. "The key word here is prevention," says Jani-King President Jerry Crawford. "We want to create a security force multiplier to help reduce the risk of terror threats."

"Jani-King is one of the only businesses where banking institutions, major corporations, educational facilities, nuclear power plants, and utilities literally hand over the keys to their buildings and provide access to secure areas," says Crawford. "We feel an obligation to put into action additional measures to help keep these buildings safe."

Crawford explained that Jani-King's training program would specifically educate employees and franchisees on three key areas that are important to terror prevention: awareness, identification, and reporting. "The training will consist of awareness of potential security threats, recognition skills, and proper reporting channels," says Crawford. "Franchise owners will not be trained to confront suspicious persons." Crawford gave an example. "Our crews clean the same buildings night after night. We see the normal activity. We want our employees to understand how to spot suspicious activity and then how to report it."

<http://www.bizjournals.com/dallas/stories/2004/09/13/daily13.html>

InfraGard is a solidly conceived and developed program. As might be expected, more substantive information exchanges tend to occur at the local level, while the national level initiatives are important for setting the tone for the public-private partnership. Critical to the success is having a special agent coordinator who fully understands the concept and its value and immerses him- or herself in the partnership to ensure that it is productive.

## SECURITY/POLICE INFORMATION NETWORK (SPIN): NASSAU COUNTY, NEW YORK

The Nassau County Security/Police Information Network<sup>662</sup> (SPIN) is a dynamic, multidimensional crime prevention partnership between the Nassau County Police Department and the private sector that seeks to increase public safety through the sharing of important and timely information. This program is designed to promote homeland security initiatives and business continuity, as well as foster the exchange of information that is critical to the success of protecting Nassau County residents and businesses.

The goals of SPIN are to share information, identify and discuss crime trends and solutions, and work together toward the common goal of protection of persons and assets. SPIN enables the police department, or any other county agency, to send out information to the general distribution group or to a specific sector (e.g., colleges/universities, hospitals, schools, malls/retail, utilities, petroleum, technology, hotels/motels, financial institutions, corporate security, civic leaders). In addition, SPIN connects local, state, and federal law enforcement agencies operating in Nassau County, as well as public transportation and other governmental agencies. As a result, SPIN's multitiered approach allows messages to be tailored for law enforcement, vetted security directors, or chambers of commerce and civic organizations.

SPIN members are contacted by email of unfolding situations as they occur. Messages include notifications of bank robberies, major road closings, disruptions in public transportation, major fires or explosions, civil disturbances, public health or weather-related emergencies, or any other situations involving public safety or effecting continuity of business. In addition, Sex Offender Registry notifications are sent to vulnerable entities using SPIN. Members can utilize SPIN to share information or to inquire about safety matters or concerns.

The establishment of such a comprehensive network has applications that are far-reaching in scope, such as aiding in the capture of felony suspects; notifying participants of the latest crime trends; helping the continuity of business through traffic delay notifications; and facilitating the large-scale exchange of information. The network also provides the police department with the ability to provide training materials to participants that will enhance the safety of all who live and work in Nassau County. Informational meetings are held as necessary to discuss timely security-related issues. Meeting topics have included domestic terrorism, the Republican National Convention, gang awareness, and the *National Response Plan*.

<sup>662</sup> <https://www.pdcn.org/143/SPiN>

Recognizing the vast amount of knowledge, expertise, and resources in the private sector, SPIN recently expanded the scope of its PPP with the formation of a Security Advisory Council. Utilizing the expertise of security professionals and police officers, the council is focused on the establishment of guidelines promoting homeland security, crime prevention, and crime reduction techniques, as well as working towards a coordinated response to critical incidents. The Security Advisory Council’s first project, “Digital Video Surveillance Guidelines,” was recently completed. The guidelines were presented at a SPIN meeting and then posted to the departmental website.

SPIN, in partnership with the Nassau County Office of Emergency Management, has the ability to send out information to the entire SPIN membership or to any specific sector of private industry that is sorted into its own email distribution groups.

The design of SPIN (see Figure 9-2) is not only logical; it is easily adaptable and scalable to meet the needs of agencies of diverse sizes.

FIGURE 9-2: NASSAU COUNTY, NEW YORK, POLICE DEPARTMENT SPIN PROJECT DIAGRAM



Surrounding its law enforcement core are non-law enforcement government agencies and responsibilities that are among the easiest in which to establish a partnership, as well as meeting and communicating on a regular basis.

Relying on email and a Web portal, SPIN has been comparatively inexpensive to implement, is less labor-intensive than face-to-face initiatives, is fast, and makes it easier for many private sector entities, particularly those with a small workforce, to participate. Yet it has empirically been demonstrated to be highly effective.<sup>663</sup>

## HOMELAND SECURITY, INFORMATION SHARING, AND THE PRIVATE SECTOR

While there is an important role in all aspects of the intelligence process for PPPs, it has been most comprehensively structured via the initiatives of DHS. Directed by legislation, Executive Orders, and Homeland Security Presidential Directives, DHS has developed a comprehensive structure for information sharing. Each of these holds potential for the intelligence process.

The DHS model has established different formal mechanisms to address its relationship with the private sector. These mechanisms are intended to reach beyond the intelligence process and include the diverse elements of the National Strategy for Homeland Security that include processes “to protect, prevent, respond to and recover from” terrorism and other human-made or natural threats to the homeland. The focus of the current discussion is to examine these processes from an intelligence perspective.

### CRITICAL INFRASTRUCTURE SECTOR PARTNERSHIP<sup>664</sup>

Critical infrastructure protection is a shared responsibility among federal, state, local, and tribal governments and the owners and operators of the nation’s critical infrastructure. Partnership between the public and private sectors is essential for three interactive reasons:

1. The private sector owns and operates approximately 85 percent of the nation’s critical infrastructure.
2. Government agencies have access to important information about threats that may disable or destroy the critical infrastructure.
3. Both the private sector and the government control security programs, research and development, and other resources that may be more effective if discussed and shared, as appropriate, in a partnership setting.

Many factors inhibit information sharing for critical infrastructure protection, ranging from limitations by the government for sharing certain types of sensitive information to reservations by the private sector about making business processes available to persons outside the corporate structure. Because of the important, yet tentative, understanding by both parties, mechanisms had to be put in place to enhance the sharing of important information yet protect the responsibilities of each. Presidential Policy Directive 21 (PPD-21) and the NIPP provide the overarching framework for a structured partnership between government and the private sector for protection of CI. This sector partnership structure encourages formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to facilitate communication and enhance information sharing policies and practices.

**Sector Coordinating Councils.** As stated previously, the term “sector” refers to businesses that share a common or closely related product or service. Often, members of a sector are business competitors—such as Delta Airlines and United Airlines in the aviation sector—yet they also share common risk and security problems. In the case of homeland security, sectors are identified as they relate to the protection of U.S. sovereignty and citizens, ranging from the provision of important services to the continuity of both government and the economy. SCCs foster and

---

663 For a comprehensive discussion of SPIN, see Simeone (2007). Op. cit.

664 <https://www.dhs.gov/cisa/critical-infrastructure-sector-partnerships>

facilitate the coordination of sectorwide activities and initiatives designed to improve the security of the nation's critical infrastructure. They are self-organized, self-led, broadly representative of owners and operators (and their associations) within the sector, and focused on homeland security and critical infrastructure protection. DHS has a strong preference that each SCC be chaired by an owner and/or operator. Government agencies may suggest the inclusion of various parts of a sector, but it is the responsibility of each SCC to identify the sector's boundaries, establish the criteria for membership, seek broad participation and representation of the diversity of the sector, and establish the governance, business case, and work processes of the sector's SCC.

**Government Coordinating Councils.**<sup>665</sup> The Government Coordinating Councils (GCCs) bring together diverse federal, state, local, and tribal interests to identify and develop collaborative strategies that advance critical infrastructure protection. GCCs serve as a counterpart to the SCC for each critical infrastructure and key resource sector. They provide interagency coordination around CI strategies and activities, policy, and communication across government and between government and the sector to support the nation's homeland security mission. GCCs coordinate with and support the efforts of SCCs to plan, implement, and execute sufficient and necessary sectorwide security to support the CI sector. GCCs can leverage complementary resources within government and between government and CI owners and operators.

## CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL

The Critical Infrastructure Partnership Advisory Council<sup>666</sup> (CIPAC) provides the operational mechanism for carrying out the sector partnership structure. The CIPAC provides the framework for owner and operator members of SCCs and members of GCCs to engage in intragovernment and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities. CIPAC sectors use the same categories of critical infrastructure described previously.

## SPECIAL NOTE: TERRORISM EARLY WARNING (TEW) GROUP

While the structure and processes of the Terrorism Early Warning Group<sup>667</sup> (TEW) concept go far beyond both private sector and intelligence issues, it is noteworthy to recognize the private sector role. The TEW includes analysts from local, state, and federal agencies as well as input from the private sector and non-law enforcement public sector to produce a range of intelligence products at all phases of police responsibility associated with terrorism (pre-, trans-, and post-attack), specifically tailored to the user's operational role and requirements. The TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team using "all source/all phase" fusion, where intelligence is derived from all potential sources (classified, sensitive but unclassified, and open sources) to provide information and decision support at all phases of a threat/response.<sup>668</sup>

In many ways, the TEW epitomizes the concept of "thinking globally, acting locally" because it seeks to identify global distributed threats and achieve an understanding of their impact on a local community. This requires more than simple information sharing—it demands collaborative information fusion and the production of intelligence among cooperative nodes that are distributed among locations where terrorists operate, plan, or seek to attack.<sup>669</sup> As a result, there is a need to develop a diverse array of intelligence in a collaborative and integrated process that encompasses multiple sources, including the private sector.

---

665 <https://www.dhs.gov/cisa/government-coordinating-councils>

666 <https://www.dhs.gov/critical-infrastructure-partnership-advisory-council>

667 [http://www.terrorism.org/wp-content/uploads/2015/12/TEW\\_and\\_National\\_Preparedness\\_Goal-TRC-May2005.pdf](http://www.terrorism.org/wp-content/uploads/2015/12/TEW_and_National_Preparedness_Goal-TRC-May2005.pdf)

668 TEW Information based on Sullivan, J. P. (2005). *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence*. Paper presented at the Canadian Association for Security and Intelligence Studies, Montreal, Quebec, Canada.

669 Ibid.

The TEW concept and approach is based on the recognition that local and regional agencies are producers as well as users of intelligence. The following precepts form a foundation for both individual TEWs and the need to link these TEWs into a national network.

- Intelligence for domestic civil protection (homeland security) is not solely a top-down, federally driven process.
- Intelligence must move top-down, bottom-up, and laterally. There is also a need for bilateral police information sharing and cooperation, independent of federal agencies.
- Local police, public safety, and health agencies may be first to observe indicators.
- The local responsibility is to protect public and craft response.
- There is a need for accountability, structure, and guidelines (i.e., doctrine) for access to national intelligence products.
- Regional entities (such as Terrorism Early Warning Groups) are partners in processing and disseminating intelligence (including providing local context and analyzing products)—there is significant value added by local knowledge.

Further, while an emphasis on prevention and deterrence (P&D) is a critical aspect of TEW operations, the domestic intelligence effort is not exclusively related to supporting criminal investigations or pre-attack, pre-event prevention. Intelligence sharing and access to a wide range of intelligence products are needed during attacks to develop effective consequence management efforts.<sup>670</sup>

Anecdotal evidence suggests that TEW is an effective process for managing complex diverse information, particularly in large, multijurisdictional areas. As mentioned previously, the TEW concept encompasses far more than the intelligence process. As such, it requires greater degrees of partnership collaboration. Nonetheless, it is an initiative that should be explored when considering any aspect of PPPs for counterterrorism.

## LOOKING AHEAD FOR TEWS

While fusion center leaders have not emphasized the TEW groups in recent years, they have still been used by some state and local agencies, such as the St. Louis Fusion Center Terrorism Early Warning Group<sup>671</sup> and the Kansas City TEW Group,<sup>672</sup> because they serve local purposes. Moreover, TEWs may be revisited by many agencies, since the threat environment has evolved. For example, targeted violence,<sup>673</sup> mass shootings,<sup>674</sup> school shootings,<sup>675</sup> and the notable rise in domestic attacks by right-wing extremists<sup>676</sup> are events America's communities are facing that could benefit from the TEW approach.

From a police operational perspective, redefining "terrorism" may be needed. The mass shooting in Las Vegas, Nevada, in October 2017<sup>677</sup> and the series of bombings in Austin, Texas, in March 2018<sup>678</sup> do not appear to be traditional ideological attacks that we associate with terrorism, but the attacks nonetheless terrorized those communities. Revisiting the processes of a TEW with a contemporary vision of mass-violence threats to our communities is a reasonable avenue to explore.

---

670 For more information, see the National TEW Resource Center, Resource Guide at <https://www.hsd.org/?view&did=472872>.

671 [https://www.hsd.org/?abstract&did=760664#:~:text=Louis%20Fusion%20Center%3A%20Terrorism%20Early%20Warning%20Group%20\(formerly%20the,be%20a%20target%20of%20terrorism](https://www.hsd.org/?abstract&did=760664#:~:text=Louis%20Fusion%20Center%3A%20Terrorism%20Early%20Warning%20Group%20(formerly%20the,be%20a%20target%20of%20terrorism).

672 <https://www.hsd.org/?view&did=779710>

673 <https://www.dhs.gov/publication/dhs-strategic-framework-counterterrorism-and-targeted-violence>

674 <https://www.rand.org/research/gun-policy/analysis/essays/mass-shootings.html>

675 <https://www.nytimes.com/interactive/2019/05/11/us/school-shootings-united-states.html>

676 <https://www.csis.org/analysis/rise-far-right-extremism-united-states>

677 <https://www.washingtonpost.com/graphics/2017/national/las-vegas-shooting/>

678 <https://www.cnn.com/2018/03/21/us/austin-explosions/index.html>

## A CRITICAL CHALLENGE FOR PARTNERSHIPS: TECHNOLOGY COMPANIES

There is perhaps no arena where PPPs may be more critical than with technology companies. Three critical issues must be resolved by law enforcement and the private sector and common ground must be found to help ensure community security while protecting privacy and speech.

**Reducing online radicalization through monitoring social media.** There is significant evidence that terrorists and criminal extremists use the Internet to radicalize followers.<sup>679</sup> Initial efforts to remove this type of information from Web pages and social media was met with resistance by the technology companies because such efforts were viewed as limiting free speech. Noting that their users were global, they argued that limiting speech online could be used as a tool by oppressive regimes to quash dissent. However, following a series of terrorist attacks—most notably by white nationalists—it was clear that online hate speech was sparking violence.<sup>680</sup> As a result, efforts are being made by technology companies to eliminate online extremist rhetoric, albeit with limited results.<sup>681</sup> For the current discussion, for the elimination of online radicalization to be most effective, partnerships between technology companies and law enforcement intelligence can begin to target individuals who post content and urge violence. Simply removing content is not enough—it will be reposted until the individuals who post the rhetoric are stopped.

**“Gaining a back door” on encrypted communications applications.** There is evidence that extremists use encrypted applications for communications<sup>682</sup>—most notably WhatsApp<sup>683</sup> and Telegram<sup>684</sup>—to plan attacks and coordinate activities. Indeed, ISIS even has a “help desk”<sup>685</sup> to aid its adherents with their encryption and IT needs. By the nature of the way encryption works,<sup>686</sup> neither law enforcement nor the Intelligence Community can eavesdrop on these communications.

Counterterrorism officials have grown increasingly concerned about terrorist groups using encryption in order to communicate securely. As encryption increasingly becomes a part of electronic devices and online messaging apps, a range of criminal actors including Islamist terrorists are exploiting the technology to communicate and store information, thus avoiding detection and incrimination, a phenomenon law enforcement officials refer to as “going dark.” Despite a vociferous public debate on both sides of the Atlantic that has pitted government agencies against tech companies, civil liberties advocates, and even senior figures in the national security establishment who have argued that creation of “backdoors” for law enforcement agencies to retrieve communications would do more harm than good.<sup>687</sup>

Efforts have been made with technology companies to develop a “back door” for law enforcement, enabling agencies to perform lawful eavesdropping on encrypted conversations. The process is challenging,<sup>688</sup> and there has been little progress in resolving the differences between law enforcement and the technology companies. For the current

---

679 <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2016.1157402>

680 <https://www.itv.com/news/2018-03-02/online-hate-right-wing-terrorism/>

681 <https://www.brookings.edu/blog/techtank/2019/08/07/how-big-tech-and-policymakers-miss-the-mark-when-fighting-online-extremism/>

682 <https://www.express.co.uk/life-style/science-technology/627577/Islamic-State-Terrorist-Attack-Paris-WhatsApp-Encrypted>

683 <https://www.whatsapp.com/>

684 <https://telegram.org/>

685 <https://thehill.com/policy/cybersecurity/268940-new-isis-help-desk-unifies-encryption-support>

686 <https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537>

687 <https://ctc.usma.edu/how-terrorists-use-encryption/>

688 <https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance/>

discussion, a partnership wherein both the government and private sector give a little on their rigid positions and work cooperatively to resolve their differences is likely the most fruitful resolution to this debate.<sup>689</sup>

**Overcoming device security for criminal investigations.** Collecting digital evidence has become a standard practice in criminal investigations. Contacts, texts, email, and searches can be extraordinarily valuable for identifying accomplices, developing evidence for prosecution, and determining whether other crimes or threats are associated with a suspect. Of course, smartphones and tablets have passcodes and/or biometric security. If a suspect will not access his or her device—even under court order—or is incapable of accessing the device (because of incapacitation or death), then law enforcement needs the cooperation of the technology company to open the device. Unfortunately, this has not always been successful, and instead of building partnerships, law enforcement and the technology companies have been at loggerheads.

As an example, in trying to access the content of a suspect’s cell phone following the terrorist attack in San Bernardino, California, to look for further leads:

...the FBI wanted to crack the PIN code on the device. The bureau got a court order and demanded that Apple write special software to thwart security measures that otherwise threatened to erase its content if muscled through. Apple refused to help and took its case public. The two sides battled it out in court, in Congress and in the media. Apple argued such software amounted to a master key and would encourage other countries, like China or Russia, to make similar demands for other iPhones. The law enforcement community said that increasingly secure encryption was making devices “warrant-proof.”<sup>690</sup>

Because of these challenges:

[The FBI director] renewed a call for tech companies to help law enforcement officials gain access to encrypted smartphones, describing it as a “major public safety issue.” Wray said the bureau was unable to gain access to the content of 7,775 devices in [the last fiscal year]—more than half of all the smartphones it tried to crack in that time period—despite having a warrant from a judge. “Being unable to access nearly 7,800 devices in a single year is a major public safety issue.”<sup>691</sup>

All three of these areas pose major obstacles because the issues are complex. The best way to overcome them is through functional and meaningful partnerships. As noted by the *Center for Long-Term Cybersecurity*:

Given the range of cyberthreats facing the United States, the government needs to work in partnership with the private sector to increase its ability to counter incoming cyberattacks on the nation. One way to do so is for the public and private sector to plan and exercise together for combined, voluntary operations that the government and companies can prepare to conduct under their own legal authorities and terms of service agreements.<sup>692</sup>

---

689 While somewhat tangential to the specific application of PPP to SLTLE, two papers developed in a PPP that may be insightful to the reader may be found at [https://www.odni.gov/files/PE/Documents/10---2017-AEP\\_Going-Dark.pdf](https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf) and [https://www.dhs.gov/sites/default/files/publications/2018\\_AEP\\_Going\\_Darker\\_Phase2.pdf](https://www.dhs.gov/sites/default/files/publications/2018_AEP_Going_Darker_Phase2.pdf).

690 <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption>

691 [https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef\\_story.html](https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html)

692 Reiber, J. (2019). *A Public, Private War: How the U.S. Government and U.S. Technology Sector Can Build Trust and Better Prepare for Conflict in the Digital Age*. Berkeley, CA: Center for Long-Term Cyber Security, p. 3. [https://cltc.berkeley.edu/wp-content/uploads/2019/12/PublicPrivateWar\\_J\\_Reiber.pdf](https://cltc.berkeley.edu/wp-content/uploads/2019/12/PublicPrivateWar_J_Reiber.pdf)

## CONCLUSIONS

The intent of this chapter was to emphasize the importance of P3I and the value such partnerships can bring to the intelligence process. Processes were described for developing and implementing PPPs as well as identification of some challenges that will be encountered. Even with the value of P3I, such partnerships require creativity, collaboration, and flexibility by both parties to be effectively developed. There will be challenges that lack clear resolution and new relationships that alter the status quo. Nonetheless, the value gained can be of significant importance for the protection of our communities.

Currently, most PPPs with law enforcement are comparatively simple and often for explicit, short-term purposes, despite the frequent call for more elaborate partnerships. Clearly, partnerships with critical infrastructure owners and operators are the most prolific. Future partnerships will most likely focus on technology, wherein the private sector has greater expertise and data—from the use of private genealogy DNA databases to identify criminal offenders<sup>693</sup> to the use of corporate algorithms for crime and intelligence analysis<sup>694</sup> to police agencies' use of social media.<sup>695</sup> Both benefits and challenges await us.

---

693 <https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.2006906>

694 <https://www.palantir.com/solutions/law-enforcement/>

695 <https://www.entrepreneur.com/article/233604>

## CHAPTER ANNEX 9-1: PUBLIC-PRIVATE PARTNERSHIP EXERCISE

### “SUDDEN IMPACT”: COMMUNICABLE CATTLE DISEASE EXERCISE DODGE CITY, FORD COUNTY, KANSAS

(Funded by the National Institute of Justice)

#### INTELLIGENCE CASE STUDY

#### SUDDEN IMPACT: THREAT PLANNING FOR INFECTIOUS DISEASE IN CATTLE

The following is an actual case study from Ford County (Dodge City), Kansas. Ford County, Kansas, is one of the largest areas for cattle production in the United States. Tens of thousands of heads of cattle are raised and processed here every year. Because of the critical role cattle play in the American food supply as well as the economic impact of the cattle industry in Kansas, the Kansas Bureau of Investigation (KBI) and the Ford County Sheriff’s Office developed a program, with funding support from the National Institute of Justice, to determine how public safety organizations can best work with private sector cattle farms, sale barns, and processing plants in the event an infectious disease is introduced either intentionally or through natural causes.

Particular challenges of the exercise were as follows:

- ◆ Information sharing
  - Would cattle producers provide sufficient critical information, including proprietary information, to public safety officials related to the identification/discovery of an infectious disease and the status of cattle from feedlots to processing to shipping?
  - What types of information could the public safety sector provide to the cattle industry with respect to threats, particularly as related to sensitive information and with consideration for privacy issues?
  - What types of public health information would be needed, and how could it be shared, particularly as related to health privacy laws (notably HIPAA)?
- ◆ Interruption of operations
  - How would the cattle industry respond to public safety requests to reduce or stop operations should an emergency occur?
  - What authority do public safety agencies have to mandate the closure of private sector operations in such an emergency?
  - At what point is the public safety threat “sufficient” to warrant a halt in cattle production operations?
  - What effect would such actions have on the local economy, and to what extent should such factors be considered in halting operations?

While there were many other aspects of the exercise, particularly as related to emergency responses, these emerged as the most critical for the current illustration. Following a comprehensive simulation exercise, it was apparent that private sector businesses and public safety officials had distinctively different perspectives on these issues, although extensive meetings and agreements had taken place prior to the simulation.

Some of the issues that emerged included the following:

- ◆ Law enforcement agencies tended to take an aggressive stance, giving orders rather than working cooperatively.
- ◆ Law enforcement agencies were reluctant to share certain types of information about threats, suspects, and associated facts under the assumption that it was improper to share this information with the private sector.
- ◆ Private companies tended to withhold certain types of critical information under the assumption that it would “not be understood” by public safety officials.

- ◆ Private companies resisted shutting down all operations to avoid the economic impact of such actions.
- ◆ Private companies argued against stop orders of cattle that were already in shipment because of the anticipated economic impact. Conversely, law enforcement tended to dismiss the economic variables.

One of the lessons learned from this exercise was that despite extensive planning by a wide variety of people with the intent to find the best method to handle an emergency, additional planning was necessary. Both groups viewed the issues from significantly different perspectives.

PPPs are necessary and can be effective. However, they are not easy. The stress and disagreement arising from an exercise such as the one described would be magnified under the conditions of an actual threat. Hence extensive planning, communications, training, and exercising are essential.





# CHAPTER 10

## MANAGING INFORMATION: A CLOSER LOOK AT SUSPICIOUS ACTIVITY REPORTS, INTELLIGENCE REQUIREMENTS, COLLECTION, AND ANALYSIS



It is all about the information. Raw information is the fuel that drives the intelligence process. The information flow should be constant and bidirectional and should originate from a diverse array of sources. Managing this information relies on a number of processes that have been introduced in previous chapters. The intent of this chapter is to build on the discussions of these processes with more detail, providing insight into current intelligence applications for information management. Because of the rapid evolution of law enforcement intelligence—particularly as influenced by fusion centers, the adoption of intelligence-led policing, and the use of intelligence in real-time crime centers—there is value in a closer examination of these integrated processes as tools for both the information collector and the intelligence consumer.

### SUSPICIOUS ACTIVITY REPORTING

Law enforcement intelligence has long used information—both solicited and unsolicited—to learn about criminal threats. Traditionally referred to as tips and leads, this information was most commonly provided to the intelligence function by officers, informants, and, sometimes, other members of the community. In some cases, intelligence personnel would disseminate specific types of information or descriptions of people they were seeking to uniformed officers in the hope of using the “extra eyes” of the patrol force to generate new information. While criminal investigators and patrol officers regularly relied on the public for information—such as through Neighborhood Watch or Crime Stoppers—use of the public was far less common for the intelligence function.

As the philosophy and processes of intelligence have changed, so have the processes related to tips and leads. It has been recognized that there is value in a proactive process to generate more reports of suspicious behaviors. Furthermore, a more structured process was needed to capture, evaluate, store, and share this information. This process has evolved with coordinated development by the Criminal Intelligence Coordinating Council (CICC); the U.S. Department of Homeland Security (DHS), in particular the Office of Intelligence and Analysis; and the U.S. Department of Justice (DOJ), particularly the FBI. These initiatives collectively refer to the management of tips and leads through the use of suspicious activity reports (SARs).<sup>696</sup>

Here is a formal description of a SAR from DHS:

Official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.<sup>697</sup>

A further description of suspicious activity reporting was provided in a project report by the Major Cities Chiefs Association with support from DOJ, DHS, and the Global Justice Information Sharing Initiative (Global). The report stated:

The Suspicious Activity Report (SAR) process, as defined in this paper, focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime—and establishing a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism.<sup>698</sup>

At this point, a key question to ask is whether tips, leads, and suspicious activity reporting affect the prevention/intervention of a crime or serious incident. In a study on the use of tip lines in public schools funded by the National Institute of Justice, survey respondents perceived tip lines as an effective school safety strategy. Findings included the following:

- ◆ Seventy-seven percent believed that their tip lines made them more aware of safety issues at their schools.
- ◆ More than fifty percent said that their schools' tip lines had prevented violent incidents.
- ◆ Two-thirds believed that their tip lines allowed their schools to respond more effectively to bullying.
- ◆ Seventy-three percent reported that their tip lines had prevented incidents of self-harm or suicide.<sup>699</sup>

While that research was not on SARs, per se, it nonetheless demonstrates the value of non-law enforcement reports of suspicious activity. Research specifically on SARs has found that the process is effective in prevention. Specifically, the observed activities of:

---

696 There are two types of SARs. One type deals specifically with financial transactions, wherein financial institutions must report large cash transactions as suspicious activity. For more information on financial SARs, see <https://www.fincen.gov/sites/default/files/shared/TheNewFinCENSAR-RecordedPresentation.pdf>. The other type of SAR, which is the current topic of discussion, is a general report of suspicious activity that may be criminal behavior.

697 *Information Sharing Environment Functional Standard for Suspicious Activity Reporting*, Version 1.5.5. (2019). Washington, DC: Department of Homeland Security. [https://www.dhs.gov/sites/default/files/publications/15\\_0223\\_NSI\\_ISE-Functional-Standard-SAR.pdf](https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf)

698 Suspicious Activity Report Support and Implementation Project. (2008). *Final Report*. Washington, DC: Major Cities Chiefs Association; U.S. Department of Justice and U.S. Department of Homeland Security, p 1. [https://bja.ojp.gov/sites/g/files/xykxuh186/files/media/document/sar\\_report\\_october\\_2008.pdf](https://bja.ojp.gov/sites/g/files/xykxuh186/files/media/document/sar_report_october_2008.pdf)

699 Planty, M., Banks, D., Lindquist, C., Cartwright, J., & Witwer, A. (2020). *Tip Lines for School Safety: A National Portrait of Tip Line Use*. Research Triangle Park, NC: RTI International/National Institute of Justice.

. . . making threats, conducting surveillance and terrorist recruitment/financing *predict law enforcement interdiction* [emphasis added] in terrorism plots, while misrepresentation (or the manufacturing and use of false documents) is more associated with terrorist success.<sup>700</sup>

This research is very explicit and provides useful evidence-based guidance on the types of suspicious activity that are likely to be most useful for the intelligence process.

## THE DEBATE: SHOULD SARs BE LIMITED TO TERRORISM INFORMATION?

Tips and leads had been used by state, local, and tribal law enforcement (SLTLE) to deal with crimes in their communities—burglary, gangs, illicit drugs, auto theft, and so forth. However, in the immediate post-September 11, 2001 (post-9/11), environment, there was a prioritized focus on developing a standardized process whereby SARs could be shared among agencies to help detect and prevent terrorism and terrorism-related criminal activity. Standards and processes were developed by the Program Manager for the Information Sharing Environment (PM-ISE) to both add structure to SAR sharing processes and ensure the protection of privacy, civil rights, and civil liberties (P/CRCL).

There was debate, however, in the state and local law enforcement community about whether SARs should be limited to focus only on terrorism or whether they should embrace all crimes. For those arguing the limitation of SARs to terrorism, the logic was that this makes law enforcement processes consistent with the Information Sharing Environment (ISE) and enhances the ability to share this type of information. Moreover, it was argued that limiting SARs to terrorism-related information may reduce the potential for collecting information where there is no criminal nexus. A final point in this argument was that having all-crimes SARs generates too many unfounded reports, which, in turn, consumes staff time that could be more effectively focused elsewhere. Each of these arguments has merit, notably as applied to major urban areas of the United States.

Those opposing this limitation, such as the definition provided above from the Major Cities Chiefs Association, argue that their intelligence units and fusion centers are designated as all-crimes, all-hazards intelligence entities. As such, limiting SARs to terrorism information would result in missing potentially important information about non-terrorist crimes. In many—if not most—jurisdictions around the United States, intelligence units or fusion centers spend more time on crime than on terrorism. Moreover, it is argued that crimes can occur which, at first review, may appear to be non-terrorist. However, further inquiry may show that there is a terrorism nexus. If this original information is not collected in a SAR, then the lead to a terrorist incident may be lost. As noted in a report of the Global Intelligence Working Group:

It may be difficult to determine whether a single incident occurring within a local jurisdiction has a nexus to terrorism, but it is important to acknowledge that many outwardly unrelated tips, leads, and suspicious incidents may in fact be related and could have multijurisdictional and national implications when analyzed, shared, and combined with other seemingly unrelated information at the local, state, regional, and federal levels. Terrorist activities are being funded via local-level crimes, and state, local, and tribal law enforcement officers in our communities are best positioned not only to observe criminal and other activity that might be the first signs of a terrorist plot but also to help thwart attacks before they happen.<sup>701</sup>

Further complicating the issue was defining terrorism. Federal agencies relied on a fairly specific approach largely based on federal statutes:

---

700 Gruenewald, J., et al. (2019). "Suspicious Preoperational Activities and Law Enforcement Interdiction of Terrorist Plots." *Policing: An International Journal*. Volume 42, Issue 1, p. 89. DOI: 10.1108/PIJPSM-08-2018-0125.

701 Global Intelligence Working Group. (2007). *Privacy Committee Report: Tips and Leads Issues Paper*. Washington, DC: Global Justice Information Sharing Initiative, U.S. Department of Justice, p. 4.

**International terrorism:** Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

**Domestic terrorism:** Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.<sup>702</sup>

State and local law enforcement viewed terrorism somewhat more broadly to include mass-casualty shootings, school shootings, and incidents within a community that “terrorized residents.”<sup>703</sup> Nonetheless, the federally funded SAR initiative developed for fusion centers, and by extension state and local law enforcement, retained a terrorism focus based on federal definitions and guidelines from the ISE.

Many SLTLE agencies continued to collect and process SARs on all crimes; however, they were not as broadly shared because without the terrorism nexus they could not be placed in the information system of the *Nationwide SAR Initiative* (NSI) (discussed later).

This is beginning to change, however. A new initiative by DHS, called the National Threat Evaluation and Reporting (NTER) program, looks to advance SLTLE ability to identify, evaluate, and report/share tips and leads linked to emerging homeland security threats, including those associated with potential mass-casualty incidents, targeted school/workplace violence, etc., in addition to terrorism threats. NTER will provide law enforcement and homeland security partners with additional resources and training to help identify and prevent targeted violence and mass-casualty incidents, including those associated with terrorism, as well as facilitating a national capacity for identifying, evaluating, and reporting/sharing tips and leads related to those threats.

NTER builds on the success of the Nationwide Suspicious Activity Reporting Initiative and will train partners to identify and evaluate threats to homeland security, regardless of motive. However, the reporting of terrorism-specific suspicious activities, as well as the associated training programs of the NSI, will continue to exist as a part of the NTER program.

Some key changes planned for the program are as follows:

- ◆ Transition from exclusively terrorism-focused incidents to incidents related to mass attacks and targeted violence.
- ◆ Transition from an indicator-based approach to behavioral threat-based approach.
- ◆ There will be increased evaluation of SARs and broader sharing of information.
- ◆ NTER will be managed by DHS, but information related to terrorism will continue to be shared via the FBI’s Sensitive But Unclassified (SBU) eGuardian<sup>704</sup> system.

At this writing, the NTER program is still in the development stage, including gaining input from SLTLE partners. While there is optimism that SARs are expanding beyond traditional categories of terrorism, state and local law enforcement would like to see the NTER program expand to all crimes and all hazards.

---

702 <https://www.fbi.gov/investigate/terrorism>

703 For example, in March 2018, five bombs were planted around the Austin, Texas, area over a three-week period, killing two people and injuring five others. The police chief at the time stated this was terrorism because of its impact on the community, even though in his video confession, the suspect never claimed any ideology. <https://www.foxnews.com/us/austin-package-bomb-attacks-timeline>

704 <https://www.fbi.gov/resources/law-enforcement/eguardian>

## NATIONWIDE SAR INITIATIVE (NSI)

Developing a process to collect and document suspicious activity is only part of the formula. To be effective, there must be a system to validate information in a SAR and share the SAR so it may be integrated with information collected by other jurisdictions. The process must be national in scope, with explicit requirements for processing and evaluating SARs and mechanisms for protecting P/CRCL. That is the role of the NSI.

The NSI was developed in response to recommendations of the 9/11 Commission to increase information sharing at all levels of government, thus increasing the probability of identifying and preventing terrorism threats. The 9/11 Commission found that some suspicious activities performed by terrorists before an attack had been observed by state and local law enforcement or reported to law enforcement by citizens. Yet there was no mechanism in place on a nationwide basis to collect this information in a consistent manner, share it, integrate it, or analyze it. Collectively, this was information that may have been able to prevent or mitigate the 9/11 attacks—yet it was lost.

Based on those findings, the *Intelligence Reform and Terrorism Prevention Act* (IRTPA) of 2004 and the 2007 *National Strategy for Information Sharing* developed the foundation to establish locally controlled information systems wherein potential terrorism-related information could be reported and shared by law enforcement agencies to determine any emerging patterns or trends. As a result, the NSI was created.

Originally developed by the PM-ISE, the NSI is now jointly managed by the FBI (taking the lead on technology) and DHS (as the lead for program management and training).<sup>705</sup> This initiative, which builds on a project originally discussed by the Major Cities Chiefs Association,<sup>706</sup> sought to develop an information sharing mechanism that ensures that all suspicious activity information is compatible; that standard processes are being developed in the way that information is collected, formatted, and exchanged; and that suspicious activity reporting is done in a manner that protects privacy and civil rights. The NSI is a process to make sure there is a common method to get suspicious activity reports through fusion centers that will, in turn, facilitate the exchange of regional and national analyses among law enforcement and counterterrorism partners. Developing a process for collecting and documenting suspicious activity is only part of the need—there must be a process for integrating and sharing SARs with SLTLE agencies.

Hence, the purpose of the NSI was to develop, evaluate, and implement common policies and procedures for the gathering, documenting, processing, analyzing, and sharing of information about terrorist-related suspicious activities. The NSI created a framework to support the reporting of suspicious activity—from the point of initial observation to the point where the information is available to be shared via the FBI's eGuardian system. A key element is that the NSI incorporates state, local, and tribal law enforcement agencies' SAR process into a nationwide effort. Importantly, the distinction has been emphasized between a national system—which meant it was directed by national authorities—and a nationwide system, which meant it was a collaborative effort among SLTLE agencies with federal agencies serving as partners.

The vision is that all agencies, regardless of size or jurisdiction, have a role in the nationwide SAR process—those which do not participate represent a weakness in our system of identifying pre-incident indicators of criminality. Each law enforcement agency's internal SAR process, once developed, can be incorporated into the NSI. Clearly, without the support and participation by local, state, and tribal agencies, the amount of valuable terrorism-related suspicious activity would be limited.

---

<sup>705</sup> <https://www.dhs.gov/nsi>

<sup>706</sup> See *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, <https://it.ojp.gov/gist/103/Findings-and-Recommendations-of-the-Suspicious-Activity-Reporting--SAR--Support-and-Implementation-Project>.

The SAR Functional Standard envisions that agencies will share potential ISE-SAR information with a state or major urban area fusion center and, when appropriate and consistent with existing practice, the local FBI Joint Terrorism Task Force (JTTF). At the fusion center, analysts or law enforcement officers will evaluate the SAR against the ISE-SAR Functional Standard. If the SAR meets criteria as defined in the ISE-SAR Functional Standard, the fusion center will designate the SAR as an “ISE-SAR” and make it available to other ISE participants through the fusion center’s shared space (i.e., computerized information system). Documenting, analyzing, and sharing of ISE-SAR information between and among SLT entities, state or major urban area fusion centers, JTTFs, and federal field components is designed to enable the identification of behaviors and indicators of criminal activity associated with terrorism.

The review and vetting process begins when a front-line law enforcement officer responds to a call for service, self-initiates law enforcement action based on a reported incident or observation, or observes suspicious behavior.

To preclude reporting on individuals involved in innocent activities, front-line personnel must be able to recognize indicators (incidents, behaviors, and modus operandi of individuals and organizations) of criminal activity associated with domestic and international terrorism and must understand the scope of their legal authority to obtain information.<sup>707</sup>

Part of this initiative was the development of a searchable data base that would allow law enforcement agencies to access the information on summary SAR reports through a Web-based portal to which all law enforcement officers have easy access. eGuardian was developed to help meet the challenges of collecting and sharing terrorism-related activities among law enforcement agencies across various jurisdictions. The eGuardian system is a sensitive but unclassified information-sharing platform hosted by the FBI’s Criminal Justice Information Services (CJIS) Division as a service on the Law Enforcement Enterprise Portal (LEEP). The eGuardian system allows law enforcement agencies to combine new suspicious activity reports of incidents with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel and analysts directly supporting law enforcement. The information captured in eGuardian is also migrated to the FBI’s internal Guardian system, where it is assigned to the appropriate JTTF for any further investigative action.<sup>708</sup>

While there is widespread recognition of the importance of identifying and reporting suspicious activities, the initiative is not without its critics. For example, the American Civil Liberties Union commented on suspicious activity reporting, stating that:

This overbroad reporting authority gives law enforcement officers justification to harass practically anyone they choose, to collect personal information, and to pass such information along to the intelligence community. Suspicious activity report policing opens the door to racial profiling and other improper police behavior, and exposes law-abiding people to government prying into their private affairs without just cause.<sup>709</sup>

Because of these concerns, training is essential. It must be emphasized that the focus is collecting information about *behaviors* that represent pre-operational indicators of criminal activity. “Unusual” or “odd” behavior or circumstances would not be included unless there is some articulable relationship between that behavior and a potential crime. Beyond training, it is essential to have ongoing supervision and a substantive assessment mechanism to document the effectiveness of the process.

DHS has taken the responsibility for developing and providing SAR training, dividing suspicious behaviors into two categories:

---

707 See <https://www.dhs.gov/publication/ise-sar-functional-standard?collection=nationwide-sar-initiative>.

708 <https://www.fbi.gov/resources/law-enforcement/eguardian>

709 German, M., & Stanley, J. (2008). *Fusion Center Update*. Washington, DC: American Civil Liberties Union, p. 2.

- ◆ Defined criminal activity and potential terrorism nexus activity.
- ◆ Potential criminal activity or noncriminal activities requiring additional information during vetting.

As illustrated in Figures 10-1 and 10-2, care was taken in developing 16 evidence-based behaviors to ensure protections of constitutional rights and to maximize the accuracy of the information to more accurately forecast threats.

## SUSPICIOUS ACTIVITY REPORTING PROCESSES IN STATE AND LOCAL AGENCIES

An important part of the suspicious activity reporting process is the underlying assumption that many people in their daily lives observe suspicious activity but either do not recognize it or think the suspicious behavior is not of sufficient consequence to report. As will be seen, a goal in the development of SARs is to generate increased reporting of suspicious activity with the belief that as these reports increase, the probability of gaining critical threat information will also increase. However, keys to success are as follows:

- ◆ Recognizing “focused” suspicious activity.
- ◆ Collecting substantive information about suspicious activity.
- ◆ Ensuring that all information about the suspicious activity is reported to the intelligence unit or a fusion center (as opposed to simply being recorded in a law enforcement agency’s records management system).
- ◆ Ensuring that the information is reviewed, analyzed, and, if credible, shared or stored in a searchable database.

Embracing this vision, the Los Angeles, California, Police Department implemented a policy for SARs as related to both international terrorism and domestic criminal extremism. The policy defines a SAR as:

... a report used to document any reported or observed activity or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result of observations or investigations by police officers or may be reported to them by private parties.<sup>710</sup>

The directive further provides specific illustrations of behavior that may be deemed suspicious as well as guidance for reporting the behavior.

This vision of suspicious activity reporting has two integrated dimensions. The first dimension is development of a model for refining suspicious activity processes. The second is broadening the scope of persons who may report suspicious activity.

Regarding the first dimension, suspicious activity can encompass a broad array of behavior. Moreover, what a person defines as “suspicious” will vary depending on that person’s life experiences, values, and other social and demographic factors. Hence, direction must be given so that suspicious activity is defined (and viewed) in the context of the types of information that are lawful and needed for the intelligence process. To accomplish this, a three-part model can be used: Observe, Document, and Report (see Figure 10-3).

---

710 Los Angeles Police Department. (March 5, 2008). *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*. Special Order Number 11, pp. 1–2.

FIGURE 10-1: DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY



FIGURE 10-2: POTENTIAL CRIMINAL ACTIVITY OR NONCRIMINAL ACTIVITIES REQUIRING ADDITIONAL INFORMATION DURING VETTING

**POTENTIAL CRIMINAL ACTIVITY OR NON-CRIMINAL ACTIVITIES  
REQUIRING ADDITIONAL INFORMATION DURING VETTING**

REPORTABLE INFORMATION ARTICULATES FACTS INDICATING HOW EACH BEHAVIOR WOULD AROUSE  
SUSPICION OF TERRORISM OR OTHER CRIMINALITY IN A REASONABLE PERSON

When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.



**ELICITING  
INFORMATION**

Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about an event or particular facets of a facility's purpose, operations, security procedures, etc.



**TESTING OR PROBING  
OF SECURITY**

Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities.



**RECRUITING/  
FINANCING**

Providing direct financial support compiling personnel data, banking data, travel data, or contacts to build operational teams.



**SURVEILLANCE**

An interest in or taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner.



**MATERIALS  
ACQUISITION/STORAGE**

Acquisition and/or storage of unusual quantities of materials (fuel, chemicals, toxic materials, timers, pagers, cell phones, or other triggering devices).



**ACQUISITION OF  
EXPERTISE**

Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities.



**WEAPONS  
COLLECTION/DISCOVERY**

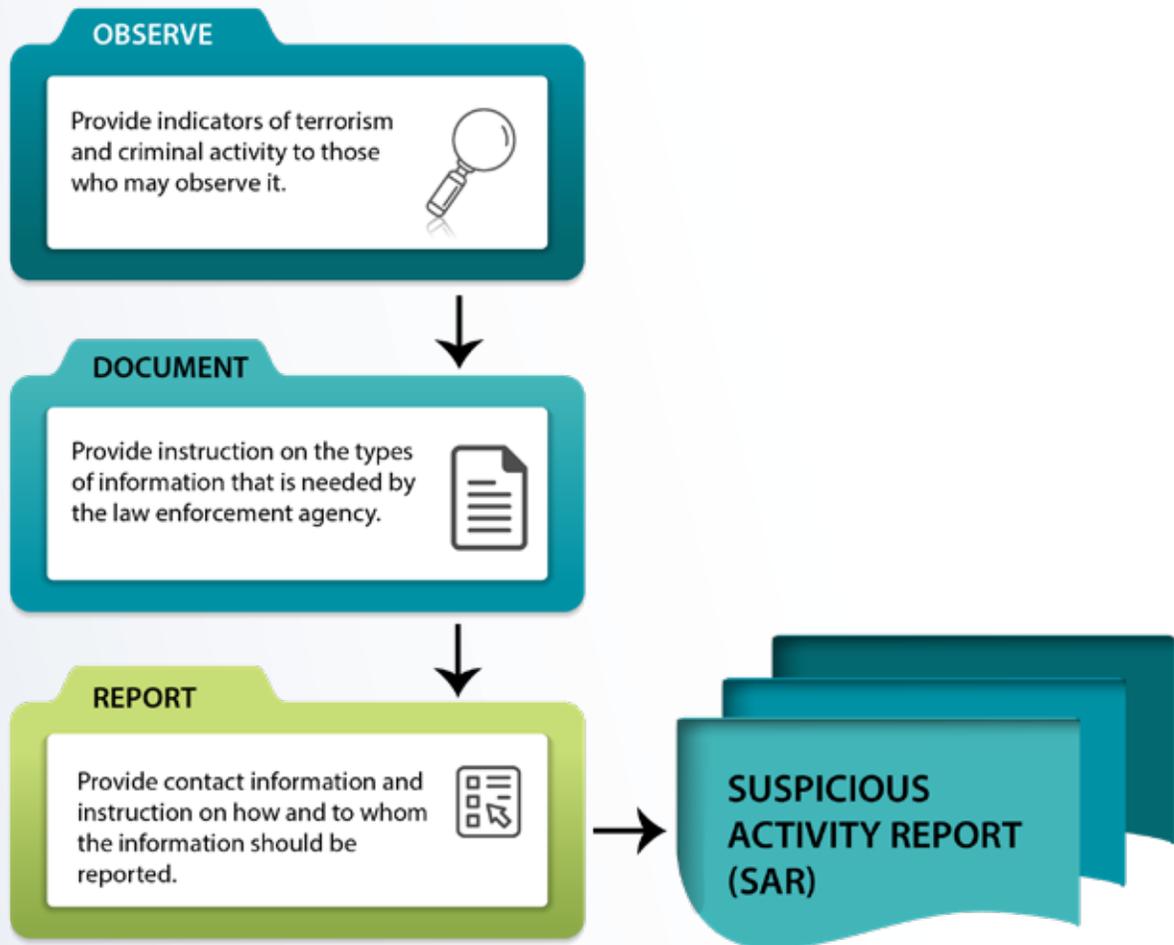
Collection or discovery of unusual amounts or types of weapons, explosives, chemicals, or shows evidence thereof, detonations or other residue, wounds, or chemical burns.



**SECTOR-SPECIFIC  
INCIDENT**

Actions associated with a characteristic of unique concern to specific sectors (e.g., the education, public health, government, etc.), with regard to their personnel, facilities, systems, or functions.

FIGURE 10-3: SUSPICIOUS ACTIVITY REPORTING MODEL FOR THE PUBLIC



**Observe.** It is necessary to be observant; however, observations need to be targeted. Hence, awareness training/ public education is needed to ensure that the behavior that is observed has a potential criminal nexus. Often, training includes providing information about threat indicators—behaviors that are reasonably linked to potentially criminal activities. There are two critical components of indicators: First, the focus must be on *behavior*—not the attributes of an individual. Moreover, there must be a reasonable likelihood that the behavior could be related to a crime; that the behavior is not just “odd” or “unusual.” Attributes of an individual would include perceived<sup>711</sup> race, ethnicity, gender, religion, and so forth. That is, a person *should not* be deemed “suspicious” simply because he or she possesses these attributes—suspicion must be based on *behavior*. If suspicious behaviors are observed and documented as they relate to the preparation or commission of a crime, then the attributes can be properly used as part of the description of the suspicious person. Of course, these guidelines are general and must be applied in the context of circumstances and other information the observer has.

The second critical component is for the observer to understand the types of behaviors and symbols (e.g., gang markings, tattoos, slogans of criminal extremists) that are particularly indicative of criminal activity. This means that observers can benefit from some type of training or information—such as intelligence reports—about suspicious activities.

<sup>711</sup> The word “perceived” is used here because often, an observer sees a characteristic that is mistaken for an attribute. For example, an untrained observer may see a person whom he or she concludes is from the Middle East when, in fact, the person is of a different ethnicity.

For law enforcement officers, training programs are available—both in-class and online—that can provide important contemporary information about threat indicators. One such program that has been highly successful and recently revised is the State and Local Anti-Terrorism Training (SLATT) program funded by the U.S. Bureau of Justice Assistance (BJA). SLATT training provides detailed information to patrol officers and others on indicators of both international and domestic terrorism/criminal extremism, demonstrating how officers may encounter and observe such behaviors during their regular work shifts.<sup>712</sup>

One program directed toward the non-law enforcement community to provide suspicious activity indicators is the Communities Against Terrorism (CAT) program, which was also BJA-funded.

The Communities Against Terrorism program has been created to assist law enforcement in the development of partnerships with community members. Community members who are aware of potential indicators of terrorism activities may provide law enforcement with valuable information. To assist law enforcement in the outreach effort, templates of flyers containing potential indicators have been created for law enforcement to distribute to specific industries.<sup>713</sup>

On the left side of the flyer are behaviors that may be deemed suspicious. Providing guidance to both law enforcement officers and the community on what types of behaviors may be deemed suspicious enhances the quality of the “observe” component of this model.

**Document.** When suspicious activity is observed, the value of the SAR is increased if the observer provides explicit information about the suspicious persons and the specific nature of the suspicious activity. While law enforcement officers are trained to collect this type of information, members of the public, who report a significant amount of suspicious activity, typically do not have this knowledge. Hence, public education programs need to inform community members of the types of information that is most valuable: detailed descriptions of the suspicious persons and their vehicles, location of the activity, the types of actions that appeared suspicious, and any objects the suspicious persons might have had that added to the suspiciousness are types of information that must be documented. Once again, the CAT program provides these types of details that are specific to different types of businesses.

**Report.** Law enforcement officers not only need to understand the NSI standards for observing suspicious behaviors but must be encouraged to report the activities through a department’s SAR procedures. Experience has shown that officers may often record details of suspicious activity observed on a daily activity log but often do not submit a formal SAR. The success of the NSI lies with individual officers and departments recording and reporting suspicious activities so they can be shared.

For community members, reporting suspicious activities has been more problematic. In many cases, information went unreported because the community member simply did not know how or to whom to report this information. For example, at one COPS-funded community education program on suspicious activity, citizens were confused about reporting. One man asked,

Who am I supposed to report this to? The FBI? My police department? The state police? Is this considered an emergency? If so, do I call 9-1-1 to report it? If not, what number do I call?<sup>714</sup>

---

712 See <http://slatt.org>. The website not only provides training schedules but also online training and a wide range of resource materials. For full access to the website, a user must register with employment verification that he or she has a bona fide need for access to the site. Because the program is funded by BJA, there is no charge for the training.

713 CAT flyers may be downloaded at <https://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/>.

714 Personal experience of the author in Topeka, Kansas, at a public education program with the Regional Community Policing Institute of Wichita State University.

While the answers to these questions may seem obvious to an officer, they are less obvious to a community member. Hence, providing such basic information can be useful for increasing public reports. A number of agencies have enhanced this by adopting a “See Something, Say Something<sup>®</sup>”<sup>715</sup> campaign, intended to bring suspicious behavior to the attention of law enforcement.

Law enforcement agencies have been improving their capacity to assist community members in reporting suspicious activities. For example, on one federal website, a person can submit suspicious activity to the FBI or link to other federal agencies.<sup>716</sup> Social media reminders with a links to websites represent a logical method to facilitate public reporting of suspicious activity.<sup>717</sup> Tip lines still have a role, however—not everyone in the community has Internet access.

As another mechanism to facilitate reporting of suspicious activity, the BJA CAT program designed the suspicious activity flyers so that each law enforcement agency could place its reporting and contact information at the bottom.

The goal of these initiatives, of course, is to encourage people to be aware of behavior that is likely to be criminal, capture critical facts about the behavior, and submit this information to a law enforcement agency. In many cases, this information can provide important missing puzzle pieces to an intelligence analyst. In other cases, the information may inform the law enforcement agency of potential criminal activity about which the agency was previously unaware.

Some agencies have formalized the process further. For example, the New York City Police Department created Operation Nexus, which:

... actively encourages business owners, operators, and their employees to apply their particular business and industry knowledge and experience against each customer transaction or encounter to discern anything unusual or suspicious and to report such instances to authorities.<sup>718</sup>

As more initiatives are developed to encourage people to report suspicious behavior, the more likely law enforcement is to identify and mitigate threats. A significant element of this process is to ensure that suspicions are based on *behavior* and that the observer captures as much accurate information as possible to report the suspicious activity.

## SARs AND PERSONALLY IDENTIFIABLE INFORMATION

An important issue related to SARs is whether the report contains personally identifiable information (PII). PII may be defined as any information or data from which a reasonable person may identify a specific individual. When P II is collected, civil rights protections and privacy standards must be afforded to the report that contains the information.

A PII-SAR is a report that names an individual or provides sufficiently specific information where identity could reasonably be established—such as the physical description of an individual and the address where the person lives. In these cases, retention, security, and dissemination guidelines must receive greater attention, with the safest approach of using information management standards that are similar to the 28 CFR Part 23 guidelines.<sup>719</sup> A non-PII-

---

<sup>715</sup> As an example, see <https://www.njhomelandsecurity.gov/njsars>. The reader should be aware, however, that there has been criticism of these campaigns, notably arguing that they lead to racial profiling by community members. See [https://www.huffpost.com/entry/the-dangers-of-see-something-say-something\\_b\\_9060958](https://www.huffpost.com/entry/the-dangers-of-see-something-say-something_b_9060958).

<sup>716</sup> See <https://tips.fbi.gov/>

<sup>717</sup> As an example, see <http://www.kansas.gov/kbi/crimereportmappage.shtml>.

<sup>718</sup> <https://www.nypdshield.org/public/nexus.aspx>

<sup>719</sup> The reader is reminded that 28 CFR Part 23 applies only to criminal intelligence information. However, even if a SAR is not retained as part of the criminal intelligence records system, the guidelines afford recognized civil rights and privacy standards to demonstrate that the law enforcement agency is doing due diligence in protecting individuals’ rights. Actual policies should be reviewed by counsel, with specific reference to the laws of each state.

SAR is a report that describes suspicious circumstances, indicators, and/or behaviors of unknown persons. If PII is not included in the report, then the law enforcement agency has significant latitude on retention and dissemination of the information.

Regardless of the SAR model used by a law enforcement agency, distinct policies with respect to the handling of SARs that have PII and those that do not should be made.

## ESTABLISHING CONTROLS ON SUSPICIOUS ACTIVITY REPORTS/INFORMATION

Information contained in suspicious activity reports is sensitive for several reasons: The basis or motivation for reporting the information, notably that of a community member, and the inherent accuracy of the information are often unknown. As such, law enforcement must determine whether lawful activity was misperceived as being illegitimate and whether the information was reported accurately. Despite these potentially limiting factors, when suspicious activity is reported, the agency has a public safety responsibility to determine whether there is evidence that a crime is being planned or has been committed. If so, the information should be retained and serve as the basis for a further criminal inquiry and operational planning to protect the public.

Because of this sensitivity, Global's Privacy Committee identified six critical factors, or points in the SAR process, wherein information management controls should be implemented to ensure security and privacy of PII while at the same time permitting the agency to further its inquiry into the behavior. These controls are based on the same principles of information management used to protect information in a criminal intelligence records system. With some modification from the Privacy Committee's report, the controls include the following:

**Receipt/Collection.** At the time of receipt or collection, suspicious activity information should be assessed and reviewed for sensitivity and confidentiality, using corroborative information if possible. Every effort should be made to validate or refute the information to resolve as quickly as possible whether there is a criminal nexus or whether the SAR is unfounded. Collection of information that is purely expressive activity protected by the First Amendment should be prohibited.

**Storage.** Storage of suspicious activity information with PII should be handled similarly to data that rises to the level of reasonable suspicion. Those requirements should include an audit and inspection process, supporting documentation and logical separation or labeling of the unconfirmed SAR from other information.

**Access.** Because of uncertainty about the information's credibility and/or accuracy, it is recommended that access to suspicious activity information be handled similarly to access to information that rises to the level of reasonable suspicion. Access should be allowed only where there is a right to know and need to know the information in the performance of a law enforcement, homeland security, or public safety activity.

**Dissemination.** Suspicious activity information, if systematically collected and stored for interagency distribution, should be disseminated primarily in response to an inquiry, and only for law enforcement, homeland security, and public safety purposes. Uncorroborated suspicious activity with personal identifying information should not be regularly disseminated in bulletins or other similar products. However, it may be included in secure information databases and disseminated to relevant law enforcement, homeland security, and public safety agencies that have the right to know and need to know the information for public safety purposes.

**Retention.** The retention period for suspicious activity information should be established by policy and be of sufficient time to determine the veracity of the information in light of the agency's expertise and resources. Suspicious activity records should have a disposition label—such as “undetermined/unresolved” or “cleared/unfounded”—to clearly notify the user of the information's status. Agencies

should also consider the need for maintaining some type of suspicious activity data for purposes of statistical reporting and performance measurement when setting retention and purge procedures.

**Security.** It is recommended that physical and electronic security measures be similar to those used for information rising to the level of reasonable suspicion.<sup>720</sup>

Permeating each factor in this process should be constant attention to privacy, accuracy, and corroborating the information in the SAR. As reinforced by a report to Congress by the PM-ISE:

Protecting the information privacy and legal rights of Americans is a top priority: At the local level, SARs will be incorporated into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public. Multiple levels of review and vetting will be established to ensure that information is legally gathered and managed, and reports containing personally identifiable information that are unfounded, or that cannot be reasonably associated with criminal activity, will not be shared beyond the originating entity.<sup>721</sup>

Complicating these processes is a common belief among many law enforcement officers that all information may be useful sometime in the unknown future. This belief produces a great reluctance to destroy any information or reports. However, it must be remembered that SARs include unsolicited tips and leads from sources that have a wide range of credibility. If the follow-up shows that the allegation in the SAR is unfounded, there is no reason to retain the information.

## POLICY RECOMMENDATIONS FOR DEVELOPING AND MANAGING A SUSPICIOUS ACTIVITY REPORTING SYSTEM

As has been evident in this discussion, law enforcement agencies are increasingly developing more comprehensive systems to stimulate the reporting of suspicious activity as well as to have a more structured process to manage SAR records. While national standards have been developed for SARs that report terrorism information,<sup>722</sup> there are no current national standards for policies related to criminal activity that is not terrorism related. As a result, the Major Cities Chiefs Association and Global approached this task with support from DOJ and DHS. A number of substantive recommendations were made from this project, as well as the identification of best practices. A summary of some of the project's findings and recommendations related to the management of suspicious activity reports includes the following:

- ◆ Agencies should educate and gain the support of policymakers about issues and processes related to suspicious activity reporting.
- ◆ All privacy and civil liberties policies and training should be reviewed to verify that they are consistent with current law and national standards.
- ◆ Information management of the SARs process should be integrated with existing processes and systems that manage criminal investigative information and criminal intelligence, thereby leveraging existing policies and protocols to protect privacy and civil rights.
- ◆ The SAR policy should be communicated to the public, since transparency is the key to acceptance.

---

720 These factors are based on the following document with some modification: Privacy Committee. (2007). *Tips and Leads Issues Paper*. Washington, DC: Global Intelligence Working Group, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, pp. 7–8. <https://www.brennancenter.org/sites/default/files/analysis/FN%20262%20%28Global%20Justice%20Information%20Sharing%20Initiative%2C%20Tips%20and%20Leads%20Issue%20Paper%29.pdf>

721 McNamara, T. (2008). *Annual Report to the Congress*, op cit., p. 29.

722 <https://www.dhs.gov/publications-library/collections/nationwide-sar-initiative>

- ◆ The gathering, processing, reporting, analyzing, and sharing of suspicious activity is critical to preventing crimes, including those associated with domestic and international terrorism. Hence, the SAR process should have an all-crimes orientation.
- ◆ The SARs process should use criminal information management processes, applying SARs to the appropriate criminal records management system or criminal intelligence records system.
- ◆ Suspicious activity submissions should not bypass the local law enforcement agency or agency of original jurisdiction and the standard 9-1-1 reporting systems.
- ◆ When an agency receives information that impacts another jurisdiction, it is the responsibility of the receiving agency to immediately notify the impacted agency and discuss coordination, deconfliction, investigation, and vetting procedures with the impacted agency. Once the information is vetted, further dissemination is the responsibility of the impacted agency.
- ◆ A process should be established to ensure that SARs are made available to fusion centers and local Joint Terrorism Task Forces (JTTFs) in a timely manner.
- ◆ An ongoing emphasis should be placed on defining and communicating trends in terrorism activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.
- ◆ There is a need for a common national methodology, including common data codes, for the sharing of suspicious activity data to discern patterns across the country.
- ◆ Training is a key component of the SAR process—all relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.
- ◆ Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.
- ◆ Develop a common national methodology to horizontally and vertically share SAR data in a timely manner that is consistent with privacy and civil liberty guarantees.
- ◆ Develop a standardized training program to provide consistent nationwide SAR training.<sup>723</sup>

The intent of these recommendations is to maximize the utility of non-terrorism suspicious activity information while protecting civil liberties. Although these recommendations are intended to bring about standardization of the SAR process, the report notes that every jurisdiction will have to develop policies and procedures that take into account the unique circumstances and relationships within that community.<sup>724</sup>

## INFORMATION SHARING ENVIRONMENT-SUSPICIOUS ACTIVITY REPORTING (ISE-SAR)

As noted previously, ISE initiatives formalized suspicious activity reporting to ensure comprehensive information sharing as specifically related to terrorism information as a mandate from the Intelligence Reform and Terrorism Prevention Act of 2004. While many detailed components of this process have been developed that are beyond the scope of the current discussion,<sup>725</sup> there is value for the reader to have some familiarity with the ISE-SAR initiatives. Remember, the ISE-SAR applies only to terrorism information.

<sup>723</sup> Suspicious Activity Report Support and Implementation Project. (2008). Op. cit., pp 2–5.

<sup>724</sup> Ibid., p. 6.

<sup>725</sup> A number of reports and documents on these issues have been posted online by DHS at <https://www.dhs.gov/publications-library/collections/nationwide-sar-initiative>.

The use of the ISE-SAR focuses on the following:

... the DOJ, DHS, DoD, and the FBI, working in partnership with state and local officials, will institute a standardized approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activities reports. Front line law enforcement personnel will be trained to recognize behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Once documented, SARs will be evaluated by trained personnel to determine if they have a terrorism nexus. If a terrorism nexus is established, the SAR will be made available to the local JTTF, regional and/or statewide fusion centers, and DHS.<sup>726</sup>

While this process has been implemented in a number of locales across the United States, it is an effort that should be undertaken nationwide.

To further this process, the ISE created the Common Terrorism Information Sharing Standards<sup>727</sup> (CTISS) program. The CTISS allows for business process-driven, performance-based common standards for preparing terrorism information for maximum distribution and access. Two categories of common standards are formally identified under CTISS:

1. **Functional Standards**—Set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.<sup>728</sup>
2. **Technical Standards**—Document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.<sup>729</sup>

The standards are designed to increase effective sharing of the ISE-SAR with the intent of enhancing the discovery and analysis of potential terrorism-related patterns or trends on a regional and national basis beyond what would be recognized within a single organization, jurisdiction, state, or territory. The ISE-SAR Functional Standard supports sharing information among federal, state, local, and tribal partners that relates to suspicious activity or incident information that has a potential terrorism nexus, in a manner that protects P/CRCL.

It should be noted that the SAR standards cannot be mandated to apply to all SLTLE agencies. However, in practice, adoption of these standards by state, local, and tribal law enforcement is a reasonable alternative, particularly in light of fusion centers serving as clearinghouses for two-way information sharing.

## SUMMARY

Suspicious activity reporting is being embraced as a key element in the contemporary intelligence process. With appropriate methods and systems in place, it serves as a valuable tool for gaining critical raw information. However, the reader is cautioned that SARs are sensitive from a civil rights perspective; hence they require careful development and controls.

## INTELLIGENCE REQUIREMENTS

With the growth of fusion centers and the development of an intelligence capacity in an increasing number of agencies, law enforcement is increasingly relying on the use of “intelligence requirements” as a method to define the types of raw information that is needed to develop a more robust analysis of threats. An intelligence gap is missing information that is needed for effective intelligence analysis. An intelligence requirement is the information needed to fill the gap. When managing information, both gaps and requirements should be identified and defined.

---

726 McNamara, T. E. (2008). *Annual Report to the Congress on the Information Sharing Environment*. Washington, DC: Program Manager-Information Sharing Environment (PM-ISE), p. 29.

727 <https://www.dni.gov/files/ISE/documents/DocumentLibrary/CTISSprogramManual20071031.pdf>

728 <https://www.dhs.gov/publication/ise-sar-functional-standard>

729 <https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise>

To illustrate requirements, a statement by former U.S. Secretary of Defense Donald Rumsfeld, which was panned by many pundits as being “nonsense,” demonstrates the concept when dissected. Secretary Rumsfeld stated:

There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don’t know. But there are also unknown unknowns. There are things we do not know we don’t know.<sup>730</sup>

Table 10-1 provides an illustration of Secretary Rumsfeld’s statement as applied to different intelligence challenges—international terrorism (according to al-Qaeda) and violent crime within a community—followed by a statement of the intelligence actions related to requirements that must be taken.

**TABLE 10-1: INTERPRETATION AND ILLUSTRATION OF THE RUMSFELD QUOTE**

	AL-QAEDA EXAMPLE	VIOLENT CRIME EXAMPLE	INTELLIGENCE ACTION
<b>THERE ARE KNOWN KNOWNS</b>	We know al-Qaeda’s intent is to commit more terrorist attacks against the U.S. and U.S. interests.	We know there is an increase in violent crime using firearms within a community.	The information we know must be consistently monitored and verified (i.e., standing requirements) to determine any changes in the status of the information we know.
<b>THERE ARE KNOWN UNKNOWNNS</b>	We know al-Qaeda has plans for future terrorist attacks, but the timing, methods, and locations are unknown.	We know there is an increase in black-market firearms, but it is unknown who the supplier is, where the guns come from, or how the transactions are made.	We know that we have intelligence gaps. Intelligence requirements, sources, and methods must be defined so that we may learn the currently unknown information.
<b>THERE ARE UNKNOWN UNKNOWNNS</b>	If al-Qaeda has developed new alliances or new methods to commit attacks, these are unknown to us.	There are factors driving the increase in violence beyond the availability of guns; however, these other factors are unknown to us at the time.	Information must be collected from all sources and analyzed in an attempt to identify new threat information.

The intelligence analyst must integrate currently held information to determine what we know about a threat—these are the “known knowns.” Because the threat environment is dynamic, these known factors must be constantly monitored to verify the threat and determine whether a change is occurring to the threat picture. In many instances, while we know a general threat exists, the specific character of the threat—the method of attack, the specific target of attack, and when the attack may be attempted—is unknown. These are “known unknowns.” Finally, there are threats that may be developing, either by a known suspect or a suspect completely unknown to us, which we are simply unaware of—these are the “unknown unknowns.” Hence the goal is to continually monitor suspicious activities and collect information from diverse sources that may give us an indicator of new threats. When these new indicators are learned, requirements are defined to better identify the threats and those who pose them.

One can understand how the layperson may interpret Secretary Rumsfeld’s statement as “nonsense”; however, he was essentially describing intelligence gaps and intelligence requirements.

730 Department of Defense News Briefing, February 12, 2002. See <http://www.slate.com/id/2081042/>.

Intelligence requirements is a concept that has not been widely used in law enforcement intelligence, although it has long been used in national security intelligence to specify information needs about threats. It is a holistic approach to collecting and analyzing information so that the most comprehensive picture of a threat emerges as well as alternatives on how to counter the threat. The use of requirements also increases the efficacy of the intelligence process by expressly focusing on information needs rather than using a broad “dragnet” approach to information collection or simply awaiting the serendipitous discovery of critical data.

For example, there is a wide array of threatening and criminal information posted on social media, imageboards, and darknet sites. Trying to scroll through this vast amount of information looking for incriminating posts—a dragnet—is labor-intensive with a low hit-to-search rate. However, knowing what type of information is needed—requirements—helps focus the search.

To use an analogy, the job of an intelligence analyst is akin to putting together a jigsaw puzzle without knowing what the final picture in the puzzle looks like. Each piece of information is like a puzzle piece—the analyst must see where it fits to create a discernable image. The missing pieces are information gaps—the intelligence requirements are to identify and collect the missing pieces, filling gaps, to make the picture more complete. As more pieces are identified, new requirements often emerge. Once sufficient information has been collected, the picture becomes clear—hence the threat is more clearly understood. Of course, in practice it is not that simple, hence the need to elaborate on the issues and processes related to requirements-driven intelligence.

## FILLING GAPS/FULFILLING REQUIREMENTS

The information collection process needs to be focused so that specific information needs are fulfilled. This increases efficiency of the process and ensures that the right information needs are being targeted. Historically, law enforcement used a tradition-driven approach that largely relied on intuition of what was suspicious. Often, it was mere suspicion based on statements or behaviors that seemed out of the norm, extreme, or unusual. This process was neither objective nor scientific and was often influenced by implicit bias<sup>731</sup> derived from a person’s attitudes, values, and beliefs. This process collected volumes of diverse raw information that was then forwarded to analysts and investigators who would examine the information in hopes that substantive threat information might emerge. As illustrated in Table 10-2, there are a number of differences between this tradition-driven approach and the requirements-driven approach to information collection. Basically, the requirements-driven approach is more scientific and hence, more objective, more focused, more efficacious, and less problematic on matters related to civil rights. On this last point, given that intelligence requirements are often the product of an ongoing criminal inquiry; the criminal predicate is more easily articulated.

Essentially, the tradition-driven approach is like throwing out a net, seeking to collect as much information as possible under the assumption that threat information and evidence of crime will emerge from the vast body of information. It is less efficient, less effective, and more likely to lead to civil rights liability. Requirements-driven intelligence is more laser-like. It focuses specifically on the types of information we need to give us an understanding about a narrowly defined area of threat.

---

731 <http://kirwaninstitute.osu.edu/research/understanding-implicit-bias/>

TABLE 10-2: TRADITIONAL COLLECTION VERSUS REQUIREMENTS-DRIVEN COLLECTION

TRADITION-DRIVEN	REQUIREMENTS-DRIVEN
◆ Data-driven	◆ Analysis-driven
◆ Exploratory	◆ Specifically focused
◆ Emphasizes amassing data	◆ Emphasizes a focused, selective approach to information collection and analysis
◆ Assumes collected information will identify criminals	◆ Analytic inference of criminal suspects from collected information
◆ An aggregate approach to information collection (dragnet); even mere suspicion	◆ Targeting/specificity on information regarding reasonable suspicion of crimes
◆ Explores all general inferences about potential criminality	◆ Selectively explores crime and threat leads based on priorities and evidence
◆ Explores collected information to see if there are questions to answer	◆ Answers questions by collecting and analyzing specifically collected information
◆ Develops intelligence records for contingency needs (i.e., just in case information is needed)	◆ Develops intelligence records in support of active threats and criminal enterprises

## APPLYING THE REQUIREMENTS TO STATE AND LOCAL LAW ENFORCEMENT

As part of the FBI’s Intelligence Branch re-engineering process, former Executive Assistant Director (EAD) Maureen Baginski employed “requirements-driven intelligence.” This concept is epitomized by the statement frequently attributed to Baginski, and previously referenced in discussions of the intelligence process, that the absence of evidence is not the absence of a threat.

This is an insightful observation to understand *why* requirements-driven intelligence is important. For example, let us say a law enforcement executive asks the Major Urban Area Fusion Center if there is a terrorism threat within the agency’s region. The response may be, “There is no evidence to suggest a terrorist threat exists within the region.” However, there may be an *unknown* threat in the community for which no evidence has been discovered (e.g., “unknown unknowns”). For example, one such unknown threat in the community was Timothy McVeigh, who placed the bomb at the Murrah Federal Building in Oklahoma City. Another unknown threat was Muhammad Atta, who had a base of operations within U.S. communities to aid in planning the attacks of September 11, 2001. Yet another threat that should have been known but was not recognized was Nikolas Cruz, who on February 14, 2018, opened fire with a semiautomatic rifle at the Marjory Stoneman Douglas High School in Parkland, Florida, killing 17 people and injuring 17 others. These were all clear threats to their communities; however, the evidence of these threats had not been discovered or exploited.

We must have a means to identify these unknown threats, assess the danger posed, and take appropriate action to prevent or mitigate the threat—this is a threat assessment (discussed in the next chapter). The process is not easy, especially for a SLTLE agency that may have limited information collection and analytic capabilities. Identifying evidence of such threats is both labor- and resource-intensive, requiring good information sharing; effective linkages with intelligence networks; constant monitoring and exchange of information; and ongoing information collection, assessment, and analysis within an agency’s jurisdiction. These needs reinforce the value of fusion centers—which have all of these characteristics—and the need for agencies to be fusion center partners. The fusion process is particularly structured to effectively use the intelligence requirements model.

Hence, while requirements-driven intelligence will work well for a law enforcement agency, it requires a commitment of time and resources to accomplish its goals. At the very least, a law enforcement agency needs a minimalist

intelligence capacity to contribute to the process at a state, regional, or major urban area level, particularly to be an effective intelligence fusion center partner.

## COMPARING INTELLIGENCE REQUIREMENTS AND CRIME ANALYSIS: AN ANALOGY

Intelligence requirements may be conceptualized as information that is needed to make decisions on how best to protect a community from threats posed by organized crime and terrorism. When requirements are filled and analyzed, the results are reported to give executives and managers sufficient reliable information to direct an operational response to a threat.

As an illustration, SLTLE agencies often make operational decisions related to incidents of predatory crime based on crime analysis requirements. Indeed, this is the fuel of the CompStat<sup>732</sup> process. Specifically, as a result of the timely analysis of reported crime, certain types of crime trends emerge. Relying on information derived from that analysis—such as type of crime, modus operandi, time and geographic factors, suspect descriptions, etc.—response strategies are developed to deal with the crimes that have occurred and the likely forecast of crime that will occur if the crime series is left unchecked. The agency may use saturation patrol, undercover officers, decoys, surveillance, or a combination of strategies to capture these repeat offenders. Without the information from the crime analysis output, the most effective operational decisions cannot be made.

Of course, crime analysis requirements are much easier to provide than intelligence requirements because of the inherent differences between criminal investigation and criminal intelligence. Essentially, investigations are crime-driven, while intelligence is threat-driven. Thus, investigations are *reactive*, responding to crimes that have occurred and a known quantifiable universe of data that have been identified through the investigation. Conversely, intelligence is *proactive* by intervening when a threat is identified. Essentially, intelligence is pre-crime and far more probabilistic—factors that pose both operational challenges and potential civil rights issues.

## REQUIREMENTS AND STRATEGIC PRIORITIES

Intelligence activities should be based on the mission of the unit or fusion center. For example, the mission of a High Intensity Drug Trafficking Area (HIDTA) intelligence center would be the production and distribution of illegal drugs. Similarly, intelligence activities of the Immigration and Customs Enforcement service are focused on the smuggling of humans and contraband across U.S. borders. However, most state, local, and tribal intelligence activities have adopted an all-crimes, all-threats, all-hazards approach. In reality, “all crimes” for intelligence purposes is somewhat of a misnomer. Because this encompasses a wide breadth of crime types, pragmatically, even an all-crimes intelligence operation must prioritize the types of crime that will be the focus of intelligence activities. As noted in the Chapter 6 discussion of strategic priorities, this priority will be based on geography, criminal history of the region, and special issues that help facilitate organized crime and terror threats, such as the presence of seaports, international airports, or unique commercial industries, for example, critical infrastructure sectors.

Intelligence requirements should also be mission-related. Known as *priority intelligence requirements*, their intent is to maintain focus on crime and threats that have been assessed as having the impact of greatest concern in the jurisdiction. We know, however, that crimes and threats change over time. For example, in the case of drugs, trends change in different geographic areas of the country quite frequently. In some geographic areas, methamphetamines are a major problem; in another region, the drug problem may be crack cocaine. As the opioid epidemic emerged, meth and crack decreased—for a while. In each case, the primary drug problem will evolve. As a result of these types of changes in crime problems, reprioritization of intelligence targets should be part of the reevaluation component of the intelligence process as well as strategic intelligence analysis.

---

<sup>732</sup> [https://www.policeforum.org/assets/docs/Free\\_Online\\_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf](https://www.policeforum.org/assets/docs/Free_Online_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf)

## TYPOLOGIES OF REQUIREMENTS

There are various ways to describe intelligence requirements, with no uniform standard for describing the different types of requirements used by law enforcement agencies. This discussion seeks to take the different models and terms currently used and not only explain them but also illustrate their relationships.

Requirements may be characterized in different ways based on their role. These different characterizations are *not* mutually exclusive. Indeed, as illustrated in the Venn diagram in Figure 10-4, there is a nexus among all the different types. The different characterizations fundamentally relate to their purpose.

*Functional* requirements are defined by the intelligence unit or fusion center for the purpose of learning about different dimensions of a threat. Information is collected through SARs and via the collection plan associated with ongoing inquiries to help analysts understand the functional evolution of threats. This is often a systemic process, wherein as more information is received and analyzed, a better understanding of the threat emerges. This, in turn, helps define additional requirements. This iterative process continues to refine the threat picture until the threat is compromised or until it dissipates.

There are four types of functional requirements:

1. **Analyst-defined**—During the course of the analysis, the intelligence analyst discovers a gap in the information that needs to be filled for a comprehensive and accurate analysis to be completed. An analyst has three SARs that suggest an interrelationship among the three as preparation to commit a crime. The intelligence requirements are information that is needed to confirm this linkage.
2. **Threat-defined**—Known threats within a jurisdiction are monitored on a consistent basis to continually assess the threat. For example, if a jurisdiction has a known white supremacist group that has made criminal threats, monitoring that group to understand changes in its structure, membership, and/or activities can help identify imminent threats.
3. **Target-defined**—Based on the nature of known threats, targets are monitored to assess vulnerability and risk. The Earth Liberation Front (ELF) threatens to burn down houses and destroy construction equipment in a new subdivision that ELF says is in an environmentally sensitive area. The requirements would be to collect information on the vulnerability of the targets for a threat assessment.
4. **Incident/event-defined**—If an event is planned or an incident occurs, requirements will be defined to determine potential threats associated with the event or future implications of the incident. For example, if a white nationalist wins a court case to give a speech at a local university, there is a high likelihood that protesters and Antifa733 will attend the event to demonstrate their disdain for the speaker and the extreme-right ideology. Some protesters will demonstrate lawfully while others are likely to commit property crimes and be disruptive of the event. The intelligence requirements are derived from the fact that the event was scheduled.

For each type of functional requirements, there are critical information needs to understand all dimensions of a threat. Threat requirements apply to both law enforcement and homeland security (all-threats and all-hazards) intelligence. As the name implies, these are information needs that help an analyst define a threat with as much precision as possible. Whether the threat is from criminal extremists or from a pandemic disease, the analyst needs a wide array of valid information from reliable sources that can provide as much insight as possible about the threat picture.

The method by which the information is solicited is referred to as the *methodological requirements*. Generally, there are two types:

---

733 <https://www.adl.org/resources/backgrounders/who-are-antifa>

1. **Standing requirements**—information that needs to be collected on an ongoing basis to monitor known and consistently present threats within a community.
2. **Case (or ad hoc) requirements**—information that is needed by analysts to determine the existence and character of a threat based on unsolicited tips, leads, suspicious activity reports, and/or other information developed through the intelligence process.

Another dimension of requirements is based on an analysis request by *intelligence consumers*. For example, a partner agency in a fusion center may request a certain type of analysis for its jurisdiction. Hence, this request will drive the requirements process. These types of requirements are:

1. **Tactical**—What information is needed to prevent or mitigate an imminent or short-term threat?
2. **Operational**—What information is needed to prevent or mitigate a developing or long-term threat?
3. **Strategic**—What changes in the threat picture exist in the coming months or years that can have an impact on operational planning and resource allocation?

Overlapping all of these is a type of requirement that is unique to law enforcement: *legal requirements*. Recall that the sole authority for law enforcement agencies to have an intelligence function is their statutory authority to enforce the criminal law. As a result, conceptually, all information collected must be viewed as if it may eventually result in a criminal prosecution. Consequently, information is needed, at the least, to aid in establishing the criminal predicate and eventually sufficient evidence to establish the burden of proof in a trial. Hence, requirements will need to be defined that help establish the *corpus delicti*—or the elements of a specific crime as it relates to the intelligence targets.

FIGURE 10-4: CHARACTERIZATIONS OF LAW ENFORCEMENT INTELLIGENCE REQUIREMENTS



## REQUIREMENTS AND CRIMINAL EVIDENCE

This issue warrants special attention because it is unique to law enforcement intelligence. In the national security intelligence community, requirements serve as information to help make decisions about threat prevention, policy development, and strategic responses. However, in law enforcement intelligence, while many of these same needs are fulfilled, there is the added dimension that information collected from requirements may also be used as criminal evidence. Given the civil rights responsibilities that law enforcement officers must uphold, intelligence requirements for a law enforcement agency must also ensure that information collected during the requirements process follows the law of criminal procedure.

This can be challenging for law enforcement because there is a constant balancing process. In some cases, information collected about an individual must be balanced and documented with the threat to public safety. In other cases, the officers may be following up on a SAR to determine the veracity of the lead and establish both a criminal predicate and determination of a threat. There are many scenarios in which decisions are made about information collection and retention that are in the arena of uncertainty. Relying on a cautious perspective, there are some fundamental guidelines that should help guide the information collection process for legal requirements:

- ◆ Follow the law of criminal evidence and procedure.
- ◆ Always act in good faith with documented evidence and rationale that are the basis for information collection and retention.
- ◆ If there is a threat to community safety, document the evidence and rationale associated with that threat and corroborate it to the extent possible.

## SUMMARY

Information is needed to make decisions—the higher the quality and the more comprehensive the information, the more sound the decision. Similarly, information that answers a specific question is more useful than information that is general. If an executive is going to make a decision about implementing a new program, he or she needs information on the specific costs, benefits, and risks of the program as well as the more difficult dimension of what benefits will be lost if the program is not implemented. Typically, the information sought is not conclusive but based on probability, the experience of others, experimentation, logic, or, sometimes, an educated guess. Not having sufficient reliable information makes the decision process more difficult (and risky).

The same process applies to the operational environment of criminal intelligence. To adequately assess the threats from a terrorist group or a criminal enterprise, information is needed for a comprehensive analysis. Often, during the analytic process, critical information is missing that prevents a complete and accurate assessment of the issue. The collection process focuses on collecting the specific information identified in the requirement to answer questions related to criminal or terrorist threats.<sup>734</sup> The fulfillment of the intelligence requirement provides critical information with respect to making strategic or operational decisions on how to respond to the threat.

The intent of this discussion was to provide some perspective of intelligence requirements as specifically related to law enforcement intelligence. Once those information needs are identified, the next step is to collect the information.

## COLLECTION

Collection of information has been previously discussed in the context of the intelligence process (Chapter 3) and information needs for ILP (Chapters 5 and 6). The current discussion builds on the previous by looking at information from a broader perspective. Collection refers to information that is brought into the intelligence process for

<sup>734</sup> FBI Office of Intelligence. *The FBI Intelligence Cycle: Answering the Questions*. A desk reference guide for law enforcement. (Pamphlet form). (July 2004).

analysis—it is the generation of raw data and, as will be seen, it is not always an overt action by the law enforcement agency to reach out and gather information.

Essentially, information enters the intelligence process in one of three ways:

1. It is deliberately sought out and collected—tasked collection.
2. It is collected as a result of another law enforcement activity—routine collection.
3. It is given to law enforcement—volunteered information.

**Tasked collection** is in response to intelligence requirements and is typically gathered as a result of a collection plan. It may be defined as a plan for gathering information from all available sources to meet an intelligence requirement. Specifically, it is a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit.

The collection plan is typically determined by an analyst, sometimes with input from a supervisor, to determine *what* types of information are needed, *where* (i.e., sources) the information may be obtained, and *how* (i.e., methods) the information will be gathered. The analyst will have an array of options to choose from, ranging from open sources to restricted databases to interviewing people and more. The key lies in the question, “Where might I find this information and how will I get it?” The collection plan is the road map to answering this question.

In some cases, assistance of operational units will be needed. In these circumstances, intelligence personnel should coordinate with operational managers or supervisors to explain what information is needed, why it is needed, and the role of the operational units in collecting the information. Even in cases where the “why” must remain confidential, a general description will help in gaining cooperation. This is particularly true when information is sought from officers’ confidential informants<sup>735</sup> (CI).

When operational units assist in collection, explicit descriptions of the types of information needed should be provided. Similarly, time constraints for when the information is needed should be established. Operational units should also be provided with precautions, if any, during the collection process. In some cases, precautions may be related to officer safety. In other cases, the precaution may be to collect the information in a subtle manner so as not to tip off an inquiry. The key, of course, is effective communication between intelligence personnel and operational personnel.

The second method, *routine collection*, refers to the collection of information as part of routine operational and law enforcement activity. It focuses on the standing intelligence requirements or other issues of intelligence significance that are known and require a constant input of raw information. Information collected in this way is usually submitted as an information/intelligence report, but it may also be recorded elsewhere such as information within or from:

- ◆ Crime reporting.
- ◆ Criminal investigations, including stand-alone proactive or reactive operational databases/case management systems.
- ◆ Firearms licensing to monitor trends and flag names of known offenders.
- ◆ Use of crime gun intelligence.
- ◆ Trends emerging from crime analysis.
- ◆ Community and partnership activities and meetings.
- ◆ Jail and corrections records including incarcerations, releases, probation, and parole.

---

<sup>735</sup> For reference, see DOJ *Confidential Informants Guidelines*. <https://www.justice.gov/archives/ag/attorney-general-renos-confidential-informant-guidelines-january-8-2001>

Routine collection can take many forms and can include open sources. For example, analysts may set Google Alerts<sup>736</sup> for key words and phrases to be automatically notified when they appear on social media or news broadcasts. In many cases, the information has limited or no value from a criminal intelligence perspective. However, in those cases where there is value, the information may have been missed without routine collection.

**Volunteered information** is offered to law enforcement by members of the public, community contacts, and private partners. Its collection is focused (but not exclusively based) on the intelligence requirement. Information obtained is usually recorded and submitted on a suspicious activity report or some form of information report depending on the nature of the information.

Different aspects of collection have been discussed to maximize the effectiveness of the intelligence process. One caveat is in order, however. As one experienced intelligence leader observed, “Collection without dissemination is the quickest way to kill the process.” If collectors perceive that they are just “collecting to be collecting” or to feed the “information black hole,” where they receive no feedback in return, the quantity and quality of data will suffer.

## COLLECTING INFORMATION FROM CORRECTIONS AGENCIES

A source of information often overlooked in the collection process is correctional agencies. Increasingly, corrections departments are creating a security intelligence threat group designed to use an intelligence-based approach to information collection and analysis to determine threats residing in prison facilities.

Despite common misperceptions, many inmates retain strong connections with criminal groups on the outside during their periods of incarceration. There is ample evidence that gangs and drug traffickers, as well as radical ideological groups (such as the Aryan Brotherhood or Islamic extremists), have outside connections and tend to know—and sometimes have influence on—the criminal organization’s activities. Corrections agencies have greater breadth for information collection and can be an important information source for the intelligence process.

Significant elements of nontraditional information and intelligence reside within corrections IT systems. In fact, corrections agencies are uniquely positioned to gather information that other law enforcement entities are not able to gather. Information such as inmate visitor data, criminal associate data, and telephone record data are but a few of the information sources that have the potential to provide valuable insight to law enforcement and homeland security investigators seeking to develop a framework for social networking to better determine the synergistic among between the criminal enterprises, gangs, and the terrorist networks that threaten the country.

The types of information that correctional agencies are able to collect and retain are invaluable. While this information has often been successfully exploited for gangs, such initiatives need to be broadened. Working with corrections agencies within a law enforcement agency’s region can provide valuable information about gangs, extremism, drug trafficking, and other crime.<sup>737</sup>

It should be noted that the law enforcement community has recognized the value of correctional intelligence and has begun to develop specific training and groups that allow individuals to share their expertise. For example, in 2018, the Association of Law Enforcement Intelligence Units (LEIU) created a working group within the association that focuses on correctional/custodial intelligence needs. In 2019, LEIU created an executive board position for the correctional/custodial liaison.

---

736 <https://www.google.com/alerts>

737 <https://it.ojp.gov/documents/d/ASCA%20Global%20short%20Presentation.pdf>

## SUMMARY

Regardless of the method used to collect information, law enforcement intelligence personnel must remember that there is a different standard for information collected for use in a criminal intelligence records system. There is (1) information that identifies individuals and groups and (2) information that contains no identifying information.

## ANALYSIS

Without analysis, there is no intelligence. There is no single methodology used for intelligence analysis; rather, various approaches and analytic tools are used depending on the type of data/information available and the type of analysis (i.e., tactical or strategic) being performed.

*The intent of this discussion is not to teach analytic methods, but to provide the consumer of analysis with insights into the process.* Such insights should make the end user a more enlightened consumer. Moreover, with a better understanding of analysis, law enforcement officers will have better insights when responding to intelligence requirements.

Intelligence analysis is often referred to as a unidimensional activity that is the central step in the intelligence process. However, a closer examination of the analysis function reveals that it is a process requiring three broad skill sets. As such, the development of knowledge, skills, and abilities (KSAs) must correlate with these skill sets.

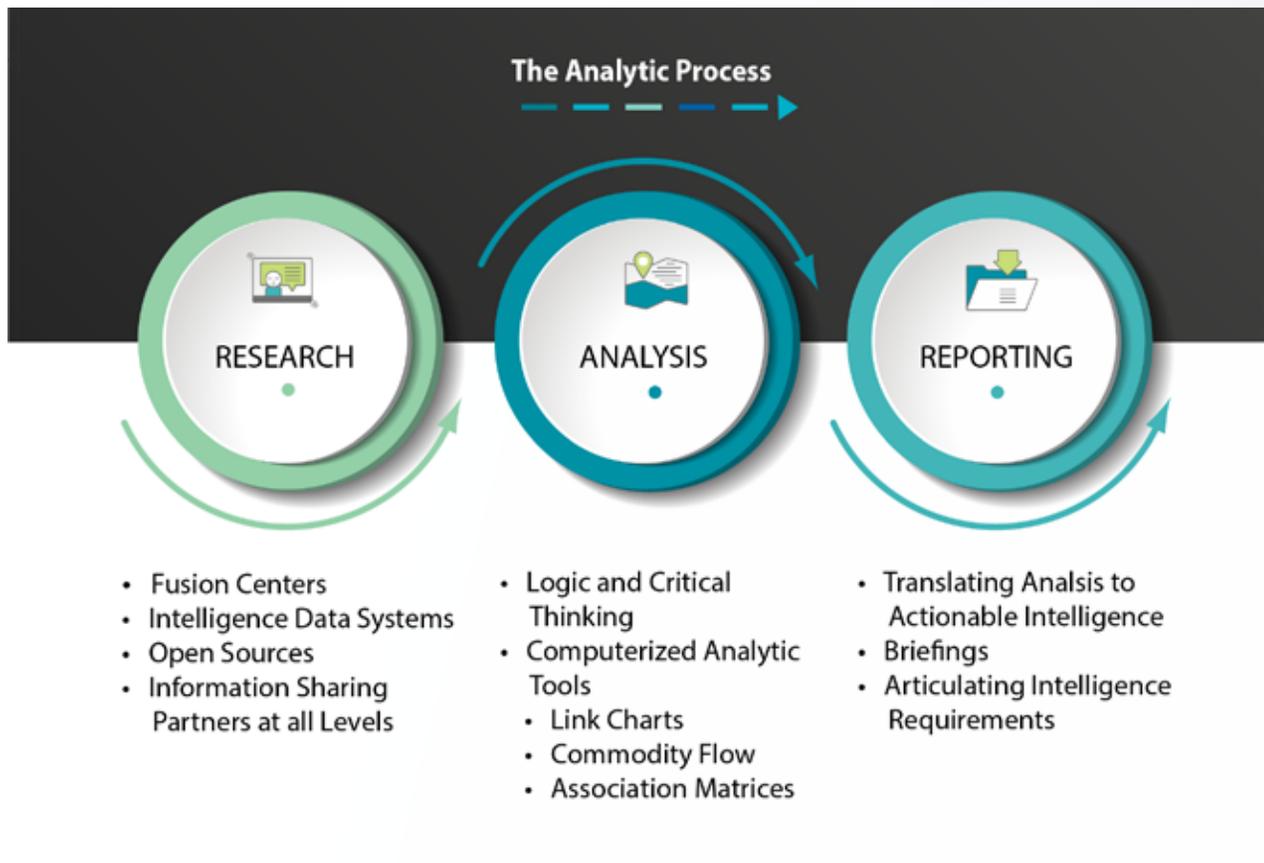
The first skill is *research*. Research involves the collection of diverse pieces of information and assessing its value (i.e., validity and reliability), as well as its relevancy and materiality to the assessment. It is somewhat different from collection. Research involves gaining information which clarifies issues and provides perspectives on an issue of interest. Examples include searching Web blogs of white nationalists to learn more about their beliefs and trains of thought; reviewing research on the characteristics and common processes of human smuggling; reviewing reports and articles on a specific issue, such as the behavioral characteristics of a person planning a suicide attack; or performing any other type of data collection that provides insight—as opposed to evidence—about a targeted issue. Certainly, there could be an overlap between research and collection; however, the roles are more complementary than duplicative. Analysts' KSAs must include both research and assessment methodologies. The analyst must be aware of the diverse sources of information—both open source information and law enforcement proprietary information—and know how to gain access to that information. While collection of information will occur from a wide array of sources beyond the analyst, the need for research skills is to be able to drill down into the information to learn what is essential to understand criminal enterprises.

Another element of research is proactive collection. The intelligence analyst must be more than a recipient of information. The analyst must be proactive in two methods. The first is to define and disseminate intelligence requirements to fill gaps in the information to have a more comprehensive and robust analysis of a threat, individual or target. The second method of proactivity is to elicit information from diverse sources. Whether the source is a database, a fusion center, a private partner, or an investigator, the analyst must proactively seek the information. Information sharing systems and practices have increased dramatically as a result of post-9/11 intelligence reengineering. Nonetheless, no system or process can ensure that all the needed information will reach the analyst's desk. Hence, proactive efforts by the analyst will add redundancy to the collection process to ensure that it is as comprehensive as possible. This is reinforced by the Law Enforcement Analytic Standard #11—*Collection Follow-up Standard*:

In the course of collection by investigators and others, analysts shall evaluate the progress of the collection to determine if the collection plan/requirements are being met and shall identify additional

sources of information, as well as identify information that may be useful to other cases or activities. Where possible, analysts shall relay that information to an appropriate body for follow-up.<sup>738</sup>

FIGURE 10-5: THE ANALYTIC PROCESS



An important part of this process means that policies and procedures must give analysts the authority to seek needed information as well as some type of accountability mechanism to ensure that the information is being provided. An unfortunate reality in many law enforcement organizations is that an intelligence analyst is often viewed as having a lower professional status than that of a sworn officer. As a result, it is sometimes difficult for analysts to give direction to investigators. While this artifact of organizational culture is slowly changing as analysts are increasingly viewed as practicing professionals, remnants of this perspective remain. Consequently, it is important for the intelligence process to ensure that analysts have the organizational authority to gain the information they need.

The second skill set, *analysis*, is essentially the scientific approach to problem solving. It relies on inductive and deductive reasoning; a balanced assessment of raw data; objectivity in the interpretation of facts; hypothesis testing; critical thinking; and decision making based on evidence. The late Carl Sagan, a world-renowned astronomer, explained the scientific process in this way:

Science is a way of thinking much more than it is a body of knowledge. Its goal is to find out how the world works, to seek what regularities there may be, to penetrate to the connection of things—from subnuclear particles, . . . to living organisms, the human social community, and thence to the cosmos as a whole. Our intuition is by no means an infallible guide. Our perceptions may be distorted by training and prejudice or merely because of the limitations of our sense organs, . . . Science is based on experiment, on a willingness to challenge old dogma, on an openness to see the universe as it really is. Accordingly, science requires courage—at the very least the courage to question the conventional

<sup>738</sup> *Law Enforcement Analytic Standards*. 2nd ed. (2012). Washington, DC: Global Justice Information Sharing Initiative and the International Association of Law Enforcement Intelligence Analysts. [https://it.ojp.gov/documents/d/Law%20Enforcement%20Analytic%20Standards%2004202\\_combined\\_compliant.pdf](https://it.ojp.gov/documents/d/Law%20Enforcement%20Analytic%20Standards%2004202_combined_compliant.pdf)

## SUGGESTED SOFTWARE NEEDED FOR EFFECTIVE ANALYSIS

- ◆ Word processing program
- ◆ Spreadsheet program
- ◆ Relational database
- ◆ Presentation software
- ◆ Flowcharting software
- ◆ Link analysis software
- ◆ Database reporting/ visualization software
- ◆ Mapping software
- ◆ Photo enhancement software
- ◆ Telephone analysis software
- ◆ Portable document format (PDF) creation software
- ◆ Security software (virus, adware, spyware software; firewall and virtual private network [VPN] security)
- ◆ Publication software
- ◆ Statistical analysis software
- ◆ Text mining software

Resource: *The Analyst Toolbox*, Global Intelligence Working Group, [http://it.ojp.gov/documents/analyst\\_toolbox.pdf](http://it.ojp.gov/documents/analyst_toolbox.pdf)

wisdom . . . [T]he scientific cast of mind examines the world critically as if many alternative worlds might exist . . . If you spend any time spinning hypotheses, checking to see whether they make sense, whether they conform to what else we know, thinking of tests you can pose to substantiate or deflate your hypotheses, you will find yourself doing science.<sup>739</sup>

This process described by Sagan is essentially what intelligence analysts do when attempting to derive meaning from a diverse array of facts. Sagan noted that science seeks to determine “. . . what regularities there may be . . .” In law enforcement, we seek to identify criminals’ modus operandi because these regularities in criminal processes are important for forecasting crime and determining prevention strategies. Similarly, Sagan observed that science seeks “. . . to penetrate to the connection of things.” Law enforcement intelligence analysts seek to find the connection between criminal conspirators (e.g., via link analysis), between different types of evidence (e.g., via association matrices), and between criminal transactions (e.g., via commodity flow diagrams).

Intelligence analysis is an intellectual exercise that has pragmatic applications. For most people, it does not come easily. It requires *structure, critical thinking, self-discipline, and strong substantive knowledge of the target*. “Structure” refers to the ability to be organized and follow accepted analytical methods without taking shortcuts and ensuring that all information and evidence is included in the analysis. “Critical thinking” means that the analyst will follow the rules of logical reasoning, not intuition. It also means that the analyst will draw conclusions based on the *known* evidence, not assumed evidence. “Self-discipline” is essential for the analyst to remain objective and not be influenced by emotion or external pressures. This objectivity also means that the evidence is considered with respect to its weight (i.e., reliability, validity, and corroboration). Beyond having the analytic KSAs, the analyst needs to have substantive knowledge of the targeted crime(s). Whether the target is an ideological criminal extremist, drug trafficking organizations (DTOs), or a money laundering network, the analyst needs to understand the terminology, beliefs, and mechanics associated with the criminal enterprise.

Training programs, continuing education, and self-directed education are valuable for developing the substantive knowledge needed for effective analysis. However, the thinking skills—which must be integrated with the substantive knowledge—are more challenging. A person can be taught the processes and tools of analysis, but critical thinking is most effectively produced through “mental calisthenics” and experience. Mental calisthenics refers to a series of written exercises or problems that challenge a person to find a solution. There may be multiple solutions, of which the next challenge is to find the best or most probable solution. This process is frequently used in problem-based learning (PBL), a strategy that builds a curriculum around a central question. The question may force the student to either solve a problem or make a decision.<sup>740</sup> The analytic skill set is the most difficult to effectively develop in an analyst—it is also the most critical.

739 Sagan, C. (1979). *Broca’s Brain: Reflections on the Romance of Science*.

740 Friedman, R. S., & Peek, F. (2002). “Problem-Based Learning and Problem-Solving Tools: Synthesis and Direction for Distributed Education Environments.” *Journal of Interactive Learning Research*. Vol. 13, No. 3, pp. 239–257.

The third skill set is *reporting*. Throughout the analytic process, there are stages in which the findings must be reported to decision makers and investigators. Reporting is translating the analytic output into descriptive status reports or actionable intelligence. A descriptive status report essentially describes the character and process of an intelligence target, probable effects, and probable future activities. The report may also include evidence currently possessed, intelligence requirements, and unexplained crime-related phenomena that need closer assessment. Typically, these reports are designed to assist in planning and direction of an inquiry, resource allocation, assessing risk to potential victims, to gain insights about threat timetables, and to plan for intervention and mitigation strategies. In contemporary intelligence, the reporting process happens when the analyst develops the intelligence products (discussed in the next chapter).

With actionable intelligence, a law enforcement agency has sufficient information to develop an operational response to threats. Within this framework, three factors contribute to effective analysis:

1. The overall quality of the information used to make a decision. Accuracy of information is essential. When information is analyzed, conclusions are drawn based on the facts that the analyst has. If the information is wrong or biased, this will inherently affect the quality of the analysis.
2. An increased body of information to make the information more comprehensive, thus corroborating other facts. As the volume of high-quality information increases, the analysis becomes more accurate. Raw information is clarified, and the quality of analysis will increase as volume increases. The key is to ensure that the quantity of information is accurate and relevant—a factor that is at the heart of the fusion process.
3. Increased specificity of the information. The more detailed the raw information, the greater the likelihood of identifying subtle factors about a threat.

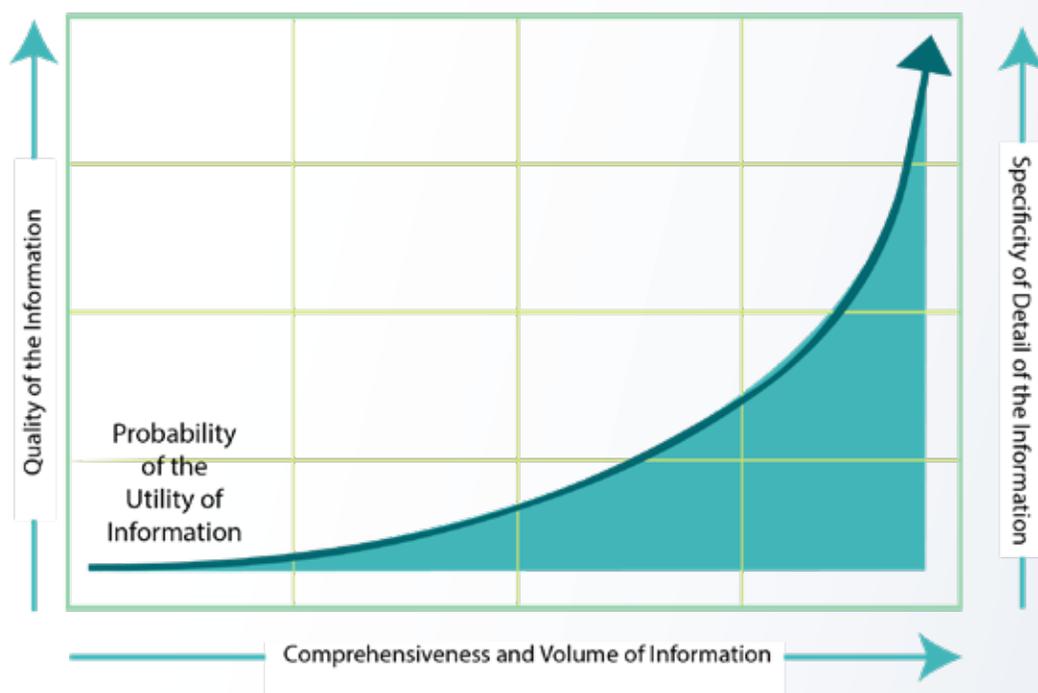


FIGURE 10-6: CRITICAL CHARACTERISTICS OF INFORMATION QUALITY

As illustrated in Figure 10-6, as each of these factors increases, the value of the analysis increases. Regardless of the skill of the analyst and the analytic tools available, the character of the raw information is fundamental to actionable analysis.

## ANALYTIC TOOLS

A number of analytic tools are available to the intelligence analyst. The word “tools” essentially refers to methodological techniques that help *organize, integrate, compare, correlate, and illustrate* a body of raw information. No analyst tool alone will produce actionable intelligence. Each tool adds a component of new knowledge—or at least new insight—about the data which, collectively, contributes to the analysis and/or leads to the definition of new intelligence requirements.

The analysis relies on the critical thinking skills of the analyst, along with his or her ability to integrate the output of these diverse methodologies into a cohesive, actionable intelligence product. These products may include portions of the analytic tools’ output to illustrate complex relationships, such as an illicit commodity flowchart or a link analysis chart showing the relationships and hierarchy of people involved in a criminal enterprise.

While the intelligence consumer does not need to know *how* to perform these various types of analysis, there is value in understanding the different analytic tools available and the types of information they provide. Although the following is not an exhaustive list, it contains the more common tools<sup>741</sup> an intelligence consumer may encounter:

- ◆ **Activity flow**—Similar to a modus operandi—or method of operation—the activity flow shows the steps a criminal enterprise uses indicating exact incidents, dates, and a description of activity that occurred. All incidents are linked together in a flowchart to understand the progression of the enterprise. The activity flow puts all the pieces together in a complex criminal organization that may be used for intervention in the enterprise as well as to determine where gaps exist. If gaps are identified, intelligence requirements will be used to fill them so that the activity of the enterprise can be fully mapped to aid in prevention and prosecution.
- ◆ **Association matrix**—This matrix seeks to correlate two or more factors in a criminal enterprise, documenting frequencies when two or more factors occur at the same time to isolate the correlating factors that are instrumental in the criminal enterprise operations and eliminate those factors that have no correlation. The factors may be alike—such as a series of telephone numbers. The factors may be inherently independent but may provide insight when they are correlated, such as the travel patterns of two intelligence targets when a telephone call or bank transaction precedes the travel.
- ◆ **Commodity flow/visual investigative analysis**—This diagram illustrates how an unlawful commodity is moved through a criminal enterprise and the transactions that are made in the commodity movement. For example, the commodity flow of Afghan heroin would show each transaction and method of smuggling that was used, along with the transaction costs, from Afghanistan to a city in Middle America.
- ◆ **Communications traffic analysis**—Important information can be gained from a traffic analysis of telephones, text messaging and email. Identifying with whom intelligence targets are communicating, as well as the frequency of communications, origins and destinations of communications, length of communications, and whether there were attachments to emails, can provide significant corroboration and evidence of criminality. While the content of communications will obviously provide important information, an analysis of communications traffic can also be valuable.
- ◆ **Crime pattern analysis**—This is a generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis, and general profile analysis; it can include mapping.
- ◆ **Criminal business profiles**—These contain detailed analysis of how criminal operations or techniques work, in the same way that a legitimate business might be explained.

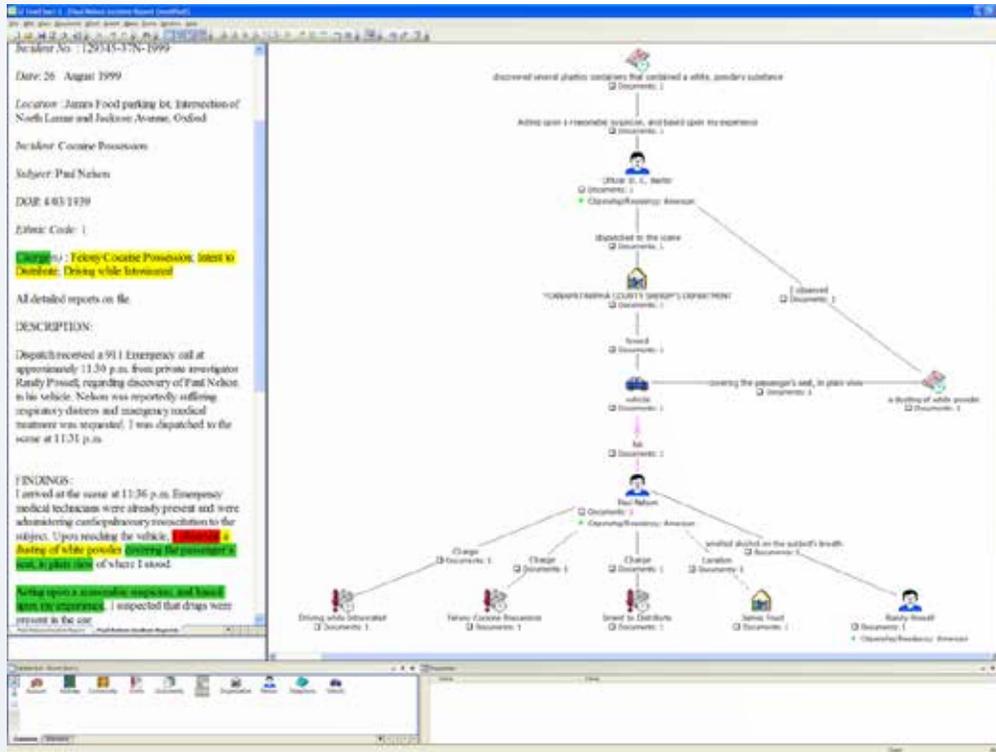
---

741 Many of these analytic tools are illustrated in: Peterson, M., et al. (1996). *Successful Law Enforcement Using Analytic Methods*. Richmond, VA: International Association of Law Enforcement Intelligence Analysts.

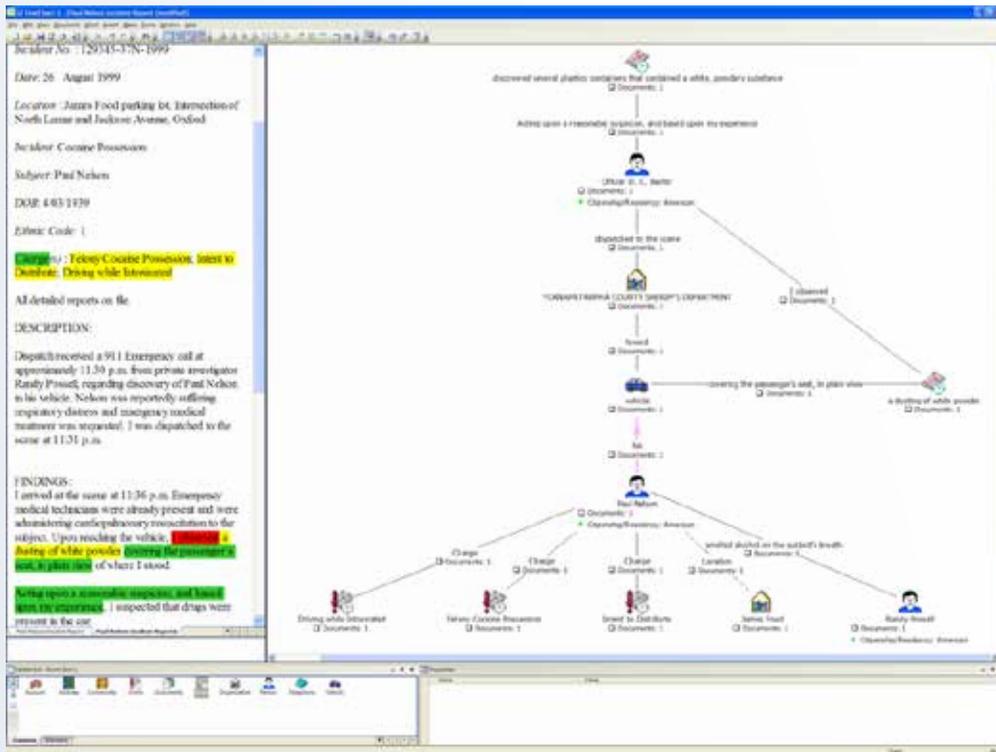
- ◆ **Demographic/social trends analysis**—An analytic method that is centered on demographic changes and their impact on criminality. It also analyzes social factors such as unemployment and homelessness and considers the significance of population shifts, attitudes, and activities as they may affect crime.
- ◆ **Event flow analysis**—These are charts providing a visual depiction of a series of important occurrences and the sequential relationship of these occurrences, such as travel of a criminal participant, monetary transactions, or other events that are critical in facilitating the crime.
- ◆ **Financial analysis**—There are a variety of financial analysis techniques that collectively seek to correlate diverse financial transactions to include the nature of the transactions; parties involved; origins, intermediaries, and destinations of transactions; and comparative analysis of income and expenditures. The intent is to document transaction trends of intelligence targets (both individuals and organizations) and to identify discrepancies or suspicious financial activities. Given that virtually all crimes have some form of financial element, financial analysis can be an important tool.
- ◆ **Hypothesis testing**—The analyst makes a hypothesis about the linkages of people and organizations in the criminal enterprise, transactions necessary for the enterprise to operate, and critical commodities or resources necessary for the enterprise to be successful. Unlike the previous items in this list, which are visual depictions of various elements of the enterprise, hypothesis testing uses these depictions to determine whether the elements in the enterprise have been identified that can be used to prevent the enterprise from continuing and, ideally, determining the criminal liability of participants.
- ◆ **Link analysis**—This chart identifies all confirmed and suspected persons and organizations in the criminal enterprise to illustrate their relationships to each other.
- ◆ **Market profiles**—These are continually reviewed and updated assessments that survey the criminal market around a particular commodity, such as drugs or stolen vehicles, or of a service, such as prostitution, in an area.
- ◆ **Network analysis**—This analysis not only describes the links between people who form criminal networks, but also the significance of these links, the roles played by individuals and the strengths and weaknesses of a criminal organization.
- ◆ **Operational intelligence assessment**—This assessment involves evaluating incoming intelligence to maintain the focus of an operation on previously agreed objectives, particularly in the case of a sizeable intelligence collection plan or other large-scale operation.
- ◆ **Results analysis**—This analysis evaluates the effectiveness of law enforcement activities, for example, the effectiveness of patrol strategies, crime reduction initiatives, or a particular method of investigation.
- ◆ **Risk analysis**—This analysis assesses the scale of risks posed by individual offenders or organizations to individual potential victims, members of the public, and law enforcement agencies.
- ◆ **Target profile analysis**—This analysis embraces a range of analytical techniques to describe criminals, their criminal activity, lifestyles, associations, the risks they pose, and their strengths and weaknesses to give focus to the investigation targeting them. Profiles also may focus on victims and vulnerable persons.

Each of these techniques is used to better understand the raw information and its relationships as well as to illustrate a criminal phenomenon. Applying contemporary technologies to these analytic methods can make the analysis even more robust. For example, artificial intelligence (AI) can organize unstructured data, including text, images, audio, and video, into structured forms, providing more insights such as with a link analysis or commodity flow. Regardless of the sophistication of the analysis, it remains a human responsibility—that of the analyst—to interpret the analytic output and give meaning to the findings—that is when we have intelligence.

FIGURE 10-7: ILLUSTRATIONS OF ANALYTICAL CHARTING<sup>742</sup>



LINK ANALYSIS CHART



TEXT ANALYSIS CHART

742 These charting illustrations are from i2's Analyst Notebook software. Images courtesy of i2.

## PREDICTIVE ANALYSIS

As a caveat to begin this discussion, predictive analysis is a methodology and a body of knowledge that pre-dates law enforcement applications. Technologies have been developed (largely by the private sector) specifically to apply predictive analytics to policing, known as predictive policing.<sup>743</sup> As a result, there are two issues to address. First, “predictive” is a misnomer for this type of analysis—to predict is to state that something will occur. Actually, this type of analysis is a forecast—which means that, given the analysis of historical data, there is a probability that something will occur.

In the private sector, these differences in terminology made little difference because there was a conceptual understanding that predictive analysis was inherently probabilistic. In law enforcement, however, many civil rights activists took the label to mean literally that law enforcement was predicting who would commit crimes as well as when and where the crimes would occur. Law enforcement would then take steps to intervene. They believed not only that there were constitutional due process issues with this type of analysis but also that there was implicit bias in the analytic algorithms that erroneously target people of color. While there is scientific research demonstrating that predictive policing does not produce biased results,<sup>744</sup> it has become an emotional issue for many critics. While predictive analysis has proven quite valuable to law enforcement, the reader should be aware of these caveats.

Predictive analysis<sup>745</sup> is a concept that has become increasingly valuable as a tool for intelligence analysis and crime analysis. As such, a brief description of the concept can be of value to the intelligence consumer. The methodology is largely borrowed from the private sector, where econometric models are used to forecast market changes. For example, based on an analysis of economic factors in a current market, buoyed by analysis of known trend data—such as changes in a sector’s economics during different times of the year—a manufacturing firm may alter its production, workforce size, and supply chain to continue profitable operations while meeting supply demands throughout varying conditions. Hence, the analysis provides strategic direction for both management and operations to make decisions about alternate futures to avoid unnecessary profit losses while fully serving customer needs.

Can such a quantitative-based approach work in the largely qualitative world of law enforcement intelligence analysis? While predictive analysis has important applications to intelligence analysis, it will not provide an analysis as robust as in more quantitative fields that have more predictable change cycles, such as those in business. Nonetheless, predictive analysis has important applications to intelligence but will require a diverse research effort, a multifaceted analytic methodology, and a broadened method of reporting that offers differential outcomes based on the evolution of social and political trends. Over time, these trends can be monitored by intelligence analysts to refine the status and threat implications of the trends being observed. While this sounds complex and labor-intensive, with the use of artificial intelligence and machine learning in commercial applications, the analysis can be done quickly and updated easily and quickly when new data are entered for analysis.

Predictive analysis is a critical thinking methodology that integrates known quantitative and qualitative variables—including incidents, events, and political and social dynamics—into a logical forecast of threat parameters. As noted previously, the label “predictive” is misleading because it is virtually impossible to truly predict events that are based on human behavior and the infinite number of variables that can influence that behavior. The process is a probabilistic analytic exercise that gathers diverse data, constantly monitors changes in the data, and refines the forecast based on the new inputs. Just like the intelligence process itself, predictive analysis is reiterative, constantly seeking new inputs of information to refine the forecast.

743 <https://nij.ojp.gov/topics/articles/overview-predictive-policing>

744 Brantingham, P. J., et al. (2018). “Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Control Trial.” *Journal of Statistics and Public Policy*. Volume 5, Issue 1, pp. 1–6. DOI: 10.1080/2330443X.2018.1438940.

745 For a comprehensive review of predictive analysis as applied to the intelligence process and beyond, see *Predictive Analytics Handbook for National Defense*. (2020). McClean, VA: Booz Allen Hamilton. <https://www.boozallen.com/d/insight/thought-leadership/predictive-analytics-handbook-for-national-defense.html>

The reiterative nature of predictive analysis complements requirements-driven intelligence. This process continuously seeks to identify information to fill intelligence gaps, or voids in our knowledge base about threats, and then identify, collect, and analyze information to fill those gaps. Hence, intelligence requirements—that information that is required to fill a gap—provide constant input into the intelligence cycle to help ensure that the base of knowledge is as comprehensive as possible.

Predictive analysis in law enforcement can have the greatest impact on strategic intelligence, although it can also have an application to aid in defining standing intelligence requirements. This analytic technique will not forecast threats, per se, but it can forecast changes in the environment that may alter conditions that contributes to threats.

Intelligence requirements and analysis are inherently related to threat assessments. The interrelationship is systemic in that a change in one of the components will affect the others. Intelligence analysis is a complex task involving the examination and assessment of information to draw conclusions about a particular topic. It is not an academic exercise because it does not involve philosophical theories. Instead, intelligence analysis is a function heavily dependent on realism and requires an objective approach to thinking. It is predominantly process-driven, and it requires continuous exhaustive research using information from a variety of sources. Analysis also involves the collation of information to identify relationships, expose indicators, and filter factual evidence. This is a process that forces the questioning of information to confirm truths and probabilities. The next process is to scrutinize the information to recognize trends that will lead to an event or pattern. Once a conclusion about the information has been formed, an assessment is made which is then presented to consumers so they can make well-informed decisions based on the analytic findings.

## QUALITATIVE METHODS OF PREDICTIVE ANALYSIS

In complex cases where multidisciplinary expertise would be valuable for analysis, a nominal group technique (NGT) and/or Delphi method<sup>746</sup> using subject-matter experts (SMEs) may also be employed to test for alternative futures.

Nominal group technique is a structured variation of a small-group discussion to reach consensus. NGT gathers information by asking individuals to respond to questions posed by a moderator, and then asking participants to prioritize the ideas or suggestions of all group members. The process prevents the domination of the discussion by a single person, encourages all group members to participate, and results in a set of prioritized solutions or recommendations that represent the group's preferences.<sup>747</sup>

The Delphi method, developed by the RAND Corporation,

... entails a group of experts who anonymously reply to questionnaires and subsequently receive feedback in the form of a statistical representation of the "group response," after which the process repeats itself. The goal is to reduce the range of responses and arrive at something closer to expert consensus.

Both approaches employ iterative processes that help to develop the best judgment findings on an issue based on the collective knowledge and interaction of experts.

The value of SMEs should never be underestimated. While not needed in all cases, there are times when the expertise of SMEs can detect subtle but important changes in the environment, politics, and other social and economic factors that can refine—and sometimes refocus—an intelligence forecast. Even experts, however, differ in the interpretation of events; hence the value of both the Delphi method and NGT for interpreting events and refining forecasts. The use of these techniques is a supplement to, not a replacement of, the intelligence analyst. The analyst

---

<sup>746</sup> See <https://www.rand.org/topics/delphi-method.html>.

<sup>747</sup> See <https://www.cdc.gov/healthyyouth/evaluation/pdf/brief7.pdf>.

focuses on the entire intelligence target and trend, whereas the use of Delphi and NGT should be more focused within the range of the SME's expertise.

When forecasts are developed, they should be based on a continuum of alternative futures. Particular focus should be directed toward critical events or circumstances that could direct behaviors toward a particular path leading to a threat. Just as important, attention should be devoted to potential "triggering events" or occurrences that could ignite a series of existing conditions to galvanize intelligence targets toward a particular incident. For example, we have seen:

- ◆ A growing visibility of right-wing extremism.
- ◆ A change from the more traditional white supremacy ideology to a broadened "white nationalism" ideology.
- ◆ A change in the approach, appearance, and demeanor of white nationalists to give their movement more legitimacy and make it look more mainstream.
- ◆ A growth in right-wing extremist nationalism internationally, notable in western Europe, Russia, and Australia.
- ◆ White nationalism moving away from rhetoric about racial differences and putting greater focus on immigration issues (both legal and illegal immigration).
- ◆ International and domestic white nationalists expressing concerns about essentially the same issues and increasingly communicating, presumably to share ideas.
- ◆ Aggressive use of social media and self-publishing<sup>748</sup> to market the ideology in a logical manner so as to push those leaning right farther to the right.
- ◆ A growing number of violent lone-wolf attacks by right-wing extremists, whose targets have been Jewish, Muslim, African American, and Latino.
- ◆ In at least two cases, publication of online manifestos by white nationalists proclaiming their ideology and serving to energize other ideologues.

Monitoring these events, an intelligence analyst would conclude that the sociopolitical caldron in the right-wing extremist community is boiling. More information is needed—these are the intelligence requirements—to see how these incidents/occurrences may be linked or how they may interact to forecast their relationship to any potential future violent attacks. Specifically, intelligence requirements would focus on such questions as these:

- ◆ In attacks that have occurred, are there triggering events that appeared to precede them?
- ◆ Are there organizations or collectives underlying this movement?
  - If so, who are the leaders/influencers?
  - What are their locations?
  - How structured are they?
- ◆ What specific types of communication are occurring between domestic right-wing extremists and those in other countries?
  - Are there actions or behaviors occurring overseas that have not traditionally happened domestically but that possibly could occur?
  - If so, what will the effects be, and how may one or more of these incidents influence the others?
- ◆ What would be likely triggering events to spawn violence on a broader scale?
  - How could these triggering events be neutralized?

The answers to these questions will help fill the intelligence gaps. More information is needed to understand the implications of these events and to forecast future events. The use of predictive analysis, as described above,

---

<sup>748</sup> <https://www.propublica.org/article/the-hate-store-amazons-self-publishing-arm-is-a-haven-for-white-supremacists>

including a panel of experts using either NGT or Delphi, can provide further insights into the subtle implications. Collectively, as requirements are fulfilled and events are analyzed in light of known facts and SME insight, operational responses can be made.

The intelligence cycle constantly seeks new information to refine the analysis and hence the forecast. This is consistent with the recursive nature and refinement processes of these techniques. Inherently, the process will not only help develop forecasts via predictive analysis, it will help refine the accuracy of the forecasts. Hence, the ultimate value of this methodology is to provide a structured foundation for planning, resource allocation, target hardening, intervention strategies, and operational readiness.

**Operationalizing the process.** The key to any type of analysis is reliance on the scientific approach to problem solving. The scientific method requires that there be a consistent, objective methodology to process information; procedures to ensure validity and reliability of the information on which decisions are being made; use of logical reasoning; accepted quantitative assessment of data when available; use of corroborative tests to verify both the raw information/data and analytic conclusions; and forecasts based on limited parameters—or confidence levels—to account for unexplained, unidentified, or variant occurrences in the behaviors being assessed.

With respect to predictive analysis as described thus far, the process embodies the following elements, representing the processes of the intelligence cycle:

1. Information is collected and analyzed based on hard data:
  - a. Derived from known past events or incidents.
  - b. Archived information/data.
  - c. New raw information based on information collection, whether human or technological.
2. This information is analyzed based on:
  - a. The *structure* of the incident—what were the primary, secondary, and tertiary motives, methods, and targets of the event?
  - b. The *constructs* of the incident—political, social, economic, and/or demographic factors that contributed to the event.
3. Intelligence gaps are identified in this segment of the analysis, and intelligence requirements are filled.
4. Further information collection and analysis continues until all intelligence gaps are filled or information collection options are exhausted.
5. The structural and construct variables are assessed in their current state to determine their impact on the probability of a future incident.
  - a. The importance of this step is to avoid linear analysis, instead relying on differential analysis of these factors in light of how they have changed or morphed.
  - b. In research, this is similar to the assessment and analysis of antecedent and intervening variables.
6. Based on the collective outcomes of the above steps, develop a logical, requirements-driven, nonlinear forecast of factors related to the incident or event.
  - a. Importantly, alternative forecasts—or alternative futures—should be developed in light of logical variations of the variables shaping the future events.
    - ii. These alternative futures represent the confidence levels or parameters of the forecasts.
  - b. The reasons on which the alternative futures are based should be clearly articulated with respect to the validity and reliability of the raw information sources and changes that have occurred in the social and political environments.

7. Based on this analysis, recommend strategies to prevent or at least mitigate the alternate future events should be offered.

It should be reinforced that predictive analysis is most applicable to strategic forecasting; however, in the cases of large criminal enterprises or terrorist organizations, the process may also be useful for tactical purposes. The greatest challenges are to have comprehensive and continuous information sources; critical thinking by the analyst; and a thorough understanding of the social and political environments of the intelligence targets.

## SUMMARY

Intelligence analysis is both the development of cognition and a cognitive process. Through ongoing analysis, the analyst is in a learning process to understand the target and the environment under analysis. Thus, it is a cognitive process because the analyst is learning as he/she performs the analysis. But it is also the development of cognition because the output of the analysis—conclusions, estimates, forecasts—is new knowledge that will be shared with others in reports and briefings. Thus, effective analysis should serve the law enforcement agency by:

- ◆ Identifying points of opportunity for intervention that might change the state of affairs in some way, especially *before* a conflict.<sup>749</sup>
- ◆ Helping states attain a comparative advantage in decision making, thus the term “actionable intelligence.”
- ◆ Protecting the state and its citizens to maximize security.
- ◆ Optimizing resources.
- ◆ Integrating information to enhance understanding of threat environments.

Analysis is a critical factor in information management because it provides the intelligence that describes criminal threats and alternatives to manage those threats. However, this information must be expressed in some form. That expression comes in the form of intelligence products.

## CONCLUSIONS

For effective information management in the intelligence process, there must be a common foundation and an ideological thread permeating the law enforcement organization. To meet the needs of contemporary law enforcement intelligence, including newly established national standards, the management of information requires:

1. **Reengineering some of the organization’s structure and information processes.** SLTLE agencies should examine their current intelligence processes, if any, to determine whether they are consistent with the NCISP and currently accepted national standards for law enforcement intelligence. If not, adjustments should be made in the organization and/or processes. This consistency is important so that there is a common understanding and acceptance of information validity, reliability, and consistency with civil rights standards. A common perspective of the intelligence process and a body of policies and procedures, all of which meet the same national standards, greatly enhances two-way information sharing—an essential element of requirements-driven intelligence.
2. **Developing a shared vision of the criminal or terrorist threat.** All agencies, at all levels of government, must define and understand the threats that face them. This does not mean that all communities are threatened in the same way, but that all agencies understand the “common enemies.” This includes a common understanding of threats and general agreement on the types of threats facing America. Important strides have occurred as cooperative initiatives and information sharing have taken place. For example, initiatives from the National Fusion Center Association and the CICC have addressed emerging issues and provided training

---

749 Rand, p. 8.

and products, respectively, to further enhance the information management in the intelligence process. With diverse membership from law enforcement agencies at all levels of government, the common lexicon is growing, and communication is increasing.

3. **A commitment to participate and follow through with threat information.** Effective information sharing can exist only if there is a true commitment by an agency to participate, not just give lip service to intelligence initiatives. To enhance output of these different national initiatives, an executive must ensure that personnel are trained in the intelligence process and policies are in place for effective, lawful, and reliable information collection and sharing (according to standards in the NCISP). Commitment also means that the chain of command reinforces the need to employ information collection and sharing processes. Too often, policies are in place, but they are irregularly applied. When this occurs, the intelligence process breaks down and the ability to connect the dots is jeopardized.
4. **A commitment of resources, time, and energy from an agency to the intelligence function.** A commitment to participate necessarily requires a commitment of resources. Intelligence is prevention-oriented. Often, it is difficult to see what has been prevented. Similarly, a great deal of information that is collected and shared leads to nothing; this is a fact of life in the intelligence enterprise. However, the critical few pieces of information that lead to the prevention of a terrorist attack are well worth the investment. The intelligence function should be a budget line in the regular agency budget, not an activity relegated to soft money or piggybacked on other agency activities. The lack of a budget line is tantamount to the lack of full commitment.
5. **Law enforcement leadership that embraces and promotes the idea that analysts are professionals who should be afforded equal treatment within the agency.** Too often, non-sworn analysts have been viewed as “second-class organizational citizens” because they are not sworn, despite the significant skills they have developed and applied to crime control within their communities.
6. **Proactive people using creative thought to identify “what we don’t know” about terrorism and organized crime.** Requirements-driven intelligence seeks to fully understand the environment of a community and how changes in that environment may influence threats or crime. Creativity requires that community conditions and potential threats be viewed through a different lens that seeks to interpret information in different ways. Terrorists and criminals have shown that they can be creative in the planning and execution of their crimes. Law enforcement must be similarly creative to identify changes in the threat environment and develop proactive operational initiatives to prevent those threats from reaching fruition.
7. **A law enforcement agency that thinks globally and acts locally.** Most people view issues in life from a provincial perspective. This is normal in that our greatest concerns are those which affect us in the most direct manner. Unfortunately, the provincial view does not always serve us well when we view events around the globe with the mistaken belief that “that won’t affect me.” Global events in terrorism and crime can affect us on local basis just as global economic events have an influence in our communities. As a simple example, terrorist events, war, economic markets, and political conflicts in the Organization of Petroleum Exporting Countries (OPEC) affect the prices we pay at our local gas pumps. We must recognize that international planning, financing, and logistical support of terrorism and criminal incidents can have an impact on our communities. Thus, local intelligence analysts must consider the extended effect of global incidents—such as the conflict between Israel and Hezbollah—and how that can be translated to local and regional reactions to those who support Islamic extremism. Similarly, the growth of right-wing extremism and nationalism in western Europe and Russia is influencing right-wing extremists in the United States. If an analyst does not have this information, it creates intelligence gaps that must be filled and applied locally.

It is all about the information—how well information is managed will dictate the quality and value of the intelligence.

# CHAPTER ANNEX 10-1: GLOBAL JUSTICE INFORMATION SHARING INITIATIVE

## CONNECTIVITY/SYSTEMS COMMITTEE INTELLIGENCE REQUIREMENTS SUBCOMMITTEE

### RECOMMENDATIONS FOR INTELLIGENCE REQUIREMENTS FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT (SELECTED EXCERPTS)

#### BACKGROUND

The Global Intelligence Working Group (GIWG) developed a series of standing intelligence requirements for the following crimes:

- ◆ Terrorism
- ◆ Major white-collar crime and identity theft
- ◆ Violent street gangs
- ◆ Drug-trafficking organizations
- ◆ Transnational and national criminal organizations
- ◆ Cybercrime
- ◆ Sexual predators
- ◆ Human trafficking/smuggling/immigration

Because of length limitations, only the standing intelligence requirements for violent street gangs are reproduced here to provide an illustration.

#### ISSUES

The FBI Intelligence Requirements Initiative and the *National Criminal Intelligence Sharing Plan* require new intelligence processes for local, state, and tribal law enforcement. Reengineering some organizations' structures and processes will be required to ensure that law enforcement in America is interoperable and able to seamlessly share important criminal intelligence information with each other. There must be a shared vision of the terrorist or criminal threat and a commitment to participate and follow through with threat information. There must be a commitment of resources, time, and energy from an agency to the intelligence function. A law enforcement agency must think globally and act locally.

The first step in the intelligence process is to develop a set of intelligence requirements so that everyone in the process clearly understands what information is needed. The FBI has developed a set of standard templates to be used to record the intelligence requirements, and they are available for use by all law enforcement agencies. For the FBI to appropriately address the intelligence needs of SLTLE, clearly defined intelligence requirements must be developed.

#### FINDINGS

Members of the GIWG Intelligence Requirements Subcommittee conducted research by reviewing existing materials, discussing this issue with members of several law enforcement agencies and the FBI, and relying on their own expertise and experience. It was determined that the whole concept of developing intelligence requirements in a formalized process is relatively new to SLTLE, with the exception of the larger and more sophisticated law

enforcement agencies. Therefore, an education process would be needed to inform SLTLE of the need and importance of developing requirements.

## RECOMMENDATIONS

### THREAT INFORMATION

When there is a specific threat that emerges from the national intelligence apparatus, the impacted SLTLE agency needs:

1. A simple standard evaluation process that rates the reliability of the source (rating system should include narrative detail, not merely a numerical or color-code quantifier).
2. Follow-up and ultimate resolution of the threat, meaning that once the federal sources discover the threat and eliminate or discount it, the local agency affected needs to be told and provided with closure. Also, during the period of evaluation, the local agency needs periodic updates as to whether the information and/or threat potential have changed. The FBI needs to ensure that the local field office supervisor or Special Agent in Charge (SAC) responsible provides quality information and liaison with the SLTLE chief executive until the matter is resolved.
3. SLTLE would prefer some guidance and action ideas on how best to deal with the threat while it is being investigated.

### INFORMATION SHARING SYSTEMS

There needs to be a single portal where SLTLE can go to access current intelligence information. Today there exist numerous law enforcement networks and systems, such as the Regional Information Sharing Systems (RISS), the Law Enforcement Online (LEO) system, the Homeland Security Information Network (HSIN), and Nlets – The International Justice and Public Safety Information Sharing Network, as well as various state and regional secure law enforcement networks. In addition, there are several classified networks that are available to SLTLE on a limited basis.

All of these networks provide a multitude of sites where pertinent intelligence information may be obtained. No matter which network an SLTLE officer may be connected to, there needs to be a single portal, available through any of the networks, where the officer can obtain all the pertinent intelligence that is available to the officer. This should be a Web-based application similar to the INTERLINK system. There also must be a simplification of the guidelines for access to the information.

### CONTENT

It is important that as much content as possible be provided to the SLTLE officer when information is provided. The intelligence requirements recommended by the subcommittee will go a long way in defining SLTLE information needs. Where possible, SLTLE agencies should be given direct access to federal data systems and reports so they may do their own analysis of the information presented. In the end, the SLTLE is going to have to make decisions on a course of action based on the intelligence information; therefore, it must be as complete as possible. Likewise, SLTLE agencies must be willing to open their files to the federal government even when they may not know the full extent of the investigation.

### PRIVACY

SLTLE agencies face mounting pressure to reassure legislative bodies and the public that they are not violating individual rights in the collection of intelligence information. This is a very sensitive issue in many parts of the country, particularly when the information is shared with federal agencies. The federal agencies need to be keenly aware of those sensibilities when asking SLTLE agencies to develop and share intelligence information.

## TRAINING

SLTLE officers and analysts need updated training and more course offerings on topics such as watch-list process; terrorism cell indicators; surveillance and reconnaissance indicators; operational security; and handling of sensitive, unclassified material. Officers are the first line of defense; therefore, providing the appropriate training is essential.

The FBI Directorate of Intelligence has committed to developing and delivering training to SLTLE officers and analysts in the process of developing intelligence requirements. It is important that the local FIGs and JTTFs be involved in that training so that SLTLE officers and analysts may start developing that professional relationship that is so important.

It is important that intelligence training be delivered to small- and medium-sized agencies that may not have the resources to have full-time intelligence operations. Even without full-time assignments, those agencies and their members are vital to the law enforcement intelligence process.

## INTELLIGENCE REQUIREMENTS FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT

This form is intended to document the federal intelligence requirements for SLTLE in the United States. In addition, it is intended to provide federal law enforcement officials with the intelligence capabilities of SLTLE agencies to support federal missions.

### CATEGORY: VIOLENT STREET GANGS

## SLTLE INTELLIGENCE REQUIREMENTS

### GLOBAL, NATIONAL, AND LOCAL TREND REPORTS REGARDING ORGANIZATIONS AND STRUCTURES OF ACTIVE GROUPS IN THE UNITED STATES

- Identity of suspects and their roles in the local area; territorial reach
- Decision-making processes; degree of subordinate autonomy
- Command-control-communications techniques, equipment, network

### TACTICS OF INTIMIDATION, INTERFERENCE WITH FREE EXERCISE OF CIVIL RIGHTS

- Targets of hate groups, ethnic supremacist organizations
- Incidents of violence or incitement against individuals, groups, places of worship, schools, commercial entities identified with ethnic or political minorities

### RECRUITMENT; TRAINING; COLLABORATION BY SUSPECT GROUPS

- Recruitment techniques and priority targets

### CHARACTERISTICS OF GROUP

- Customs, norms, patterns
- Goals
- Recruitment, membership, principal ethnic group
- Advancement
- Expulsion
- Control methods
- Dress
- Colors
- Graffiti
- Signs/signals, communication, codes/vocabulary/terms
- Locations for meetings/housing/public forums

## ORGANIZATIONAL FUNCTION/METHOD OF OPERATIONS

- Email address/IP address; ISP
- Chat rooms, bulletin boards/websites visited
- Communication system; Instruments/equipment used
- Equipment source
- Base location
- Radio frequencies, two-way radios
- Scanner use
- Codes/call signs
- Telephone service; caller ID, call waiting, conference call
- Interactive data/video capabilities; cable/satellite
- Page service provider/type
- Software/hardware/networks used, encryption devices

## WEAPONS

- Type
- Serial number
- Source
- Proficiency
- Explosives
- Biological (anthrax, ricin, smallpox)
- Chemical (blister agents, cyanide, nerve gas)

## SUSPECTS

- Background, education, nationality, citizenship, ideology, etc.
- Employment/professional associations and affiliations
- Computer knowledge (level of proficiency)
- Computer access/authorized access/ISP/IP addresses/emails/Internet identities
- Use of IRC/public Internet access/wireless devices
- Motive
  - White hate
  - Malicious
  - Revenge
  - Economic gain

## ASSETS/BUSINESS/FINANCIAL

- Bank accounts
- Credit cards, credit information
- Debt/loans
- Economic status/financial security
- Safety deposit box
- Real estate
- Vehicles/boats/planes
- Business employment, type, background, location, and articles of incorporation
- Books/record keeping
- Civil/criminal cases
- Correspondent banks
- Dunn and Bradstreet, Prentice Hall
- Minutes of director meetings
- Questionable/at-risk transactions
- Regulatory actions

# CHAPTER 11

## THREAT ASSESSMENTS AND INTELLIGENCE PRODUCTS



Much of the work of an intelligence analyst involves following up on tips, leads, and suspicious activity reports; supporting ongoing criminal inquiries; aiding in the planning for special events; monitoring threat streams; communicating with analysts and investigators from other jurisdictions; and consuming intelligence reports and products from other agencies to determine their applicability to their jurisdictions. All of this work is essential, but it is also generally *reactive*—that is, the analyst is reacting to requests and information feeds.

Another important responsibility of intelligence analysis is to perform *threat assessments* to determine whether community safety is in jeopardy—this is a *proactive* analytic responsibility. If threats are identified, the analyst seeks to determine the likelihood of a criminal event occurring from the threat and the impact of the criminal event on the community, including injury/death, property damage, disruption of essential services, and other potential impacts on community safety that are unique to the nature of the criminal event. The results of a threat assessment are communicated in intelligence products that will have different content and structure based on the intended consumer (e.g., police command, line officers, elected officials, businesses, and organizations likely to be impacted by the criminal event, community members, and relevant special interest persons or groups).

A threat assessment is “a behavior-based and deductive process.”<sup>750</sup> Unlike profiling, which compares characteristics of an individual to characteristics of past offenders, the threat assessment focuses on behavior—demonstrable

---

750 Modzeleski, W., & Randazzo, M. R. (2018). “School Threat Assessment in the USA: Lessons Learned from 15 Years of Teaching and Using the Federal Model to Prevent School Shootings.” *Contemporary School Psychology* 22, 109–115, p. 111.

actions that are indicative of probable criminality. It is ultimately concerned with whether a person, a group of people, a criminal enterprise, or a criminal extremist movement *poses* a threat to commit targeted violence or other crimes—not whether the criminal entity has *made* a threat. Threats are often made without the ability or intent to actually follow through with the threat. A threat assessment focuses on determining whether the criminal entity not only has the intent but also the capability to carry out the threat. The assessment also includes operational options to prevent the threat from being carried out.

## THREAT ASSESSMENTS AND TARGETED VIOLENCE

While threat assessments can be performed for any type of criminal enterprise, the greatest threat concern is targeted violence. As explained by the Targeted Violence Research Team from the University of Nebraska:<sup>751</sup>

**Targeted violence** refers to violence that is goal-directed, predatory, and focused towards a specific individual(s) (e.g., stalking, terrorism, sexual assault). **Threat assessment** is the process of gathering information in an effort to estimate the threat of violence posed by a person or group of persons. **Threat management** refers to strategies that can be taken to prevent violence and mitigate a threat. In contrast to the assessment of impulsive behavior, law enforcement and mental health practitioners addressing “targeted violence” address situations in which there is the assessment of risk posed to an identified (or identifiable) target by an identified (or identifiable) perpetrator. (Emphasis in original.)

While the underlying rationales may differ, the threats of targeted violence and terrorism increasingly overlap, intersect, and interact with each other. Likewise, there is some alignment in the tools that can be applied to address them. Preventing targeted violence and terrorism necessitates using all tools in the law enforcement and homeland security toolbox: *reactive* measures, such as the traditional law enforcement tools of investigations and prosecutions, and *proactive* measures that are aimed at building protective capabilities of individuals and groups who are probable victims. These proactive prevention activities range from target hardening to public education to empowering communities and individuals to marginalize violent messaging while protecting and championing democratic responsibilities and values (the approach of countering violent extremism<sup>752</sup> or CVE).<sup>753</sup>

During the threat assessment process for targeted violence, analysts seek to develop answers to core questions:<sup>754</sup>

1. How do attackers develop the idea of committing a targeted violence attack?
2. How does a person move from the idea of an attack to the action of attacking?
3. What motivates people to act violently toward the intended victims of the attack?
4. What relationships exist—if any—between potential victims and targeted violence behaviors?
5. How do people who plan to commit targeted violence select their specific target(s)?
6. What planning strategies are used by people who commit acts of targeted violence?
7. What relationships exist—if any—between threatening to commit violent action and carrying out violent action?
8. Were there key life events and patterns in the histories of people who have committed acts of targeted violence that are notable indicators?

---

751 <https://psychology.unl.edu/targeted-violence/home>

752 <https://www.dhs.gov/CP3>

753 <https://www.dhs.gov/tvtpgrants>

754 *Modified to reflect current issues and trends from:* Fein, R., & Vossekuil, B. (1999). “Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approaches.” *Journal of Forensic Sciences* 44(2), 321–333.

The Safe School Initiative, a joint project of the U.S. Secret Service and the Department of Education, examined 37 incidents of “targeted school violence” that occurred in the United States.<sup>755</sup> The findings, while focused on school shootings, likely have broader applications to other forms of targeted violence, which can aid in developing a threat assessment. These include the following:

- ◆ Incidents of targeted violence at school rarely were sudden, impulsive acts.
- ◆ Prior to most incidents, other people knew about the attacker’s idea and/or plan to attack.
- ◆ Most attackers did not threaten their targets directly prior to advancing the attack.
- ◆ There is no accurate or useful profile of students who engaged in targeted school violence.
- ◆ Most attackers engaged in some behavior prior to the incident that caused others concern or indicated a need for help.
- ◆ Most attackers had difficulty coping with significant losses or personal failures. Moreover, many had considered or attempted suicide.
- ◆ Many attackers felt bullied, persecuted, or injured by others prior to the attack.
- ◆ Most attackers had access to and had used weapons prior to the attack.
- ◆ In many cases, other students were involved in some capacity.
- ◆ Despite prompt law enforcement responses, most shooting incidents were stopped by means other than law enforcement intervention.

With increasing numbers of law enforcement agencies expected to develop plans and operational responses that prevent school shootings, developing an expertise in assessing targeted violence threats becomes a high priority.

In a recent threat assessment guide published by the United States Secret Service National Threat Assessment Center, the cautionary advice of the authors was:

Despite having a comprehensive targeted violence prevention plan in place, and despite a school and Team’s best efforts at prevention, incidents of targeted school violence may still occur. It is critical to develop and implement emergency response plans and procedures and provide training on them to all stakeholders. The U.S. Department of Homeland Security recommends that emergency response plans be developed with input from local law enforcement and first responders. For example, procedures should be developed for reporting emergencies, evacuation procedures and routes, use of emergency notification systems, and information regarding local hospitals or trauma centers. Law enforcement and first responders should be apprised of these plans and procedures and know how to implement them.<sup>756</sup>

Beyond school shootings, targeted violence has become all too common in the United States.<sup>757</sup> While there are exceptions such as workplace violence, most targeted violence of recent years was committed by lone-wolf ideological extremists. Consequently, the most effective threat assessments would likely focus on probable victims and targets more than likely offenders per se.

---

755 Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*. Washington, DC: U.S. Secret Service and U.S. Department of Education.

756 Alathari, L., et al. (2018). *Enhancing School Safety Using a Threat Assessment Model*. Washington, DC: U.S. Secret Service National Threat Assessment Center, p. 23.

757 *DHS Strategic Framework for Countering Terrorism and Targeted Violence*. (2019). [https://www.dhs.gov/sites/default/files/publications/19\\_0920\\_plcy\\_strategic-framework-countering-terrorism-targeted-violence.pdf](https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf)

## THE THREAT ENVIRONMENT

In Chapter 10, a caveat was noted: “The absence of evidence is not the absence of a threat,” whether that threat is targeted violence or some other crime. Hence, a key factor in an assessment of a threat is to identify previously unknown evidence of threats to monitor trends and key indicators. Illustrations include the following:

- ◆ **Threats from Islamic extremists:** Examining trends notably from ISIS and al-Qaeda where they state their priorities and changes in methods and targets. The organizations are typically quite open in their social media posts, using the material for not only propaganda but also to inspire adherents who are often self-radicalized. “Thinking globally, acting locally” is a perspective used when assessing these threats, recognizing that self-radicalized homegrown violent extremists (HVEs) have a higher probability of committing the attack than do ISIS or al-Qaeda.<sup>758</sup>
- ◆ **Threats from white nationalists and right-wing extremists:** Look for trends in targets (e.g., synagogues, immigrants, and minorities) and trends in ideology (e.g., ecofascism) and apply them to the local community. At least two white nationalists posted manifestos<sup>759</sup> online before their attacks, which provided detailed insight about their thought processes. This can be very valuable for understanding their intent and targets. Importantly, there is a significant right-wing extremist presence in western Europe that communicates with its North American counterparts. Historically, the focus on right-wing extremism did not look beyond U.S. borders—this needs to change.<sup>760</sup>
- ◆ **Emerging and changing extremist trends:** The presence of extremism in our communities historically varies based on many factors ranging from politics to economics, changes in social trends, government policy, and even legislation and judicial decisions. The anti-government movements, anti-immigration movements, anti-abortion extremists, environmental extremists, left-wing anti-Fascists (e.g., Antifa), and Incels<sup>761</sup> have all been involved in violence at some point. Monitoring the range of extremism and assessing the threat that extremists pose when their issues become more prevalent is an important aspect of contemporary threat assessment.<sup>762</sup>
- ◆ **Gangs:** Whether the violent international gang MS-13;<sup>763</sup> regional gangs, such as Tango Blast/Vallucos;<sup>764</sup> a gang that is essentially a crime cartel with a long reach, such as Los Zetas;<sup>765</sup> or local street gangs known for violence, each can pose a threat to a community. Less likely to use targeted violence such as the ideologues, these gangs nonetheless affect the community not only as a result of criminal operations but also intergang violence that can too many times victimize nongang members. Monitoring the trends in gangs, particularly rivalries and involvement in crime, is necessary for community safety. Changes in gang trends may warrant a full gang threat assessment.

---

758 Wray, C., Director, FBI. (October 30, 2019). *Global Terrorism: Threats to the Homeland*. Washington, DC: Statement Before the House Homeland Security Committee.

759 For example, see <http://republicbroadcasting.org/wordpress/wp-content/uploads/2019/03/the-great-replacement-e28094-manifesto-e28094-new-zealand-mosque-shooter-ver-3.pdf>.

760 McGarrity, M., & Shivers, C. (FBI). (June 4, 2019). *Confronting White Supremacy*. Washington, DC: Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties.

761 <https://www.psychologytoday.com/us/blog/minority-report/201804/the-incel-involuntary-celibacy-problem>

762 National Counterterrorism Center. (2019). *Homegrown Violent Extremists Mobilization Indicators*. Washington, DC: Office of the Director of National Intelligence.

763 <https://www.dhs.gov/keywords/ms-13>

764 Texas Joint Crime Information Center, Intelligence and Counterterrorism Division. (2018). *Texas Gang Threat Assessment*. Austin, Texas: Texas Department of Public Safety.

765 <https://ctc.usma.edu/a-profile-of-los-zetas-mexicos-second-most-powerful-drug-cartel/>

- ◆ **National trends that could translate to local threats:** Sometimes, instances of targeted violence are inexplicable.<sup>766</sup> Moreover, there is often the fear that these incidents will induce “copycat” events. Frankly, it is almost impossible to assess a threat of such incidents. Other national trends, notably school shootings, are more amenable to assessments. Monitoring trends, establishing tip lines, and working with school resource officers and school personnel can aid in performing this type of threat assessment.<sup>767</sup>
- ◆ **Human trafficking:** Threats are not always targeted violence but are sometimes directed toward vulnerable victims. Human trafficking has long been involved in the sex trade; however, trends have shown increasing numbers of human trafficking victims working as housekeepers in hotels and in agriculture. Hotels in tourist areas, large agricultural operations, particularly seasonal ones, and other businesses that require a workforce of largely unskilled laborers should be viewed as potential targets for human trafficking.<sup>768</sup>
- ◆ **Illegal drug trafficking:** The DEA has stated that illicit drugs, and the transnational and domestic criminal organizations that traffic them, continue to represent significant threats to public health, law enforcement, and national security in the United States. The opioid threat (controlled prescription drugs, synthetic opioids, and heroin) continues at ever-increasing epidemic levels, affecting large portions of the country. Meanwhile, the stimulant threat (methamphetamine and cocaine) is worsening and becoming more widespread as traffickers continue to sell increasing amounts outside of each drug’s traditional markets. New psychoactive substances (NPSs) remain challenging, and the domestic marijuana situation is evolving as state-level medical and recreational legalization continues. Drug poisoning deaths are the leading cause of injury death in the United States.<sup>769</sup> Beyond the public health threat posed by drug abuse is the violence too often associated with trafficking. It is an ever-changing threat that warrants assessing at the local and regional levels.
- ◆ **Illicit consumer goods:** Trends vary with illicit consumer goods. For example, in states where recreational marijuana has been legalized, black-market marijuana is thriving because it is cheaper; when new phones or other technologies become available, the black market for these items grows; in recent years, there has been a growing market in stolen arts and antiquities; similarly, there are illegal conservation markets dealing with such things as pelts of endangered species and ivory. Beyond the inherent crimes committed, smugglers and organized crime are also typically involved. Trends emerging in a community or region may warrant a threat assessment of these types of goods and their impact on a community.<sup>770</sup>
- ◆ **Cyberthreats:** While often not the type of assessment performed by most state and local law enforcement agencies, there is a need for agencies responsible for cybercrimes to monitor cyberthreat trends and perform assessments as appropriate for their authority. Examples of such threats are darknet criminal trends, ransomware, new malware, emerging attack targets and methods, and cybercriminals taking advantage of a crisis, such as the 2020 novel coronavirus pandemic, to commit fraud and attacks.<sup>771</sup>

766 Such as the 2017 mass shooting in Las Vegas, Nevada, that killed 59 people and injured more than 500. See *Las Vegas Metropolitan Police Department Preliminary Investigative Report of 1 October 2017 Mass Casualty Shooting*. [https://www.lvmpd.com/en-us/Documents/1\\_October\\_FIT\\_Report\\_01-18-2018\\_Footnoted.pdf](https://www.lvmpd.com/en-us/Documents/1_October_FIT_Report_01-18-2018_Footnoted.pdf)

767 School threat assessments provide more resources than other types; for example, see <https://www.schoolsafety.gov/prevent/threat-assessment-and-reporting> and <https://www.nasponline.org/resources-and-publications/resources-and-podcasts/school-climate-safety-and-crisis/systems-level-prevention/threat-assessment-at-school/threat-assessment-for-school-administrators-and-crisis-teams>.

768 <https://www.fbi.gov/investigate/violent-crime/human-trafficking>

769 <https://www.dea.gov/sites/default/files/2020-02/DIR-007-20%202019%20National%20Drug%20Threat%20Assessment%20-%20low%20res210.pdf>

770 As an example, see <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/illicit-trafficking-in-cultural-goods-including-antiquities-and-works-of-art>.

771 <https://www.fbi.gov/investigate/cyber>

Threat assessments can be difficult and time-consuming to perform but can significantly enhance community safety. In efforts to make the process easier, there have been attempts to make threat assessment checklists and model forms; however, these are significantly limited because of the diverse nature of threats and the need to invest time in the collection and analysis of information to make more accurate assessments. Essentially, there are few shortcuts. For example, assessing the threat to a school from possible school shooters, the threat to computer systems from possible ransomware attacks, and the threats posed by the Sinaloa drug cartel all require different methods, different types of subject-matter expertise and different sources of information. The approach taken herein is to provide the conceptual framework for threat assessments and present methodological considerations. As a foundation, there are two fundamental concepts to understand: threat and risk.

## UNDERSTANDING THREATS AND RISK

There is often confusion involving the concepts of threat and risk. While sometimes the terms are used synonymously, they have distinctive, yet interrelated, meanings. It should be noted that these concepts have different applications to different industries: Oil exploration, public health, and life insurance, for example, all have different definitions and approaches to threats and risks.<sup>772</sup> Hence, the current discussion has specific application to law enforcement's responsibility for public safety from criminal threats.

To begin, an important responsibility for the analyst is to identify *threats* to the community through the intelligence process. From a law enforcement intelligence perspective, a threat exists when an extremist ideological or criminal entity has:

- ◆ The intent to commit an attack/crime.
- ◆ Developed a plan for an attack/crime.
- ◆ The personnel to execute the plan.
- ◆ The resources necessary to make the plan a reality.

These four factors may be detailed and sophisticated or they may be incidental and somewhat disorganized, but they nonetheless exist. For example, a self-radicalized lone-wolf extremist decides to commit an attack in furtherance of his/her ideology with the use of a vehicle as the weapon.<sup>773</sup> The attacker has developed the *intent* through self-radicalization. For the attack *plan*, the attacker must decide when and where the attack will occur as well as how he or she will use the vehicle as a weapon. In this case, the only *personnel* needed to execute the plan are the attackers themselves. *Resources* for this plan are few, but importantly must include a vehicle. Hence, even though this is a logistically simple attack, the elements exist. More sophisticated attacks, complex criminal enterprises, and even gang crimes use these four elements—in differing degrees of sophistication—to commit their crimes or attacks. While lone wolf-attacks are extremely difficult to identify and forecast, the advantage of investigating more sophisticated criminal and terrorist organizations is that there are more people, logistics, and materiel involved, providing more evidence for analysis and thereby increasing the accuracy of the assessment.

In identifying a threat, the intelligence process seeks as much information as possible on these four factors because this information will guide analysts toward making a judgement about the viability of the threat, possible targets, and possible timing. Law enforcement often receives threat information—such as a threat at a school, a criminally extreme ideological group making threatening statements directed toward possible targets, or gang members threatening violence against a rival gang. As a result, law enforcement must determine whether the individual or group is *capable* of following through with the threat. In particular, the *plan*, *personnel*, and *resources* will provide important information about the *capability* to commit the attack. Capability is not a dichotomous assessment but exists on a continuum ranging from *no capability* to *absolute capability*. As capability to commit the crime or attack

<sup>772</sup> A later discussion will also address “vulnerabilities,” a factor that increases the probability of victimization from the threat.

<sup>773</sup> <https://www.counterextremism.com/vehicles-as-weapons-of-terror>

increases, so does the probability that the criminal event will occur. Hence, the more information that can be collected and effectively analyzed, the more it will help analysts decide where, on the continuum of capability (hence probability), a particular threat lies. Broadly speaking, key factors where information needs to be developed include the following:

- ◆ What is the likelihood that an attack/criminal event will occur?
- ◆ What/who are the likely target(s)/victims/commodities?
- ◆ What is the probable time frame(s) for the criminal event(s)?

The answers to these questions will aid in planning for the prevention, mitigation, and response to the threat. Rarely is there a high degree of certainty; typically, it is a matter of probability.

From the perspective of threat assessments, risk can be defined in several ways depending on the context—for example, risk of investing in the stock market, risk for determining car insurance premiums based on one’s driving record, or risk of disease based on one’s lifestyle. For the current discussion, *risk* is the probability of harm coming to victims of the threat. The term “victims” can be widely defined and is dependent on the nature of the threat. Victims may be individuals, groups, or classes of individuals or may be broadly defined as the community as a whole, to include facilities, services, and infrastructure. A community is also a victim when threats instill fear and/or have a negative social and/or economic impact on the entire community.

Whereas threats focus on the probability of an *offender* committing a crime or attack, risk refers to the probability of being the *victim* of a crime or attack. While exact probabilities of victimization cannot be determined, broad categories of risk levels—such as “low risk,” “moderate risk,” and “high risk”—can provide guidance for community members to make informed decisions about where to go/what to do and when. For example, if there is a credible high-risk threat to a subway system, one’s risk can be reduced by not riding the subway. Similarly, understanding the threat and identifying victims at risk can help harden targets to provide intervention to potential victims. Thus, one goal in intelligence is to reduce risk—ideally through *prevention* but also through *mitigation of the seriousness* of the harm. With knowledge about the capability, likely targets, and time frame of the threat, we seek to reduce the risk of an attack by intervening with the threat components.

## THE CHARACTER OF THREAT ASSESSMENTS

Based on the discussion of threats and risks, the next challenge is to determine whether a threat exists. A threat assessment is defined by the U.S. Department of Homeland Security (DHS) as “a product or process of evaluating information based on a set of criteria for entities, actions or occurrences, whether natural or manmade, that have or indicate the potential to harm life, information, operations and/or property.”<sup>774</sup> This obviously encompasses a wide range of threats from terrorism to tornados.<sup>775</sup>

As defined by DHS, threat assessments include natural disasters as part of the homeland security mandate. However, examining threat assessments from the narrower law enforcement intelligence perspective, there are five core purposes for the assessment.

1. **Prevention and mitigation.** The best outcome from a threat assessment is to prevent a harmful event from occurring. Pragmatically, however, that is not always possible; hence we should also seek to mitigate the effects of a threatening event. For example, if right-wing extremists are threatening a synagogue, efforts

---

<sup>774</sup> *DHS Lexicon Terms and Definitions*. (2017). Washington, DC: Management Directorate, U.S. Department of Homeland Security, p. 662. [https://www.dhs.gov/sites/default/files/publications/18\\_0116\\_MGMT\\_DHS-Lexicon.pdf](https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf)

<sup>775</sup> Note that the DHS responsibility goes beyond all crimes and includes all hazards. While state and local law enforcement agencies will assist their public safety partners in preparing for and responding to all hazards, the law enforcement threat assessment responsibility is typically limited to criminal threats, including terrorism.

should be made to harden the target, such as increasing security measures. If a gang threat assessment suggests that two rival gangs are preparing for an armed confrontation, having gang investigators contacting members of the gangs to intervene as well as increasing the marked police presence on the gang turf may help prevent or mitigate violence.<sup>776</sup> A criminal event may not be completely prevented; however, law enforcement should take steps to reduce the risk to the victims and minimize the intended effects of the event.

2. **Resource allocation/deployment.** If an assessment of a threat indicates a high risk to a specific class of victims and/or location(s), a strategy to prevent the threat will often require reallocating resources. For example, a threat to an entertainment venue may result in the deployment of metal detectors, increased surveillance resources, deployment of tactical teams to stand by, temporary assignment of analysts and investigators to work exclusively on the threat, and deployment of uniformed officers for a more visible police presence at the venue. Virtually any type of credible threat of a criminal event will require some type of personnel adjustments. The threat assessment should thus include information about geographic and temporal factors, whether special expertise (e.g., a bomb squad) is needed and any unique issues/circumstances that can aid law enforcement management in making decisions on the needs, character, and duration of resource reallocation.
3. **Identification of indicators.** An important role in the analysis of a threat is to identify indicators of the threat. Indicators are factors that are consistently associated with the threat and collectively suggest the presence of the threat. Indicators may include signs, symbols, words, gestures, language, clothing, colors, and behaviors. For example, there are some consistent indicators of human trafficking,<sup>777</sup> gangs,<sup>778</sup> white supremacy,<sup>779</sup> terrorism,<sup>780</sup> drug couriers,<sup>781</sup> school shootings,<sup>782</sup> illicit wildlife trafficking,<sup>783</sup> and virtually any other type of criminal enterprise or extremist activity. While these types of indicators are good guideposts, analysis of the threat will typically produce additional, more specific indicators that are unique to the particular threat at hand. The importance of indicators is to inform law enforcement officers, security personnel and often the public of what to look for and report if the indicators are observed. Care must be taken to focus human indicators on behaviors and not exclusively on attributes such as race or ethnicity.
4. **Training.** Most police officers receive a barrage of intelligence products and reports on various threats and community safety issues. Because of the volume, many officers admit they do not read all the material they receive, much of which is irrelevant to their assignments, which is indeed true. Threat assessments typically have more detail than many other intelligence products officers regularly receive, and the assessment will be more jurisdiction-specific. As a result, when a threat assessment identifies a credible threat within a certain geographic area or jurisdiction, officers need to receive training on the offender indicators, likely targets, and actions that need to be taken for both prevention and response. Typically, this can be done in roll-call training but nonetheless needs to be done in certain high-threat circumstances to ensure that officers are being fully prepared for the threat.
5. **Public education.** When a credible threat is identified in a community, there is an obligation to inform the public for two reasons: first, to help members of the public become self-aware to avoid circumstances where they may risk victimization by the threat and second, to aid the public in knowing what to look for to report suspicious activity (e.g., “See Something, Say Something®”). Because of the research and analysis performed in

---

776 There is an explicit example of this gang tactic being used by the Richmond, Virginia, Police Department. It is called the Retaliation Assessment Tool. See Carter, D. L. (2013). *Homicide Process Mapping: Best Practices for Increasing Homicide Clearances*. Tallahassee, FL: Institute for Intergovernmental Research and the Bureau of Justice Assistance, p. 24. <https://www.nationalpublicsafetypartnership.org/clearinghouse/Resource/175>

777 <https://www.dhs.gov/blue-campaign/indicators-human-trafficking>

778 <https://www.annapolis.gov/637/Indicators-of-Gang-Activity>

779 <https://www.adl.org/hatesymbolsdatabase>

780 <https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf>

781 <https://apps.dtic.mil/dtic/tr/fulltext/u2/a620185.pdf>

782 [https://www.cisa.gov/sites/default/files/publications/18\\_0711\\_USSS\\_NTAC-Enhancing-School-Safety-Guide.pdf](https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf)

783 [https://cites.org/sites/default/files/eng/prog/iccwc/ICCWC-Ind-FW-ASSESSMENT\\_TEMPLATE-FINAL.pdf](https://cites.org/sites/default/files/eng/prog/iccwc/ICCWC-Ind-FW-ASSESSMENT_TEMPLATE-FINAL.pdf)

a threat assessment, more explicit detail about a threat is likely to be known, as compared with general threat indicators and safety information. Providing detail about a potential threat can help keep the public safe and increase the probability of prevention.<sup>784</sup>

Hence, an important responsibility of an intelligence unit is to understand the nature of criminal threats likely posed to one’s jurisdiction and then provide an assessment on the presence, probability, and impact of the threat.

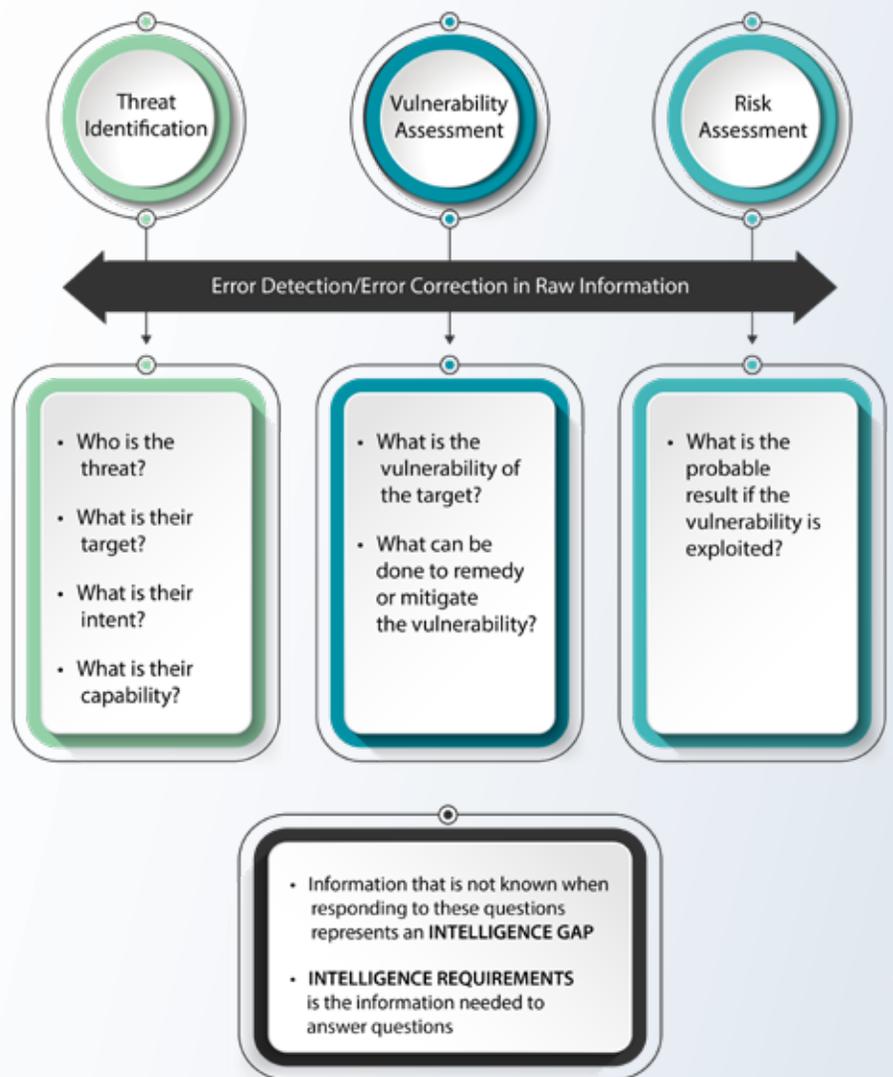
## CRITERIA FOR ASSESSING THREATS

A threat must be assessed on multiple criteria, as illustrated in Figure 11-1. The first threat component is *threat identification*. When evidence of a threat is identified, the intelligence process must assess where the threat lies on a multivariate continuum of probability. While quantifying a threat would add an element of precision, typically the variables related to a threat can be measured only on an ordinal scale.<sup>785</sup> For example, based on qualitative data, a judgment can be made on the relative value of a threat variable on a scale of 1 to 10. As illustrated in Figure 11-2, the

first two variables (A and B) measure the *quality* of the information. The second two variables (C and D) measure the *probable outcome* of the threat. Combined, they provide guidance for decision making. A moderate assessment of the *quality of information* may produce a different operational response as the severity of the threat increases. As severity decreases, a higher quality of information may be desired before an operational response is made. This is basically a method to weigh risk/outcome tradeoffs.

The next step is a *vulnerability assessment* of probable targets. When a threat is identified, then the universe of targets is typically narrowed. Regardless of whether the probable number of targets is large or small, some judgments can be made on how vulnerable the targets are. As vulnerability increases, so does the probability of the threat. For example, assume that a small group of ecoterrorists plans on fire-bombing the sales inventory of various automobile dealers who sell large trucks. Most dealership sales lots are accessible 24 hours a day. As such, their vulnerability increases and so does the threat. In a different scenario, assume that the same

FIGURE 11-1: THREAT ASSESSMENT COMPONENTS FOR PLANNING AND DIRECTION



784 As an example, in 2018, an individual left a series of bombs over a period of roughly three weeks around Austin, Texas. With each bomb that was left, police analysts obtained more information about the bomber. See <https://www.nytimes.com/interactive/2018/03/19/us/austin-explosion-bombings.html>.

785 An ordinal scale is a scale of measurement in which data are put in rank order, but there is no fixed amount of difference between the points on the scale. For example, college sports rankings rate the top 20 teams. The ranking, however, does not mean that the team ranked first is 20 times better than the 20th-ranked team.

group of ecoterrorists plans to fire-bomb tanks at a military installation to protest the fuel consumption and damage done to the environment by the tanks traversing their training range. In this case, target vulnerability is low because of the inaccessibility of the tanks on the military base and the ability of the tanks to withstand Molotov cocktails should the intruders get near them. As should be apparent, target vulnerability is an important variable in any threat assessment.

Once threats and target vulnerability have been identified, a *risk assessment* is made. Risk is epitomized by the question: What is the probable result if the attack/criminal event occurs? In the above illustration, the risk to the automobile dealers may be high and the risk to the military installation low. However, before a conclusion may be drawn on risk, more information is needed to corroborate judgments and determine whether there are other, previously undiscovered, compounding factors. This process helps define further *intelligence requirements*—information that needs to be collected to better understand the threat.

Essentially, the threat assessment process seeks to make a distinction on whether an intelligence target is making a threat or posing a threat. This is obviously subjective; hence as much information as practicable should be collected and analyzed on these three factors. In most instances, there will be insufficient information to make a precise assessment of each component of the threat assessment model. As a result, answers to the requirements questions will help clarify the threat picture. Obtaining additional information will increase the *quality* of intelligence by identifying and eliminating error.

It should also be recognized that previously undefined threats may also emerge. Changes in the character of a community may stimulate new threats, the presence of a particular target may draw a threat, or the threat may simply appear as a result of the combined effect of many factors. The point is that law enforcement personnel must be trained to identify behaviors that are more than merely suspicious, record the behaviors with as much detail as possible, and forward this information to the intelligence analysts.

## METHODS

Conducting threat assessments often requires creative analysis, developing a depth of knowledge on different subject matter, developing new methods of information collection, and often exploring nontraditional avenues of information collection and analysis to fully understand a threat. Two examples are understanding patterns of violent death from the CDC Violent Death Reporting System<sup>786</sup> for strategic analysis and using social network analysis<sup>787</sup> to examine the relationships among and between criminal groups.

---

786 <https://www.cdc.gov/violenceprevention/datasources/nvdrs/index.html>

787 <http://www.analytictech.com/networks/whatis.htm>

FIGURE 11-2: SIMPLIFIED THREAT ASSESSMENT ILLUSTRATION<sup>788</sup>



Beyond using the scientific approach to problem solving, there is no single threat assessment methodology for law enforcement intelligence—the process tends to differ based on the threat, the target, and the sources and types of information available for analysis. For example, threat assessments may be performed on the illicit trafficking of stolen arts and antiquities,<sup>789</sup> human trafficking,<sup>790</sup> threats from the illicit drug trade,<sup>791</sup> school shootings,<sup>792</sup> terrorism,<sup>793</sup> or any of a wide variety of other threats to public safety.<sup>794</sup> It is immediately apparent from looking at these diverse threats that each requires different sources of information and different methodologies. As a result, initial steps in the assessment are as follows:

- ◆ **Understanding the entity posing a threat.** If the threat is posed by a criminal enterprise, is it one organization or multiple organizations? What is the structure of the organization/movement? Who makes decisions about the criminal enterprise? What is its size? Does it have a fixed base of operations? What are the characteristics of organization/movement? What are the financial foundation and the different sources of income? Any type of criminal enterprise has structure, infrastructure, and decision makers, and understanding these factors can have a significant influence on determining the capability of the criminal entity.
- ◆ **In terrorism and criminal extremism, understanding the effect of contagion.** Contagion is often referred to as a copycat in popular media; however, the term “copycat” does not adequately describe the phenomenon. Lone wolves often are self-radicalized, which does not mean they are radicalized in isolation. For example, they consume ideological statements and ideas, typically online, from individuals who are themselves radicalized and are urging others to not only embrace the ideology but also act on it. We have seen lone wolves commit

788 This scale is not intended to be a threat assessment tool but an illustration of the threat assessment concept in the discussion.

789 <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/illicit-trafficking-in-cultural-goods-including-antiquities-and-works-of-art>

790 [http://www.wunrn.org/news/2010/11\\_10/11\\_01\\_10/110110\\_canada.htm](http://www.wunrn.org/news/2010/11_10/11_01_10/110110_canada.htm)

791 <https://www.dea.gov/press-releases/2018/11/02/dea-releases-2018-national-drug-threat-assessment-0>

792 <https://www.nasponline.org/resources-and-publications/resources-and-podcasts/school-climate-safety-and-crisis/systems-level-prevention/threat-assessment-at-school/threat-assessment-for-school-administrators-and-crisis-teams>

793 <https://www.rand.org/topics/terrorism-threat-assessment.html>

794 <https://www.secretservice.gov/protection/ntac/research/>

ISIS-inspired attacks, meaning they were committing the attacks based on the inspiration of the ISIS ideology. Much like a cold is a contagion that can be spread to other people under the right conditions, so can an extremist ideology. The contagion—and inspiration—can come from other sources as well. The attacks on the mosques in Christchurch, New Zealand,<sup>795</sup> have likely served as a contagion to other white nationalists because of (1) the bravado shown by the attacker; (2) the use of the live Facebook stream of the attack; and (3) his belief system and rationale based on his written manifesto.<sup>796</sup> Each of these factors can serve as a contagion to other white nationalist believers to commit an attack<sup>797</sup>—the contagion pushes their commitment to act farther. Hence, understanding the effect of contagion can aid in assessing threats—including potential lone wolves—who may be on a law enforcement watchlist.

- ◆ **Understanding the threatening entity’s motives, methods, and targets.** These factors are important for understanding the modus operandi of the group or individual(s) posing the threat. For example, criminal extremists are driven by their ideology or belief system. Understanding their ideology will identify potential targets and, in some cases, methods, such as when synagogues have been targets of white nationalists.<sup>798</sup> A criminal hacker group may focus on stealing consumer credit card information from a company,<sup>799</sup> may focus on making ransomware<sup>800</sup> attacks, or may be composed of “hacktivists”<sup>801</sup> who seek to bring about culture or social change through the hacking of computer systems. Drug trafficking organizations<sup>802</sup> (DTOs) seek to make as much money as possible; however, they have complex logistics to include product processing, transportation, smuggling, money laundering, and other aspects of managing their organizations. Hence their motive is income, their methods are various logistics, and their targets include not only the end users of the drugs but also all levels of the supply chain. It is human to be consistent in one’s plan—if a trafficking supply chain works, it probably will not be changed until necessary. The more that can be learned about the motives, methods, and targets, the greater the ability to forecast criminal events aimed at intelligence targets.
- ◆ **Identifying sources of information to learn more about the current status of the threatening entity.** Based on what is learned about the criminal entity and its modus operandi, sources of information can be identified to collect more information for analysis. Relying on law enforcement and intelligence databases tends to help lay the foundation for information collection, but examining the full array of additional sources—social media, open source searches, confidential informants, previous victims, community members, physical surveillance, surveillance by drones, fixed surveillance and security cameras, cell phone towers, trap and trace of phone calls, cell site simulators, wiretaps, license plate readers, and virtually any other lawful source or method of collecting and validating information—helps build a reliable analysis to assess a threat. In some cases, deep Web sources and darknet searches can also provide useful information.<sup>803</sup>
- ◆ **Determine whether the threatening entity has collaborators.** If so, who are they? What is the purpose of the collaboration? For example, human traffickers may collaborate with smugglers, drug traffickers may collaborate with money launderers, or gangs may collaborate with people in the illicit firearms trade. Typically, collaborators not only have information related to the threatened criminal event; they are often

---

795 <https://www.nytimes.com/spotlight/christchurch-attack-new-zealand>

796 <https://www.theatlantic.com/technology/archive/2019/03/the-shooters-manifesto-was-designed-to-troll/585058/>

797 Indeed, roughly five months after the Christchurch attack, another white nationalist committed a mass-violence attack in El Paso, Texas, and, in his own online manifesto, stated, “I support the Christchurch shooter and his manifesto.” <https://thefederalistpapers.org/opinion/el-paso-shooters-entire-purported-manifesto>

798 <https://www.nbcnews.com/tech/tech-news/synagogue-shooting-unfolded-extremists-congregated-facebook-page-connected-gunman-n999856>

799 <https://smallbusiness.chron.com/hackers-card-number-64333.html>

800 <https://www.us-cert.gov/Ransomware>

801 <https://www.uscybersecurity.net/hacktivist/>

802 <https://www.justice.gov/archive/ndic/pubs38/38661/dtos.htm>

803 For more information and distinctions between the deep Web and darknet, see <https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/>.

critical for the threat to be fulfilled. Learning about collaborators, their operations, and their organizations can not only help focus on the character and viability of the threat but also may be important for preventing the threat.

- ◆ **Research a brief history of the movement/criminal entity and past crimes/activities.** Even with shifts in ideology, changing illicit commodities, and/or methods in the evolution of criminal enterprises (such as increased reliance on technology), there is likely to be some consistency in patterns, processes, and collaborators. Moreover, history provides context—and is often repeated. For example, a criminal enterprise trafficking in illegal weapons typically has some consistency in its suppliers, buyers, and smuggling methods. While in the past, individuals involved in such an enterprise may have communicated in code over a telephone, today they may communicate using encryption options on an app such as Telegram.<sup>804</sup> The weapons and accessories they supply may change, such as adding bump stocks, high-capacity magazines, and suppressors where these items are outlawed. So while communications and commodities change, the processes and people are likely to have similarities—that is the value of history.
- ◆ **Clearly articulate the evidence and justification/rationale** for:
  - The type of threat that is posed.
  - The forecast of activities of criminal offenders and collaborators.
  - Observations to inform police management for police staffing and resource reallocation to address the threat.
  - Information that should be disseminated to investigators and patrol officers about the threat.

To meet civil rights requirements, justify agency investment of resources to address a criminal event, develop tactics and strategies to intervene and respond to a criminal threat, and reinforce validity of a threat analysis, the threat assessment needs to not only state what the proposed threat is but also the *logic/rationale/evidence* on which that conclusion is based. For example, after a series of fights and drive-by shootings, a gang threat assessment shows that gang members are stockpiling weapons and ammunition in preparation for a violent confrontation to show which gang is dominant. The likely location of the gang war is a populated urban center, increasing the likelihood of innocent victims in the crossfire. The assessment hypothesizes that the confrontation will occur within a 20-day window. To reallocate police resources for a 20-day period, police management officers will want the rationale and evidence not only to support their decision but to also determine which police resources and tactics need to be devoted to prevent the gang war from occurring and defusing tensions between the two gangs. The stronger the justification and rationale, the more robust the assessment. If there is confidence in the assessment, support for the response by an agency will be stronger, as will the legal foundation for operations.

## RESEARCH AND THE SCIENTIFIC METHOD

A threat assessment is essentially a research project employing a mixed-methods<sup>805</sup> approach using both qualitative and quantitative data that relies on the scientific method.<sup>806</sup> Data and information are collected; assessed for quality, validity, and reliability; and analyzed on an ongoing basis—largely based on the incoming information stream—to develop hypotheses about the criminal event. Standard and accepted research methods apply with the added component of ensuring the information being used has been lawfully obtained. Applying standard social science research methods to the threat at hand, which includes designing the methodology to meet the facts and

---

804 <https://telegram.org/>

805 [https://cirt.gcu.edu/research/developmentresources/research\\_ready/mixed\\_methods/overview](https://cirt.gcu.edu/research/developmentresources/research_ready/mixed_methods/overview)

806 <https://plato.stanford.edu/entries/scientific-method/>

circumstances of the threat, is the best approach to take. A solid research methods text that addresses quantitative, qualitative, and mixed methods approaches should be a resource on every analyst's bookshelf.<sup>807</sup>

A key difference in threat assessment methods is that analysts are not experimenting to test a theoretical hypothesis; rather, the analysts are doing applied policy research. This type of research is largely parallel with evidence-based methods<sup>808</sup> that translate research into practice. While the goals are different, the methods are guided by the same principles of the scientific method.

As a result, using the scientific method an analyst will develop detailed knowledge about a subject area such as a criminal extremist group—e.g., white nationalists; criminal methods—e.g., lone wolves, human traffickers; and/or commodities—e.g., illicit drugs, illegal firearms; to understand the dynamics of that entity. This will often involve performing *creative* information/data collection, including verifying the validity and reliability of the information and corroborating the information. Then, these diverse pieces of information are integrated to provide a comprehensive, meaningful, seamless, and practical vision of the criminal threat at hand to inform others who may have only limited, or no, understanding of the problem. Collectively, all of this information, including evidence, linkages, and processes, will be detailed in a comprehensive threat assessment report.

Weaknesses in the assessment also need to be clearly stated and explained. Consumers of intelligence need to see the complete threat picture clearly to make informed decisions. Sometimes an analyst, investigator, or decision maker will have an intuitive feeling of a threat based on the collective weight of circumstantial evidence and personal experience. It is important, however, to ensure a focus on validated information and evidence—intuition is often fallible. Experience should not be completely discounted; however, intuitive conclusions must be balanced against known facts.

For all of these reasons, analysts need not only good research skills but also good writing and communication skills to maximize the utility of the threat assessment report.

## CRITICAL THINKING

There is a tendency for humans to follow the same path of thought when addressing a problem. That path is determined not only by one's own life experiences but also through one's workplace practices and associations. It is further reinforced by others agreeing with the thought process and relying on traditional approaches to problems. This is akin to "groupthink:"

Groupthink occurs when a group of well-intentioned people make irrational or non-optimal decisions that are spurred by the urge to conform or the discouragement of dissent. This problematic or premature consensus may be fueled by a particular agenda or simply because group members value harmony and coherence above rational thinking. In a groupthink situation, group members refrain from expressing doubts and judgments or disagreeing with the consensus.<sup>809</sup>

Going against tradition and common practice is socially uncomfortable, potentially exposing a person to criticism or simply dismissal of his or her perspective. Hence it is sometimes easier to agree with the majority. Groupthink does not necessarily produce "wrong" solutions to problems, but it rarely produces the best solutions. It is not uncommon to encounter this phenomenon in any organization, including an intelligence unit. The result may mean a less-robust threat assessment that may not as precisely identify the threat, the actors, or the target. To avoid groupthink, we encourage our analysts to develop and apply *critical thinking* skills.

807 There are many good research methods books available. A popular one that address all of these methods is Creswell, J. W., and Creswell, J. D. (2019). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 4th ed. Thousand Oaks, CA: Sage Publications.

808 <https://cebcp.org/evidence-based-policing/>

809 <https://www.psychologytoday.com/us/basics/groupthink>

Critical thinking is that mode of thinking—about any subject, content, or problem—in which the thinker improves the quality of his or her thinking by skillfully analyzing, assessing, and reconstructing it. Critical thinking is self-directed, self-disciplined, self-monitored, and self-corrective thinking. It presupposes assent to rigorous standards of excellence and mindful command of their use. It entails effective communication and problem-solving abilities, as well as a commitment to overcome our native egocentrism and sociocentrism.<sup>810</sup>

Critical thinking is important for all intelligence analysis and is particularly important for a threat assessment. The need to step beyond traditional sources and analytic methods and look at a criminal threat from a different paradigm is part of the critical thinking process. This is particularly true when dealing with complex threat problems such as the unpredictability of lone wolves or the multiplicity of issues involving threats to computer networks and critical infrastructure.

Often, critical thinking can be enhanced by talking through the issues and problems with persons of different expertise or experience. Examples include speaking with an auto theft investigator if stolen cars are being used in a criminal enterprise; speaking to a forensic analyst at the crime laboratory if changes are seen in seized illicit drugs; speaking with a psychologist about group behavior in a gang assessment; or speaking with a forensic accountant to understand a money laundering network. Speak to analysts from other jurisdictions about different approaches to information collection and analysis on a particular case/problem. Not only can valuable substantive knowledge be gained by this approach, it can stimulate one's own critical thinking. The challenge to the analyst is to push the boundaries of critical thought—the results can prove valuable to law enforcement and be personally rewarding.

## INTELLIGENCE PRODUCTS

The output of analysis—i.e., intelligence—must be placed in a reporting format that maximizes the consumption and use of the information. This is referred to as the intelligence product. In describing the relationship of analysis to products, Radcliffe observed:

. . .criminal intelligence is the creation of an intelligence knowledge product that supports decision making in the areas of law enforcement, crime reduction and crime prevention. In this context, an intelligence knowledge product is a product that can influence the thinking of a decision maker. It is the result of a criminal intelligence analysis and could be a written bulletin, a presentation, a verbal report or some combination of these in a briefing. An intelligence knowledge product could even be a brief telephone conversation if the intelligence is timely and has an effect on the decision making of the recipient of the intelligence.<sup>811</sup>

Typically, different types of products are developed to meet the needs of different consumers and different types of analysis. A tactical analytic product will differ from a strategic analytic product. The product developed for a comprehensive threat assessment of a targeted criminal enterprise will differ from a product intended to make officers aware of criminal indicators. An executive briefing of a criminal threat will differ from a patrol briefing of a criminal threat. Regardless of the type of product, all should contain five fundamental elements in the context of the product's intent:

1. Identify the targeted consumer of the information (patrol officers, administrators, private sector, others).
2. Convey the critical information clearly needed by the intended consumer.
3. Identify time parameters wherein the intelligence is actionable.

---

<sup>810</sup> <https://www.criticalthinking.org/pages/our-conception-of-critical-thinking/411>

<sup>811</sup> Radcliffe, J. H. (2007). *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice, p. 8.

4. Define additional intelligence requirements, if needed.
5. Provide operational recommendations in light of the analysis.

Ideally, products are a series of regularly produced intelligence reports that have a specific format and type of message to convey. A product is most useful when it has a specific purpose; is in a consistent, clear, and aesthetic format; and contains all critical information the consumer needs with no superfluous information. As a general rule, at least three types of products should be developed by an intelligence unit or a fusion center to provide situational awareness:<sup>812</sup>

- ◆ Products directed toward the prevention of known threats
- ◆ Products that provide threat advisories identifying indicators of threatening behaviors and threatened targets
- ◆ Products that describe changes in the terrorist or criminal threat picture as it applies to a jurisdiction

While most law enforcement officers are very familiar with investigative reports and records, they are less familiar with intelligence products. As indicated in Table 11-1, there are notable differences that are important for the consumer to understand. With a clear understanding of the distinction, there will be greater use of the products.

There are two broad distinctions in law enforcement intelligence outputs characterized in Table 11-2. The first type is case intelligence, sometimes also referred to as investigative intelligence. A critical characteristic of case intelligence is that it identifies individuals or organizations. Conceptually, its ultimate goal is arrest and prosecution of particularly described persons as a means to prevent a threat from reaching fruition.<sup>813</sup> It is important to note that with case intelligence, civil rights attach to individuals who have been identified in any type of intelligence report. The second type, intelligence advisory products, describes (i.e., “advises”) general indicators of crime and threats for which officers must be aware. The goal is for law enforcement personnel to be aware of the indicators and, if these are observed, take appropriate action to ensure public safety and prevent a criminal incident from occurring. In general, there are no explicit civil rights issues<sup>814</sup> of advisory products until a person or an organization is identified as related to the criminal indicators.

TABLE 11-1: DIFFERENCES BETWEEN INVESTIGATIONS AND INTELLIGENCE REPORTS

CRIMINAL INVESTIGATION REPORTS AND RECORDS	LAW ENFORCEMENT INTELLIGENCE REPORTS, RECORDS, AND PRODUCTS
◆ Primary goal is prosecution	◆ Primary goal is threat-based prevention
◆ Report is documentation of a criminal incident that occurred	◆ Report focuses on suspected criminal threats
◆ Report is an official record and is evidentiary	◆ Report documents information associated with a threat inquiry
◆ Motive is irrelevant as a legal element of the crime	◆ Motive is an important tool for forecasting
◆ Evidence is documented to prove the <i>corpus delicti</i>	◆ Information is documented to build hypotheses about criminal threats

812 Situational awareness is broadly defined as the description of the threat environment, events, and/or people with regard to time and geography and the status of a potential threat.

813 It should be remembered that the only authority for law enforcement agencies to be in the “intelligence business” is based on their statutory authority to enforce the criminal law. Hence, development of a criminal case is a sound model to follow.

814 Specifically, when no person is identified in an intelligence product, no civil rights issues attach. However, civil libertarians will argue that descriptions of classes of persons—for example, African-American or Muslim—in an intelligence product, without personally identifiable information, hold the potential for racial profiling. Analysts should be aware of this factor when preparing intelligence products.

TABLE 11-2: CASE/INVESTIGATIVE INTELLIGENCE VERSUS INTELLIGENCE PRODUCTS

CASE/INVESTIGATIVE INTELLIGENCE	INTELLIGENCE ADVISORY PRODUCTS
<ul style="list-style-type: none"> <li>◆ Individuals are identified</li> <li>◆ Specific offenses are identified</li> <li>◆ Intelligence develops evidence of criminal liability</li> <li>◆ The goal is to develop a criminal case for prosecution</li> </ul>	<ul style="list-style-type: none"> <li>◆ Trends in crime and/or their methodologies are identified</li> <li>◆ A change in criminal trends is forecast</li> <li>◆ Indicators of the new crime types are identified for awareness by law enforcement personnel</li> <li>◆ The goal is prevention of the crime</li> </ul>

Any intelligence unit or fusion center can determine the type of products it needs to develop based on the administrative mandate of the unit. Some are designed to meet unique jurisdictional needs, such as the High Intensity Drug Trafficking Area intelligence centers focusing on illicit drugs. In general, law enforcement intelligence reports may be in a typology with two broad components: (1) the nature of the report and (2) the nature of the analysis.

**Nature of the intelligence product.** Different types of intelligence products are created to meet the needs of specific audiences. For example, an “intelligence alert” may be a short report giving the basic facts about indicators or persons related to a threat that is time-critical. An “intelligence bulletin” may provide more detailed information about indicators or threats that are not imminent but which personnel may encounter. An “intelligence assessment” typically provides an historical perspective of a threat and how the current status of the threat has changed. At this point, there are no uniform classifications of intelligence products across all agency types and levels of government; rather, each agency or fusion center produces products that tend to meet these general guidelines. Law enforcement personnel should receive training on the types of products that are used in their jurisdictions and the intent of each report type.

**Nature of the analysis.** Perhaps adding confusion to the universe of intelligence reporting is that some terminology has different meaning to the intelligence community, the military, and federal law enforcement when compared with state, local, and tribal law enforcement. The current discussion is directed toward the latter. Previously, the differences between tactical and strategic analysis were described from the law enforcement perspective. Again, while there are no uniform categories of specific report types based on the type of analysis performed, intelligence consumers should be aware that some report outputs will describe threats in need of an operational response (tactical) while other reports will describe changes in the threat picture (strategic).

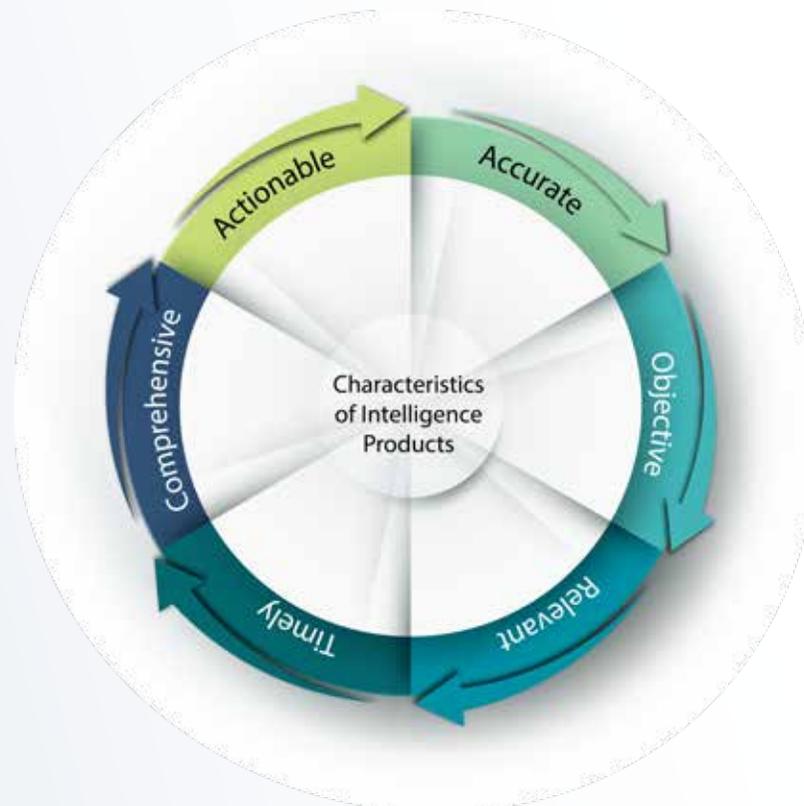
Other product types exist or will emerge. Intelligence briefings are oral summaries of analyses that require yet a different approach to reporting that pays homage to the often-repeated comment of Sergeant Joe Friday in the old television series *Dragnet*: “I want the facts, just the facts.” We are increasingly seeing new report types emerging based on technology, ranging from text messaging to podcasts. Regardless of the method of reporting, it is essential that each product type contain the information that the intended consumer needs to be effective in fulfilling his or her responsibilities.

As illustrated in Figure 11-3, regardless of the type of product, each will ideally reflect six core characteristics. Intelligence products should be:

- ◆ **Actionable**—The product should provide sufficiently definitive information that some type of operational activity or response may be developed from the intelligence.
- ◆ **Accurate**—The nature of the analytic process is often probabilistic; hence concrete conclusions and forecasts can rarely be made. Despite this, every effort should be made to be as accurate as possible, with weaknesses in the conclusions clearly documented.

- ◆ **Objective**—Intelligence products should be free of bias. All information should be provided in a balanced manner, clearly articulating knowns and unknowns as well as strengths and weaknesses in the analysis.
- ◆ **Relevant**—The analysis, hence the products, should focus on threats that are part of the strategic priorities and/or emerging threats that could have a significant effect on public safety in the region.
- ◆ **Timely**—Timeliness has two components. First, the intelligence product should be of a threat that is of current concern. Second, when practicable, the product should be made available to maximize the time permitted for operational units to develop a response and put it in place.
- ◆ **Comprehensive**—The intelligence product should provide as much information as possible about all dimensions of the threat.

FIGURE 11-3: CHARACTERISTICS OF INTELLIGENCE PRODUCTS



## PRACTICES TO AVOID WITH INTELLIGENCE PRODUCTS

In the post-9/11 environment with an emphasis on information sharing, some practices related to intelligence products have created more problems than solutions. Information should be targeted—that is, *useful information needs to be shared with people who can use it*. Unfortunately, this axiom has gone unheeded too frequently.

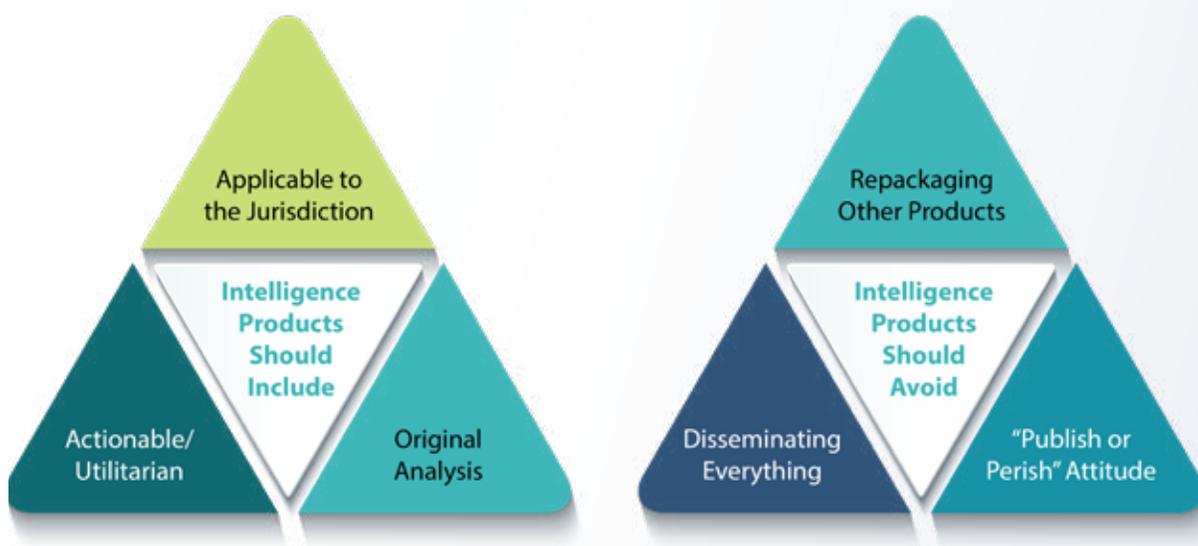
Three fundamental practices have evolved as related to analysis and intelligence products; they should be avoided. These practices might be expressed as the “three don’ts of information sharing”:

1. **Don’t repackage the intelligence products of another organization.** Most agencies will have received the original product; hence the practice is duplicative and can be confusing. A repackaged product adds little value and may have a misleading effect if the same information is distributed as the product of two different agencies. Finally, if another agency’s product is simply repackaged, the agency will not be able to provide any follow-up detail should inquiries be made.
2. **Don’t disseminate everything to everybody.** Receiving too much information can be just as ineffective as receiving no information. If personnel are inundated with a cascade of information that has little value to

them, they tend to pay little attention to any information. The intelligence function, not the consumer, must separate the wheat from the chaff. Targeted dissemination of information to people who need it is critical.

3. **Don't develop a "publish-or-perish" attitude.** This can become a systemic problem. Managers want to see productivity by intelligence analysts; however, productivity is difficult to quantify in the intelligence function. One activity that can be easily counted is the number of intelligence products published. Hence, some intelligence units and fusion centers have used products as a measure of effectiveness. While it is understandable how this has evolved, the publication of products alone is not a measure of success. Even if a product is interesting, it provides little value unless it is actionable. It is not the quantity of products that should be measured, but the quality and utility of the products. Of course, this process is difficult and somewhat subjective. Evaluation is often difficult to perform effectively.

FIGURE 11-4: ATTRIBUTES OF INTELLIGENCE PRODUCTS



To avoid the problems embodied in the "don'ts of intelligence products," those responsible for the intelligence function should answer the following questions affirmatively:

1. **Tactical and Operational Intelligence:** Does the intelligence product provide sufficient detail about a threat within your region or service area so that operational personnel can develop tactical plans or activities to prevent or mitigate an identified threat?
2. **Strategic Intelligence:** Does the intelligence product describe the characteristics, modus operandi, or change in the threat picture in sufficient detail as related to your region or service area so that effective decisions can be made about strategic priorities and resource allocation?
3. **Actionable Dissemination:** In light of the nature of the threat and content of the intelligence product, who within your region or service area has the right to know and need to know this information for threat prevention, mitigation, and/or planning?

## THREAT ASSESSMENT PRODUCTS

Threat assessment products are comprehensive reports designed to communicate necessary information for decision making and awareness to a family of defined consumers. Consumers of the product will vary depending on the threat and targets or commodities. For example, a trafficking threat of high-value arts and antiquities stolen in Egypt and heading for sale to a local U.S. underground market is important for organized crime investigators, but drug and gang investigators would not be consumers of this intelligence.

Basic principles that reflect good practice apply to all intelligence products, not just threat assessments. The intent of the principles is to ensure an accurate, effective product that is consistent with civil rights guarantees and provides actionable intelligence to prevent or mitigate criminal threats, including the apprehension of criminal actors.

1. **An evidence-based criminal nexus must be established before individuals or organizations can be identified in an intelligence product.** Law enforcement intelligence products are intended to provide information about criminal threats to consumers; therefore, a criminal predicate must be established before disseminating a product that identifies an individual or an organization.
2. **Lawful actions of individuals exercising First Amendment expressive activity, even if unpopular or controversial, must not be the subjects of intelligence products.** The law enforcement intelligence function is designed to prevent criminal threats. It is inappropriate for a law enforcement intelligence entity to document constitutionally protected lawful behaviors even if controversial or offensive.
3. **All personnel developing and reviewing intelligence products have an obligation to ensure that facts and information contained in the product are accurate and supported by source reliability and information validity.** Accuracy is important both for protecting civil liberties and for ensuring that the analysis of criminal threats is as precise as possible. Inaccuracy threatens privacy, diminishes quality, and wastes resources.
4. **Intelligence products should be based on facts, interpretations, and conclusions that are objective and relevant. Intelligence products should be free of bias.** Information in the product must be based on known behaviors, not on assumptions associated with race, ethnicity, religion, or beliefs of persons who are the subjects of an intelligence inquiry. All information should be provided in a balanced manner, clearly articulating knowns and unknowns as well as strengths and weaknesses in the analysis.
5. **Law enforcement intelligence products must not include political statements or personal opinions.** Most people have political opinions about various issues—some are stronger than others. Care must be taken to not incorporate any type of political or personal view to influence the assessment or content of the products.
6. **The conclusions and indicators contained in intelligence products must be logical and consistent with known evidence, not tainted by supposition or unsupported conclusions.** Intuition, supposition, and personal beliefs of intelligence personnel can easily influence the narrative of an intelligence product. Care must be taken to ensure that all statements and conclusions are based on known evidence and rely on scientific principles of logic.
7. **Intelligence products should provide sufficient detail of information to be actionable.** The products should provide sufficiently definitive information that some kind of operational activity or response may be developed from the intelligence.
8. **Intelligence products should be comprehensive to ensure that the consumer is fully informed about the totality of circumstances surrounding the information in the products.** Indicators and evidence of threats cannot be viewed in isolation but must be presented in such a way that the consumer can see how all of the pieces of information fit into the puzzle that constitutes a threat. The product should clearly articulate the need for the consumer to view the information in light of the totality of the circumstances.
9. **The information in the intelligence product must be timely and relevant to a current or emerging threat.** The intelligence product should be of a threat that is of current concern and, when practicable, the product should be made available to maximize the time permitted for operational units to develop a response and put it in place.
10. **The intended group of consumers of the intelligence product should be clearly articulated to ensure that the dissemination restriction is appropriately identified.** An intelligence product that is intended for dissemination to non-law enforcement personnel must be reviewed for greater sensitivity to ensure that

privacy requirements are met. Both the developer and the reviewing official must be cognizant of the intended consumers to meet right-to-know and need-to-know conditions.

11. **The content of the intelligence product must be reviewed and approved by a supervisor.** Every intelligence product must be reviewed and approved by at least one supervisor before being disseminated. The reviewing supervisor must ensure that all of the conditions described above are met.

Unfortunately, we have seen instances in which intelligence products were not written sufficiently clear or contained information that was inappropriate for an intelligence report. While intelligence products are typically labelled “For Official Use Only,” it should always be assumed that a product will become publicly available. In those cases in which there is a political or unclear statement in the document, it can cause problems. For example, one particular intelligence product that was leaked on the Internet stated that the Gadsden flag<sup>815</sup> is a symbol of white supremacy. While the flag has been displayed by the extreme right, it is a symbol of American history displayed by many people. The controversy following this release ended up costing some people their jobs because the statement, as written,<sup>816</sup> was unclear and was not caught by supervisors before the report was disseminated. Following the principles described above will help prevent future incidents such as this.

## THE THREAT ASSESSMENT BRIEFING

No one knows more about a threat than the analyst who performed the assessment. That critical knowledge needs to be shared, which often includes a summary of critical facts for law enforcement leaders and commanders in the form of a briefing. As implied by the name, a briefing is a concise oral presentation of critical facts and evidence that support the threat assessment findings as well as the likely impact of the threat and potential interventions. The use of visual aids—for example, photographs, maps, graphics, link charts—can significantly enhance the quality of the briefing; however, ensure that all such visual aids make a substantive contribution to the message of the briefing and are not simply items of interest. Experience has provided some guidelines to help make briefings more successful:

- ◆ **Tailor the briefing to the audience.** Executives will need different information than investigators. Know your audience, and be sure to include the types of information the audience needs.
- ◆ **Critical elements about the threat should be clearly and concisely stated at the beginning.** A briefing is not a story building to a climax. The threat information—to include targets, methods, actors, timing, impact, etc.—should be stated early in the briefing.
- ◆ **Provide key rationale and evidence to support the findings.** While not everything developed in the analysis needs to be presented in the briefing, provide sufficient information/evidence/logic to inform the audience.
- ◆ **Be thorough but concise.** Long explanations and side notes typically are not needed in a briefing. Provide the key information succinctly.
- ◆ **Try to anticipate questions.** Typically, there will be questions about the threat. It will be more efficient to address the obvious ones during the briefing presentation.
- ◆ **Be aware of the limitations to the threat assessment.** Decision makers and investigators need to know areas of uncertainty and information or evidentiary voids in the threat assessment.
- ◆ **Be prepared to answer questions and provide evidence and the rationale for all conclusions that are drawn.** There will always be some persons in the briefing who agree with your logic and others who will be skeptical. The key is to provide all the information available in response to questions. Do not try to win over skeptics; rather, inform them of the assessment’s findings.

---

815 A historical flag designed in 1775 with a yellow background depicting a coiled rattlesnake ready to strike. The words below the snake read, “Don’t tread on me.”

816 It should have stated that the Gadsden flag was one of many factors and should not be considered an indicator of white supremacy in itself. Providing detail and context is important in a report.

## CONCLUSIONS

A comprehensive threat assessment is difficult. The raw information is often difficult to obtain; the analysis is difficult to perform, and fully explaining the entire assessment in a consumable intelligence product is difficult. However, that difficulty can be significantly reduced by understanding the goals of the assessment, the methods to be used, and the expected outputs. Like most things in life, with experience not only does the process become easier, but the assessments are typically better. The threat assessment is a valuable tool for community safety as well as for investigators and decision makers.

Intelligence products are means by which critical threat information reaches the street. Developing the types of products of greatest use to an intelligence unit or a fusion center's consumers and placing the right product in the hands of the people who need it are critical processes.

# CHAPTER ANNEX 11-1: THREAT ASSESSMENT INFORMATION COLLECTION TEMPLATE

THE FOLLOWING TEMPLATE WAS DESIGNED TO COLLECT INFORMATION FROM A PERSON REPORTING A THREAT OF TARGETED VIOLENCE IN SCHOOLS. WITH MINOR AMENDMENT, IT HAS A BROADER APPLICATION—IT SERVES AS AN ILLUSTRATION OF CRITICAL INFORMATION NEEDED TO BEGIN THE THREAT ASSESSMENT PROCESS BASED ON A REPORT.

## THREAT ASSESSMENT TEMPLATE

This document should be used as a starting point for areas to consider during threat assessment. This should not limit other sources of information that may be invaluable in assessing a threat.

Date: \_\_\_\_\_ Person Reporting Threat: \_\_\_\_\_

Date of Threat: \_\_\_\_\_ Time: \_\_\_\_\_

Intended Targets/Victims: \_\_\_\_\_

Exact wording and nature of the threat:

### STEP ONE: TYPES OF THREATS

(Is this a threat?) Keep in mind the following types of threats:

**Direct Threat:** Identifies a specific act against a specific target and is delivered in a straightforward, clear, and explicit manner: “I am going to place a bomb in the school’s gym.”

**Indirect Threat:** Tends to be vague, unclear, or ambiguous. The plan, the intended victim, the motivation, and other aspects of the threat are masked or equivocal: “If I wanted to, I could kill everyone at this school.” Violence is implied but tentatively (“if I wanted to”) and suggests that a violent act COULD occur, not that it WILL occur.

**Veiled Threat:** Strongly implies but does not explicitly threaten violence. “We would be better off without you around anymore” clearly hints at a possible violent act but leaves it to the potential victim to interpret the message and give a definite meaning.

**Conditional Threat:** Warns that a violent act will happen unless certain demands or terms are met: “If you don’t pay me one million dollars, I will place a bomb in the school,”

### STEP TWO: LEVELS OF THREATS

This step could be used alone if the threatener is not known.

#### PRESUMPTIVE INDICATORS

##### LOW LEVEL

- ◆ Threat is vague and indirect
- ◆ Information within the threat is inconsistent or implausible or lacks detail
- ◆ Threat lacks realism
- ◆ Content suggests person is unlikely to carry it out

##### MEDIUM LEVEL

- ◆ Threat is more direct and more concrete than a low-level threat
- ◆ Wording suggests threatener has given some thought to how the act will be carried out

- ◆ General indication of a possible place and time (but not a detailed plan)
- ◆ Strong indication that the threatener has taken preparatory steps, although there may be some veiled reference or ambiguous or inconclusive evidence pointing to that possibility—an allusion to a book or movie that shows the planning of a violent act or a vague, general statement about the availability of weapons.
- ◆ Specific statement seeking to convey that the threat is not empty: “I’m serious!” or “I really mean this!”

#### HIGH LEVEL

- ◆ Direct, specific, and plausible
- ◆ Threat suggests that concrete steps have been taken toward carrying it out; for example, statements indicating that the threatener has acquired or practiced with a weapon or has had the victim under surveillance.
- ◆ “At 8 a.m. tomorrow morning, I intend to shoot the principal. That’s when he is in his office by himself. I have a 9mm. Believe me, I know what I am doing. I am sick and tired of the way he runs this school.”

## STEP THREE: FOUR-PRONGED ASSESSMENT

### PRONG ONE: PERSONALITY TRAITS AND BEHAVIOR (CHECK ALL THAT APPLY)

- Leakage:** Intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act. These clues can be subtle threats, boasts, innuendos, predictions, or ultimatums. They may be spoken or conveyed in stories, diary entries, essays, poems, letters, songs, drawings, doodles, tattoos, or videos (maybe a rap song on a CD). Students may ask other students to help them prepare for a violent act, maybe even through deception (asking a friend to buy ammunition for them because they are going hunting). See examples attached.
- Low tolerance for frustration:** The student is easily bruised, insulted, angered, and hurt by real or perceived injustices done to him by others and has great difficulty tolerating frustration.
- Poor coping skills:** The student consistently shows little if any ability to deal with frustration, criticism, disappointment, failure, rejection, or humiliation. His or her response is typically inappropriate, exaggerated, immature, or disproportionate.
- Lack of resiliency:** The student lacks resiliency and is unable to bounce back even when some time has elapsed since a frustrating or disappointing experience, a setback, or a putdown.
- Failed love relationship:** The student may feel rejected or humiliated after the end of a love relationship and cannot accept or come to terms with the rejection.
- “Injustice collector”:** The student nurses resentment over real or perceived injustices. No matter how much time has passed, the “injustice collector” will not forget or forgive those wrongs or the people he or she believes are responsible. The student may keep a “hit list” with the names of the people he feels have wronged him.
- Signs of depression:** The student shows features of depression such as lethargy, physical fatigue, a morose or dark outlook on life, a sense of malaise, and a loss of interest in activities that he or she once enjoyed. May show unpredictable and uncontrolled outbursts of anger, a generalized and excessive hatred toward everyone else, and feelings of hopelessness about the future. Restlessness, inattention, sleep and eating disorders, markedly diminished interest in everything that previously occupied and interested him or her.
- Narcissism:** The student is self-centered, lacks insight into others’ needs and/or feelings, and blames others for failures and disappointments. The narcissistic student may embrace the role of victim to elicit sympathy and to feel temporarily superior to others. He or she displays signs of paranoia and assumes an attitude of self-importance or grandiosity that masks feelings of unworthiness (Malmquist, 1996). A narcissistic student may be either very thin-skinned or very thick skinned in responding to criticism.
- Alienation:** The student consistently behaves as though he or she feels different or estranged from others. This sense of separateness is more than just being a loner. It can involve feelings of isolation, sadness, loneliness, not belonging, and not fitting in.

- ✓ **Dehumanizes others:** The student consistently fails to see others as fellow humans. He or she characteristically views other people as “nonpersons” or objects to be thwarted. This attitude may appear in the student’s writings and artwork, in interactions with others, or in comments during conversation.
- ✓ **Lack of empathy:** The student shows an inability to understand the feelings of others and appears unconcerned about anyone else’s feelings. When others show emotion, the student may ridicule them as being weak or stupid.
- ✓ **Exaggerated sense of entitlement:** The student constantly expects special treatment and consideration and reacts negatively if he or she does not get the treatment to which he or she feels entitled.
- ✓ **Attitude of superiority:** The student has a sense of being superior and presents him- or herself as smarter, more creative, more talented, more experienced, and more worldly than others.
- ✓ **Exaggerated or pathological need for attention:** The student shows an exaggerated, even pathological, need for attention, whether positive or negative, no matter what the circumstances.
- ✓ **Externalizes blame:** The student consistently refuses to take responsibility for his or her own actions and typically faults other people, events, or situations for any failings or shortcomings. In placing blame, the student frequently seems impervious to rational argument and common sense.
- ✓ **Masks low self-esteem:** Though the student may display an arrogant, self-glorifying attitude, his or her conduct often appears to veil an underlying low self-esteem. The student avoids high visibility or involvement in school activities, and other students may consider him or her a nonentity.
- ✓ **Anger management problems:** Rather than expressing anger in appropriate ways and in appropriate circumstances, the student consistently tends to burst out in temper tantrums or melodramatic displays or to brood in sulky, seething silence. The anger may be noticeably out of proportion to the cause or be redirected toward people who had nothing to do with the original incident. The student’s anger may come in unpredictable and uncontrollable outbursts and may be accompanied by expressions of unfounded prejudice, dislike, or even hatred toward individuals or groups.
- ✓ **Intolerance:** The student often expresses racial or religious prejudice or intolerant attitudes toward minorities or displays slogans or symbols of intolerance in such things as tattoos, jewelry, clothing, bumper stickers, or book covers.
- ✓ **Inappropriate humor:** The student’s humor is consistently inappropriate. Jokes or humorous comments tend to be macabre, insulting, belittling, or mean.
- ✓ **Seeks to manipulate others:** The student consistently attempts to con and manipulate others and win their trust so they will rationalize any signs of aberrant or threatening behavior.
- ✓ **Lack of trust:** The student is untrusting and chronically suspicious of others’ motives and intentions. This lack of trust may approach a clinically paranoid state. The student may express the belief that society has no trustworthy institution or mechanism for achieving justice or resolving conflict and that things have to get settled in his or her own way.
- ✓ **Closed social group:** The student appears introverted, with acquaintances rather than friends, or associates only with a single small group that seems to exclude everyone else. Students who threaten or carry out violent acts are not necessarily loners in the classic sense, and the composition and qualities of peer groups can be important pieces of information in assessing the danger that a threat will be acted on.
- ✓ **Change of behavior:** The student’s behavior changes dramatically. His or her academic performance may decline, or the student may show a reckless disregard for school rules, schedules, dress codes, and other regulations.

- ☑ **Rigid and opinionated:** The student appears rigid, judgmental, and cynical and voices strong opinions on subjects about which he or she has little knowledge. The student disregards facts, logic, and reasoning that might challenge these opinions.
- ☑ **Unusual interest in sensational violence:** The student demonstrates an unusual interest in school shootings and other heavily publicized acts of violence. He or she may declare admiration for those who committed the acts or may criticize them for “incompetence” or failing to kill enough people. The student may explicitly express a desire to carry out a similar act in his or her own school, possibly as an act of “justice.”
- ☑ **Fascination with violence-filled entertainment:** The student demonstrates an unusual fascination with movies, TV shows, computer games, music videos, or printed material that focus intensively on themes of violence, hatred, control, power, death, and destruction. He or she may incessantly watch one movie or read and reread one book with violent content, perhaps involving school violence. Themes of hatred, violence, weapons, and mass destruction recur in virtually all of the student’s activities, hobbies, and pastimes. The student spends inordinate amounts of time playing video games with violent themes and seems more interested in the violent images than in the game itself. On the Internet, the student regularly searches for websites involving violence, weapons, and other disturbing subjects. There is evidence that the student has downloaded and kept material from these sites.
- ☑ **Negative role models:** The student may be drawn to negative, inappropriate role models such as Hitler, Satan, or others associated with violence and destruction.
- ☑ **Behavior appears relevant to carrying out a threat:** The student appears to be increasingly occupied in activities that could be related to carrying out a threat—for example, spending unusual amounts of time practicing with firearms or on various violent websites. The time spent in these activities has noticeably begun to exclude normal everyday pursuits such as homework, attending classes, going to work, and spending time with friends.

#### **PRONG TWO: FAMILY DYNAMICS**

- ☑ **Turbulent parent-child relationship:** The student’s relationship with his parents is particularly difficult or turbulent. This difficulty or turbulence can be uniquely evident following a variety of factors, including recent or multiple moves, loss of a parent, addition of a stepparent, etc. The student expresses contempt for his or her parents and dismisses or rejects their role in his or her life. There is evidence of violence occurring within the student’s home.
- ☑ **Acceptance of pathological behavior:** Parents do not react to behavior that most parents would find very disturbing or abnormal. They appear unable to recognize or acknowledge problems in their child and respond quite defensively to any real or perceived criticism of their child. If contacted by school officials or staff about the child’s troubling behavior, the parents appear unconcerned, minimize the problem, or reject the reports altogether, even if the child’s misconduct is obvious and significant.
- ☑ **Access to weapons:** The family keeps guns or other weapons or explosive materials in the home, accessible to the student. More important, weapons are treated carelessly, without normal safety precautions; for example, guns are not locked away and are left loaded. Parents or a significant role model may handle weapons casually or recklessly and, in doing so, may convey to children that a weapon can be a useful and normal means of intimidating someone else or settling a dispute.
- ☑ **Lack of intimacy:** The family appears to lack intimacy and closeness. The family has moved frequently and/or recently.
- ☑ **The student “rules the roost”:** The parents set few or no limits on the child’s conduct and regularly give in to his demands. The student insists on an inordinate degree of privacy, and parents have little information about his or her activities, school life, friends, or other relationships. The parents seem intimidated by their child. They may fear that the child will attack them physically if they confront or frustrate him or her, may be unwilling to face an emotional outburst, or may be afraid that upsetting the child will spark an emotional crisis. Traditional family

roles are reversed. For example, the child acts as if he or she were the authority figure, while parents act as if they were the children.

- ☑ **No limits or monitoring of TV and Internet:** Parents do not supervise, limit, or monitor the student's television watching or his or her use of the Internet. The student may have a TV in his or her own room or is otherwise free without any limits to spend as much time as desired watching violent or otherwise inappropriate shows. The student spends a great deal of time watching television rather than in activities with family or friends. Similarly, parents do not monitor computer use or Internet access. The student may know much more about computers than the parents do, and the computer may be considered off-limits to the parents while the student is secretive about his or her computer use, which may involve violent games or Internet research on violence, weapons, or other disturbing subjects.

### **PRONG THREE: SCHOOL DYNAMICS (STUDENT'S PERSPECTIVE)**

- ☑ **Student's attachment to school:** The student appears to be detached from school, including other students, teachers, and school activities.
- ☑ **Tolerance for disrespectful behavior:** The school does little to prevent or punish disrespectful behavior between individual students or groups of students. Bullying is part of the school culture, and school authorities seem oblivious to it, seldom or never intervening or doing so only selectively. Students frequently take on the roles of bully, victim, or bystander (sometimes, the same student plays different roles in different circumstances). The school atmosphere promotes racial or class divisions or allows them to remain unchallenged.
- ☑ **Inequitable discipline:** The use of discipline is inequitably applied or has the perception of being inequitably applied by students and/or staff.
- ☑ **Inflexible culture:** The school's culture—official and unofficial patterns of behavior, values, and relationships among students, teachers, staff members, and administrators—is static, unyielding, and insensitive to changes in society and the changing needs of newer students and staff members.
- ☑ **Pecking order among students:** Certain groups of students are officially or unofficially given more prestige and respect than others. Both school officials and the student body treat those in the high-prestige groups as though they were more important or more valuable to the school than other students.
- ☑ **Code of silence:** A code of silence prevails among students. Few feel they can safely tell teachers or administrators if they are concerned about another student's behavior or attitudes. Little trust exists between students and staff members.
- ☑ **Unsupervised computer access:** Access to computers and the Internet is unsupervised and unmonitored. Students are able to use the school's computers to play violent computer games or to explore inappropriate websites, such as those that promote violent hate groups or give instructions for bomb making.

### **PRONG FOUR: SOCIAL DYNAMICS**

- ☑ **Media, entertainment, and technology:** The student has easy and unmonitored access to movies, television shows, computer games, and Internet sites with themes and images of extreme violence. The student is intensely and exclusively involved with a group that shares a fascination with violence or extremist beliefs. The group excludes others who do not share its interests or ideas. As a result, the student spends little or no time with anyone who thinks differently and is shielded from the reality check that might come from hearing other views or perspectives.
- ☑ **Drugs and alcohol:** Knowledge of a student's use of drugs and alcohol and his or her attitude toward these substances can be important. Any changes in the student's behavior involving these substances can also be important.
- ☑ **Outside interests:** A student's interests outside of school are important to note since they can mitigate the school's concern when evaluating a threat or increase the level of concern.

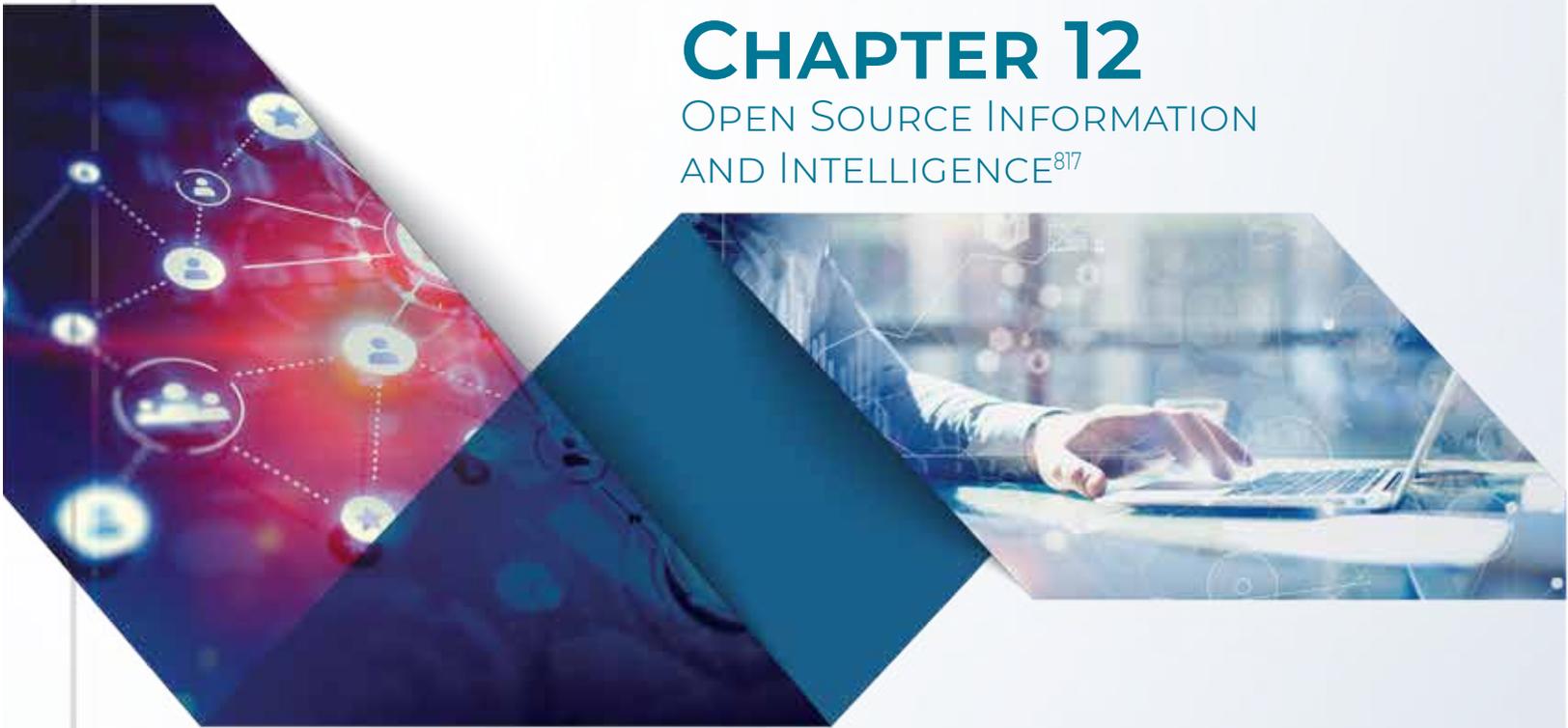
- ☑ **The copycat effect:** School shootings and other violent incidents that receive intense media attention can generate threats or copycat violence elsewhere. Copycat behavior is very common. Anecdotal evidence strongly indicates that threats increase in schools nationwide after a shooting has occurred anywhere in the United States. Students, teachers, school administrators, and law enforcement officials should be more vigilant in noting disturbing student behavior in the days and weeks, or even several months, following a heavily publicized incident elsewhere in the country.

## ADDITIONAL INFORMATION NEEDED

INFORMATION NEEDED	PERSON RESPONSIBLE

# CHAPTER 12

## OPEN SOURCE INFORMATION AND INTELLIGENCE<sup>817</sup>



When the collection of information for the intelligence process is considered, a historically undervalued resource has been open source information.<sup>818</sup> In many ways, open source information holds some of the greatest value for the intelligence process because of the vast array of diverse reliable information that is available for analysis—this is particularly true with digital networking. A great deal has been written on open source information, particularly as it is used in business intelligence and in national security intelligence.<sup>819</sup> The intent of the current discussion is to provide perspective for open source application in the law enforcement community, including important limitations that may be imposed on the retention of certain types of open source information that does not apply to the Intelligence Community or to the private sector.

While a wide range of open sources are not digital, it should go without saying that the growth of technology has radically changed the character of open source information. To provide perspective, as the public embraced the World Wide Web *en masse* beginning in the mid- to late 1990s, the Internet emerged as the primary source to search

<sup>817</sup> For an effective discussion of open source information, certain topics are most effectively illustrated using examples from commercial services and websites. Attempts were made to be objective in the illustrations and, where possible, use multiple sources. References to businesses and websites are for illustration purposes only and should not be construed as an endorsement in any form.

<sup>818</sup> Best, R., & Cumming, A. (2007). *Open Source Intelligence (OSINT): Issues for Congress*. Washington, DC: Congressional Research Service, p. 4.

<sup>819</sup> Williams, H., & Blum, I. (2018). *Defining Second Generation Open Source Intelligence for the Defense Enterprise*. Santa Monica, CA: RAND Corporation.

for all types of information. As computer memory and processing speeds increased, more information was being stored and processed, including audio and video files. The integration of computing into nearly every aspect of daily life—from workstations to the smartphones in our hands—spurred a greater reliance to search for online information millions of times a day. In turn, this has caused the development of faster, more discriminating search software and more search-friendly indexed websites. Similarly, content providers have increased the type and mass of content available on websites, not to mention the vast amount of information available through social media. Collectively, technological development and the willingness of the public to embrace these technologies have contributed dramatically to the ease, diversity, and value of open source information.

There is a caveat, however: Quantity of information does not equal quality of information. Open source users must take care by assuring the information collected from open sources to be used in decision making is accurate and dependable. Information absent quality control is not only of little value but also can have negative effects. The challenge, particularly when massive amounts of information are at one’s fingertips, is to make good end-user decisions about what information should be kept and which information should be discarded, particularly given the amount of information that is reposted on social media without any attention to validity and accuracy.

## UNDERSTANDING “OPEN SOURCE”

The concept of open source information and intelligence has increasingly been relied on by both the Intelligence Community and law enforcement. A brief discussion on the concept and its application in the current context will provide perspective.

## WHY IS THERE VALUE IN OPEN SOURCE INFORMATION?

Historically, open source information often held a second class status in the intelligence world because of the erroneous assumption that people, movements, and conditions that pose threats would not leave information that is available about their intent, characteristics, or behavior in the open.

This assumption is erroneous for six fundamental reasons:

- ◆ First, individuals and groups who pose threats because they have an extremist ideology—even those who support violence for their ideological goals to be fulfilled—typically want to share their beliefs and goals, usually with the intent to persuade others to adopt them. As a result, they often post such information on social media, on websites, in print, and in various broadcasts.<sup>820</sup> They want their beliefs known and the information available to radicalize others.
- ◆ Second, criminals use the Internet, particularly the dark Web, as a largely anonymous instrumentality to traffic in contraband. Offenders can easily reach a U.S. market from overseas and use techniques to make them difficult to track, both of which add to the lure. But the fact that they are operating on the Internet, including the dark Web, means it is open source.
- ◆ Third, certain types of information that are useful for the intelligence process—including information that identifies individuals—are openly available as a result of policy, regulation, or law that permits the custodian of such information to make it publicly available. For example, in some states public databases are available for motor vehicle licenses, property ownership, voter registration, business licenses, sex offenders, salaries of public employees, and a wide array of other information for which an individual has little, if any, control over its public release.<sup>821</sup>
- ◆ Fourth, people want selected information public. This can occur for a multitude of reasons: phone numbers, business names and addresses, and various reports of research and marketing are but a few examples. Not

820 For example, see media files supporting the World Jihad at <http://www.memri.org/>.

821 For example, see the Michigan Internet Criminal History Access Tool (ICHAT) at <https://apps.michigan.gov/>.

only do the individual pieces of information provide insight, but a surprising amount of new knowledge can be gained when such information is analyzed in the aggregate.

- ◆ Fifth, non-law enforcement entities—such as the news media or advocacy groups—may conduct inquiries that become open sources. These sources may provide personal information, descriptions of behavior, personal relationships, activities of a given group, relationships, and descriptions of an incident to satisfy the purpose of their businesses or causes.<sup>822</sup>
- ◆ Finally, often information becomes openly available because of carelessness by an individual. For example, a person making an incriminating statement in the presence of an open microphone or video recording on a smartphone in a public venue or a person writing incriminating information in a blog are examples. In each of these cases, valuable information that may be used in the intelligence process is often available via open sources.

## DEFINITIONS AND CATEGORIZATIONS

Open source *information* is any type of lawfully and ethically obtainable information that is collected without legal processes that describes persons, behaviors, locations, groups, events, or trends. The information may be freely available or purchased, the key is that anyone has access to the information. It is the method by which the information was collected that makes it open source, not the content or character of the information.

The array of information that falls within the open source arena is very broad. From a law enforcement perspective, one of the values of open source information is that it can be searched for and collected without legal process. However, as will be described later, civil rights issues may emerge related to the retention of open source information in a criminal intelligence records system.

As one should assume, when raw open source information is evaluated, integrated, and analyzed, it provides new insight about threats and trends—this is open source *intelligence*. (For reference, notably in the Intelligence Community, “open source information” is often abbreviated OSIF and “open source intelligence as OSINT.)

As noted previously, open source information is wide-ranging. To provide perspective, examples of categories of open source information include:

- ◆ All forms of social media.
- ◆ All types of news media.
- ◆ Shortwave broadcasts and conversations.
- ◆ Publicly available databases.
- ◆ Directories.
- ◆ Databases of people, places, and events.
- ◆ Open discussions, whether in forums, classes, presentations, online discussions on blogs, or general conversations.
- ◆ Government reports and documents.
- ◆ Scientific research and reports.
- ◆ Statistical databases.

---

822 For example, one advocacy group, the Plain View Project, is an online “. . .database of public Facebook posts and comments made by current and former police officers from several jurisdictions across the United States. . .that could undermine public trust and confidence in our police.” <https://www.plainviewproject.org/>

- ◆ Commercial vendors of information.
- ◆ Websites that are open to the public, even if there is an access fee or a registration requirement.
- ◆ Search engine results.
- ◆ Any kind of publication.
- ◆ Any kind of Internet or social media post.

The main qualifier that classifies information as open source is that no legal process or clandestine collection techniques are required to obtain the data. While open source information has virtually always existed, networking has obviously significantly increased its accessibility. For example, if an analyst is preparing a strategic intelligence report on trends in international terrorism, open sources the analyst may search are the websites of the National Counterterrorism Center,<sup>823</sup> the U.S. Department of State Bureau of Counterterrorism,<sup>824</sup> the Federal Bureau of Investigation’s (FBI’s) terrorism page (particularly the section reporting “terrorism news”),<sup>825</sup> the National Consortium for the Study of Terrorism and Responses to Terrorism (START) database,<sup>826</sup> and the Statista terrorism page<sup>827</sup> to download the various reports and data. If the analyst is preparing a report on white nationalism, open sources of value would include the Southern Poverty Law Center,<sup>828</sup> the Anti-Defamation League,<sup>829</sup> and once again the START database. In addition, the analyst may visit a white supremacy website, such as Stormfront,<sup>830</sup> to read posts and document trends in issues and topics as a basis for a qualitative analytic report. All of these are illustrations of open sources.

## SOURCE OF FIRST RESORT

Open sources are increasingly referred to as “the source of first resort.” This means that analysts and information collectors should exploit open sources of information as the first step in the information collection process. Particularly when intelligence gaps—whether tactical or strategic—are identified, open sources can provide important insights which may give functional direction to a line of inquiry.

For example, if a unique crime trend emerges within a community, an open source search of newspapers nationwide can identify other locations where crimes with similar *modus operandi* have occurred.<sup>831</sup> (This happened—belatedly—with the opioid crisis.) Similarly, unknown graffiti or a unique tattoo may be searched via image files. A blog search can provide unique insights about virtually any extremist group just as information may be obtained about a unique problem. Similarly, insightful information about sovereign citizens can be found on YouTube and information about MS-13 can be found on Tumblr.

As another illustration, because of the threat posed by jihadists, there is value of knowing the beliefs, language, arguments, and perspectives of jihadists. In order to:

---

823 <https://www.dni.gov/index.php/nctc-home>

824 <https://www.state.gov/bureaus-offices/under-secretary-for-civilian-security-democracy-and-human-rights/bureau-of-counterterrorism/>

825 <https://www.fbi.gov/investigate/terrorism>

826 <https://www.start.umd.edu/>

827 <https://www.statista.com/topics/2267/terrorism/>

828 <http://www.splcenter.org>

829 <https://www.adl.org/>

830 <http://www.stormfront.org/>

831 Some subscription services have a wide array of open source search capability, including newspapers. While an agency can subscribe to these services, if one has library privileges at a college or university, these search services—and many more—are available to users. Some public libraries may have these subscriptions, but a university library’s online resources are far more robust.

...improve strategic understanding of the of the jihadist threat by more effectively mining the Internet and other open sources for information. Such an effort, it is suggested, also will enable. . . a better tactical understanding of how jihadists use the Internet’s Web-television capabilities, chat rooms, and “news” sites, to train forces and raise money. Ultimately, these observers suggest, the United States must develop the capability to understand and influence foreign populations—“not in their council of states but in their villages and slums”—if it is to effectively counter the threat posed by jihadists. In such circumstances, it is argued, the information that should matter most to policymakers can be derived from open sources.<sup>832</sup>

Thus, the value of open sources as the “first resort” is multifold. When an issue or threat emerges, open sources can often provide an efficient, effective, and fast insight on the issue that may often validate the need for further inquiry. Similarly, open sources can provide a broad view of a person or threat as a means of establishing context and perspective. Moreover, open sources can often provide insights and relationships that may be missed by the inherent nature of many “closed” sources.

Allen Dulles estimated in 1947 that over eighty percent of the “information required for guidance of our national policy” was available in open sources. George Kennan revised the estimate to upwards of ninety-five percent in a 1997 *New York Times* interview.<sup>833</sup>

With this estimated amount of valuable information available through open sources, it is only reasonable to use these sources as a starting point in a line of inquiry. The application to law enforcement is just as valid as it is for national security. The scenarios described below—all of which are based on actual cases—illustrate this point.<sup>834</sup>

- ◆ A land developer reports that he has received a threat from an obscure radical environmental group saying that if he does not stop construction of condominiums at an environmentally sensitive location that “he will pay the price.” A quick search of news stories identifies the presence of the environmental group in other locations, its past activities and attacks, and the methods of attack. This can be an important element for defining specific intelligence requirements and methods of prevention in the current case.
- ◆ A tip is provided to a law enforcement agency that a radical Islamic cleric who preaches violence is going to be in the community to speak to a local group. An open source search provides information about the individual’s past speeches, the content of the speeches, and any public safety issues that emerged associated with the speech.
- ◆ The manager of a nursery reports that a man driving a rental van just purchased an unusual quantity of fertilizer. While a criminal history check was negative, an open source search of a commercial integrated database identified the individual’s address and persons known to use the same address. An Internet search engine identifies some of the man’s associates named on a right-wing extremist website.
- ◆ A confidential informant states that members of a violent gang are slowly moving into the region. An intelligence analyst conducts an open source search to learn more about the gang, identify gang characteristics and locate samples of the gang’s graffiti and tattoos that are distributed to patrol officers so that law enforcement can record the presence of gang symbols in the community.
- ◆ A group of anarchists announces that it is going to demonstrate against the president of the World Bank, who is speaking at the commencement ceremony of a local university. A search of anarchist blogs finds a discussion of plans by the anarchists to cause major disruption during the protests by destroying targeted property and resisting arrest.

---

832 Ibid. Best, R., & Cumming, A. (2007), p. 2.

833 Office of the Director of National Intelligence. (2007). *National Open Source Enterprise*. Washington, DC: ODNI, p. 3.

834 The author received this sample of cases from analysts and investigators during training and research site visits across the country.

In each case, the initial tip or lead was followed by a quick, open source search to gather more information. Not only did the open source information provide more insight about the threat, but the information aided analysts in defining explicit intelligence requirements to help in fully articulating the threat picture.

As a source of first resort, open sources are not only fast; they also represent a minimal intrusion on civil liberties. Furthermore, open sources are less expensive than traditional law enforcement information collection methods.

## OPEN SOURCE AND LAW ENFORCEMENT INTELLIGENCE— “TRADECRAFT”

“Tradecraft” is a collective term used by the Intelligence Community referring to the methods used in the intelligence process—particularly collection and analysis—on both broad and specific scales. While the term is rarely used in law enforcement, it is useful to understand its meaning in light of developments in the Information Sharing Environment.

Therefore, “open source tradecraft” has two meanings for law enforcement. At the macro level, it broadly refers to how open sources can be used in the intelligence process. At the micro level, it means the explicit procedures in conducting open source searches as well as collecting and interpreting raw open source information. There is a need for law enforcement to understand open source tradecraft at both levels.

The fact that information is collected from an open source should not dissuade a law enforcement officer or an analyst from using it. Indeed, there is often high-quality, insightful evidence available from open sources—so much so that the 9/11 Commission’s Final Report recommended that a new “open source agency” be added to the U.S. intelligence structure.<sup>835</sup> However, like virtually every other aspect of intelligence, the use of open sources in law enforcement intelligence has unique applications and parameters that vary from open source exploitation by Intelligence Community agencies. Fundamentally, the reports and resources focused on open sources by the IC are of international strategic importance to U.S. sovereignty with much less attention to issues related to crime. Despite these differences, as will be seen, there are many open source applications for law enforcement intelligence that should be incorporated as standard protocol in the intelligence process.

## LAW ENFORCEMENT APPLICATIONS OF OPEN SOURCE

There are both tactical and strategic applications of open source for law enforcement intelligence. Among these are:

- ◆ **Fact identification and verification.** Perhaps one of the most common uses of open sources in law enforcement is to identify and verify a wide range of facts. Dates and times of incidents, personal information, addresses and phone numbers, email addresses, vehicles known to have been used, property records, and other facts can easily be identified through open source public and commercial databases and directories.
- ◆ **Social networking.** Social media sites—such as Facebook, Instagram, and Flickr, among many others—provide a wealth of information about individuals and persons with whom they interact. Social media sites contain identity information of the user and his/her friends, often with photographs, as well as posts and statements about beliefs and behavior. Likes and dislikes are often enumerated—ranging from entertainment to politics to people—as well as contact information. As a result of the amazing array of information and images people post (often without good judgment), a great deal can be learned about them by just reviewing their posts and profile.

---

<sup>835</sup> National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. Washington, DC: U.S. Government Printing Office, p. 413. In 2005, the Open Source Center was created and encouraged access to the center by state and local law enforcement, who had access to the center for a decade. In 2015, its name changed to the Open Source Enterprise, and it was absorbed by the CIA’s Directorate of Digital Innovation. The Open Source Center website was decommissioned after the change.

- ◆ **Identifying criminal offenders.** In a surprising number of cases, people make incriminating statements in open sources. This has occurred in media reports but most commonly either in social media sites or on websites devoted to a particular deviant or unlawful behavior. Sexual predators, drug traffickers, persons trafficking in stolen property, and criminal extremists are all examples that are found with regularity on the “dark Web.” While incriminating statements alone will not meet the burden of proof for conviction, they can establish a criminal predicate and basis for further inquiry.
- ◆ **Understanding and interpreting of ideologies.** An important element of analysis that aids in defining and forecasting threats is to understand the motivation or rationale of individuals involved in criminal behavior. Particularly in the case of ideological extremists, websites can be a valuable source. Extremist websites typically articulate their beliefs as well as what behaviors or changes their movement will cause. Moreover, “drilling down” and reading blogs can provide more information about individuals’ beliefs and behaviors, including incriminating statements. Similarly, open sources can help analysts understand new or unusual ideologies such as incels<sup>836</sup> or ecofascism.<sup>837</sup>
- ◆ **Identification of criminal methodologies.** Collecting information from media sources, websites, and/or blogs can provide important insight about methods and targets of criminal acts. The modus operandi of violent serial offenders, criminal extremists, and criminal enterprises can be identified in many cases. This can be valuable information for developing preventive strategies. For example, a technique used by anarchists is the “black bloc,” which includes property destruction and other activities which could be criminal. The tactics can be learned via various open sources.<sup>838</sup> Similarly, everything from “how to cook meth”<sup>839</sup> to “how to make bombs”<sup>840</sup> can be found online.
- ◆ **Identification of emerging crime issues and trends.** Just as criminal methodologies can be learned from open sources, so can new and emerging crime trends. In many cases, certain types of crime geographically disperse in a consistent pattern. Drug trafficking and gang activity serve as good examples. Monitoring new and emerging crimes or changes in crimes on a broad geographic basis can often provide insight about crime problems that are on the horizon for a community. For example, methamphetamine hydrochloride first emerged in urban areas on both coasts of the United States. Its movement to rural areas and to the Midwest was on a fairly definable path permitting forecasting. Much of this information was easily identifiable through media reports. Opioid abuse followed a significantly different path, beginning with an overprescription of the drugs and marketing by drug producers. Investigative journalism documented the spread of opioid abuse on a national and regional basis, which has been insightful for law enforcement.<sup>841</sup>

836 See <https://www.vox.com/2018/4/28/17290256/incel-chad-stacy-becky> and <https://incels.co/>.

837 See <http://www.ecofascism.com/>.

838 <https://theanarchistlibrary.org/library/harsha-walia-10-points-on-the-black-bloc>

839 [www.drugalcoholrehabnow.com/how-to-make-crystal-meth.htm](http://www.drugalcoholrehabnow.com/how-to-make-crystal-meth.htm)

840 <https://1001guns.blogspot.com/2009/01/instructions-how-to-make-homemade-pipe.html>

841 As an example, see <https://www.tennessean.com/story/news/2017/04/08/timeline-how-opioids-crisis-began-took-hold-tennessee/98866140/>.

## AN EXAMPLE OF “PUSHED” OPEN SOURCE INFORMATION

During a trip to San Francisco for a training project, the author witnessed a series of direct-action demonstrations occurring in the city. Predominantly focused on the continued U.S. military presence in the Middle East, demonstrators were also expressing their views on other issues including opposition to the U.S. policy toward Israel, economic issues, and global warming. Some demonstrators stated on direct-action websites that they would be involved in civil disobedience and getting arrested as part of the protests.

To learn more about the protests and the plans, the author searched several direct-action websites related to the demonstrations. One website provided cell phone text messages on plans and events throughout the day. The author signed up for the text service and had information on the demonstration “pushed” to his cell phone, therefore not only monitoring the events, but arriving at locations where civil disobedience was planned before most demonstrators arrived.

The texts were open sources in near real time—which illustrates that with technology, open source information can take diverse forms.

An important word of caution: There is always a need to verify sources and content found from open sources. Particularly on social media posts, accuracy is rarely a prevailing concern.

## OPEN SOURCES AND CIVIL RIGHTS

While a great deal of discussion about open sources focuses on social media, remember that open sources are much more and can include not only information posted online (including the deep Web) but also documents and publications, such as physical public records or books. Unlike the Intelligence Community and the private sector, state, local, and tribal law enforcement (SLTLE) agencies must be vigilant in the management of open source information because of unique rules that apply to information retention in a criminal intelligence records system.

Raw information obtained from open sources tends to fall into three categories that have important significance for an SLTLE agency: (1) Information about *identified individuals and organizations*, (2) information and activities about *unidentified individuals and organizations* and (3) *aggregate* nonidentifying information. As a general rule, when a law enforcement agency conducts an open source search for information, it should be assumed that civil rights protections attach to any information that identifies individuals or organizations no matter how innocuous that individual piece of information appears to be. Conversely, as a general rule, no civil rights attach to aggregate information or descriptions of issues, trends, ideologies, activities, and so forth that do not identify an individual or organization.

As noted in Chapter 7, of particular importance is information involving expressive activity that is protected by the First Amendment. It is fairly common to find information posted on blogs and websites that express extreme statements about a diverse array of behavior, such as support for white nationalism, extreme opposition to immigration, vehement opposition to policies of government officials, and even advocacy of pedophilia and so forth. The difficulty lies in distinguishing between extreme expressive beliefs and statements that have a criminal nexus.

The statements in Table 12-1 illustrate expressive beliefs (left column) versus statements with a likely criminal nexus (right column). Assume the statements are made by a person who has been identified by an SLTLE officer.

The differences are sometimes subtle. The expressive statements, while extreme, are less explicit. Moreover, even in these illustrations, additional facts and circumstances would be needed to establish a criminal predicate.

TABLE 12-1: COMPARISON OF EXPRESSIVE STATEMENTS AND STATEMENTS WITH A CRIMINAL NEXUS

EXPRESSIVE STATEMENT	STATEMENT WITH A CRIMINAL NEXUS
◆ “All politicians are corrupt and ought to be shot.”	◆ “The only way to make our point is by killing Senator Doe.”
◆ “Doctors who perform abortions are committing murder and must be stopped no matter what.”	◆ “The only way to stop Dr. Doe from performing abortions is for us to blow up her clinic.”
◆ “Everyone should try fentanyl.”	◆ “DM me if you want some fentanyl.”
◆ “Violence is the only message our opponents understand.”	◆ “I urge you to kill our opponents, regardless of who or where they are.”

It is good practice to assume that any information identifying individuals or organizations collected from open sources must be 28 CFR Part 23-compliant.<sup>842</sup> Thus, there must be evidence establishing a reasonable suspicion that there is a nexus between the person or organization identified in the open source and a crime—that is, the “criminal predicate test.” The essential principle is not the *source* of the information but *what information is being retained* by a law enforcement agency in its criminal intelligence records system. Illustrations of open source applications include the following:

<sup>842</sup> The reader is reminded that 28 CFR Part 23 applies only to information that is placed in a criminal intelligence records system.

- ◆ If information is being collected from open sources as part of the criminal investigation of a crime that has already occurred, the criminal predicate test for intelligence records typically does *not* apply. Information from a criminal investigation would be placed in the law enforcement agency's records management system (RMS), rather than the criminal intelligence records system.
- ◆ If a group plans a protest or demonstration in a jurisdiction, open source information may be used to determine how past protests or demonstrations have been conducted, what tactics have been used in other protests and demonstrations, and what outcomes and behaviors of the protesters and demonstrators have occurred with no criminal predicate required.
  - While there is some debate, the general rule is that an open source inquiry identifies people who have been arrested in the past during a protest or demonstration (such as from a news story); this information alone is not sufficient to establish a criminal predicate in the current demonstration.
  - If the law enforcement agency receives a suspicious activity report that an identified person may commit a crime during the course of the protest or demonstration, that information may be retained in a temporary criminal intelligence file until further information can be collected to verify the veracity of the suspicious activity information. In these cases, the law enforcement agency's criminal intelligence records policy should be followed.
- ◆ Descriptive information about extremists' ideological beliefs; behaviors of those supporting those beliefs; changes and trends in extremists' beliefs or collective behavior; methods advocated for accomplishing the goals of the extremist ideology; and potential targets of the extremists' actions may all be collected, analyzed, and retained by a law enforcement agency without a criminal predicate as long as specific individuals or organizations are not identified.

Creating intelligence records on persons who are merely "suspicious" is both tempting and easy using open source data. Exploring a social media site through its search utility to determine whether something interesting is located about a person is similarly easy. However, law enforcement personnel must follow 28 CFR Part 23 compliant procedures for collecting and retaining open source information in a criminal intelligence records system just as they would for any other form of criminal intelligence information. It warrants repeating: The issue is not whether the information is from an open source, but whether a law enforcement agency can properly keep the information. Decisions must focus on the *reason* for which information is being retained (i.e., criminal predicate), not the *source* of the information.

An important point to remember is that laws vary by state and locality, whether it is intelligence records laws, open records legislation, a state Freedom of Information Act, or a state privacy act. There is sufficient variability among the states to warrant a careful review of state law as it relates to criminal intelligence records.

**Working with technology companies.** Often, open source searches lead to the need to use the legal process to gain further information on an inquiry. Of course, when a law enforcement agency seeks information on the specific behaviors of an individual who is a customer of a private company or a member of a social media site, privacy concerns arise.

While this process moves beyond open sources, it should be noted that technology companies typically have a published policy and guide to work specifically with law enforcement agencies. While it is important for the reader to be aware of this, since legal process has to be used and information is being sought that is not openly available, it is not open source information when the process requires a request for information about a specific customer (or customers) of a technology company.

## ATTRIBUTION AND COPYRIGHTED MATERIALS IN INTELLIGENCE PRODUCTS AND TRAINING MATERIALS

Much of the open source information acquired through the intelligence process is in the public domain (i.e., information for which no copyright is claimed). In other cases, as with certain commercial databases, rights to the information have been obtained by contract in accordance with usual government procurement procedures. In many other cases, however, agencies acquire copyrighted information and use it beyond the fair use standard sometimes without the authorization of the copyright holder and, more frequently, without attribution.

Too often, work products from law enforcement agencies—including training materials and documents reproduced without attribution or permission of the copyright holder—are distributed to employees, handed out in training classes, and/or posted on an intranet or Web page. Attribution is important for four basic reasons:

1. It gives corroboration and support for the line of logic, inference, or conclusion that is presented in the report.
2. It permits the consumer to go to the original source for further information on the subject as well as giving the consumer the opportunity to independently evaluate the original source.
3. Attribution will typically meet the standards of law for copyrighted materials fair use.
4. Attribution is the ethical and correct method of operation by giving appropriate recognition to the thoughts, ideas, creativity, and work of others.

The importance of attribution has been reinforced by the ODNI through Intelligence Community Directive (ICD) 206—*Sourcing Requirements for Disseminated Analytic Products*.<sup>843</sup> The directive states:

Source reference citations shall be included as endnotes in disseminated analytic products. These endnotes shall be provided for all significant, substantive reporting or other information upon which the product's analytic judgments, assessments, estimates, alternative hypotheses and views, or confidence levels depend.<sup>844</sup>

The importance of attributing information to the original source is based on the notion that:

[t]horough and consistent documentation enhances the credibility and transparency of intelligence analysis and enables consumers to better understand the quantity and quality of information underlying the analysis.<sup>845</sup>

Of course, not all attributed material is copyrighted work—particularly in the case of public records. Most public documents and information that has been originally collected by the law enforcement agency are not copyrighted. In these cases, attribution is important for validity purposes.

Beyond public records there is information that should be attributed, particularly if it is from a copyrighted source. For example, information in a strategic intelligence product is drawn from a research report on drug trafficking trends, a video from a television network that is used to illustrate terrorist attack methods or the original concept and ideas of a consultant that is used in an intelligence report, all should be considered as copyrighted or at least attributable materials from the original source.

A copyright is a form of protection provided by the laws of the United States<sup>846</sup> to the authors of original works, including not only written materials—both published and unpublished works—but also video and audio materials.

843 <http://www.fas.org/irp/dni/icd/index.html>

844 Office of the Director of National Intelligence (ODNI). (October 17, 2007). ICD 206. *Sourcing Requirements for Disseminated Analytic Requirements*. Paragraph D.2., p. 2.

845 Ibid., Paragraph B., p. 1.

846 United States Code, Title 17.

Under the protection of federal copyright law,<sup>847</sup> the owner of a copyright has the exclusive right of use, distribution, and limitation to distribution, as well as to authorize others to reproduce copies; use the copyrighted material; prepare derivative works based on the original; and rent, sell, or transfer the copyright.

Law enforcement agencies are obliged to follow copyright law just as any other individual or organization. While it is important to understand and respect copyrighted works, there is an exemption that permits use of the materials without seeking permission of the copyright owner. This exception is referred to as the fair use exemption.<sup>848</sup>

The fair use of a copyrighted work, including such use by reproduction in copies or phonorecords<sup>849</sup> or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use, the factors to be considered shall include:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes.
2. The nature of the copyrighted work.
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
4. The effect of the use on the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.<sup>850</sup>

Even when using materials under the fair use exemption, attribution (i.e., referencing) to the original source must be done. With specific reference to copyright law and open source intelligence, a Congressional Research Service report stated:

In using such copyrighted information, intelligence agencies, like other users of public information, are governed by the doctrine of “fair use” (based on common law and codified in the Copyright Act of 1976 (17 USC 107)).<sup>851</sup>

Clearly, law enforcement agencies are also obliged to conform to copyright law. Beyond the legal requirements, it is simply good practice to offer attribution of information where applicable.

Complicating the copyright and attribution issues, law enforcement agencies sometimes use the services of a commercial vendor whose work product has copyright protection. Care must be taken to ensure that users of the information understand the copyright implications in the service contract. For example, if a commercial vendor is contracted to perform analytic work and produce a report, a contract provision should ensure that the work products created under the contractual agreement are the intellectual property of the law enforcement agency, not the vendor.

---

847 United States Code, Title 17, Section 106, with reference to the Copyright Act of 1976.

848 Ibid., Section 107.

849 “Phonorecords” is language from the 1976 law and has been interpreted to include all forms of audio and video media that meet the other standards for copyright protection. Similarly, digital materials such as Web pages are also included.

850 <http://www.copyright.gov/title17/92chap1.html#107>

851 Ibid., Weimer, D. R. (2005). *The Copyright Doctrine of Fair Use and the Internet: Case Law*. Washington, DC: Congressional Research Service.

In the process of collecting information and the preparation of intelligence products, law enforcement personnel should not avoid materials because they are copyrighted. The rule is to simply be certain to provide proper sourcing<sup>852</sup> of the information and be aware of the proper procedures in the fair use exemption.<sup>853</sup>

## METRICS FOR OPEN SOURCE USE

A great deal of information has been discussed about the effectiveness of open source information; however, the only true measure of effectiveness is to ensure that it is designed and evaluated to meet the specific needs of the intelligence environment in which it is being used. A challenge, however, is the absence of widely accepted measurements or metrics related to open source intelligence. Responsible managers must develop outcome measures for intelligence practices to ensure they are accomplishing their intended goals (i.e., effectiveness) and are doing so in a manner that does not waste resources (i.e., efficiency). Moreover, the metrics may be used to help justify expenditures for commercial database subscriptions.

Simple open source metrics may include the following:

- ◆ A count of open sources attributed in intelligence products.
- ◆ The proportion of all analysis where open sources are used.
- ◆ The proportion of time when open sources are the source of first resort for intelligence requirements.
- ◆ Time requirements for locating needed information in the open source environment versus the closed source environment.

While somewhat superficial, these metrics represent more than is typically used. Moreover, inasmuch as open source information is used by all-source analysts in connection with information from closed sources, it is difficult to measure how much open source information contributes to a specific intelligence product.

It is anticipated that open source information will increasingly be relied upon given its greater availability, the nature of issues that today's analysts must cover, and the heavier emphasis placed on it by senior intelligence leaders.<sup>854</sup>

The ultimate open source metric is the qualitative contribution open sources make to the analysis. While this is difficult to measure, long-term evaluative assessments should be developed in a descriptive narrative that focuses on the type of open sources that are used and the methodology of their inclusion in the intelligence process that is most productive.<sup>855</sup>

## ONLINE OPEN SOURCE CONTENT FOR THE INTELLIGENCE PROCESS

While open sources include information beyond the Internet, it is apparent that information about virtually any topic can be found online. Indeed, the quantity of information can be overwhelming. Having some perspective of different types of open source content that has particular value for law enforcement intelligence and how to find that content can make the navigation and collection process more manageable.

---

852 Intelligence Community Directive 206 provides a significant amount of detail of information that should be included in the attribution.

853 The United States Copyright Office website <http://www.copyright.gov/> is very comprehensive and should provide answers to most copyright questions, including the fair use doctrine.

854 Ibid., Best, R., & Cumming, A. (2007). *Open Source Intelligence (OSINT): Issues for Congress*. Washington, DC: Congressional Research Service, p. 17.

855 Pherson, R. H., & Heuer, R. J. (2020). *Structured Analytic Techniques for Intelligence Analysis*. 3rd ed. Thousand Oaks, CA: Sage Publications.

## OPEN SOURCE INFORMATION IDENTIFYING PEOPLE AND ORGANIZATIONS FROM SUBSCRIPTION SERVICES AND THE MEDIA

Two open sources that frequently identify people and organizations that warrant special attention are subscription database services and media reports. While these are often subject to question with respect to the propriety of their use, both may be properly used and can be of great value to law enforcement intelligence. However, just as in the case of any open source, the nature of the sources must be understood and the regulations concerning retention in criminal intelligence records systems must be applied in the same manner as any other information.

The search of media sources<sup>856</sup> can also provide a significant amount of information about individuals, organizations, trends in crime, movements, and criminal extremist ideologies. News services have global networks of sophisticated communications and informants with trained staff to conduct research and investigate virtually all issues that would be of interest to a consuming public. As a general rule, responsible news organizations also have editorial policies to ensure that the information used in news stories is valid, reliable, and corroborated (i.e., well-sourced). Crime and criminal extremism are important news; hence some journalists often seek to learn as much as possible about these incidents. The depth of information frequently includes details that are useful in the intelligence process. The news media can openly identify individuals and organizations involved in criminal incidents and often link similar individuals and incidents in diverse geographic locales. A search of news stories can provide both important leads and important undiscovered detail about a line of inquiry. A word of caution, however: Not all media sources adhere to the same high standards. The practices and reputation of the media source must be evaluated just as any other source. Moreover, ensure that information that is being used from news sources is fact-based reporting and not opinion or editorial pieces.

A number of companies have developed systems that permit a search for information from public and commercial databases using proprietary data integration software.<sup>857</sup> Examples of the types of data that may be obtained are listed in Table 12-2. Companies that provide subscription databases permit the development of extraordinarily detailed information about people into a summary report—some services also provide an analysis of the information. Even though a fee is charged for these services, they are still open source because anyone can purchase the data and neither legal processes nor surreptitious collection methods are used.

Using artificial intelligence (AI), images, video, and text can be easily linked to develop a comprehensive dossier of a person, all through open sources. At least one company has taken this a step farther through the use of “Web scraping”—the harvesting of information, images, and video from websites, such as all social media. Using AI to integrate the data and facial recognition to identify people, this is an amazingly powerful open source collection and analysis service available to law enforcement.<sup>858</sup>

Since both subscription services and media sources can provide a significant amount of detail about individuals and organizations, it is important to repeat once again that the criminal predicate rule is still applicable for information placed in law enforcement intelligence records.

---

856 For example, searching via a subscription service such as Lexis-Nexis: <https://www.lexisnexis.com/en-us/home.page>.

857 As one example, see LexisNexis Accurant for Law Enforcement: <https://risk.lexisnexis.com/products/accurant-for-law-enforcement>.

858 While it is lawful, there have been ethical issues expressed about the use of this technology. Civil libertarians have expressed opposition to the technology, notably Web scraping and the use of facial recognition. Collecting information from social media posts is legal because of the Third Party Doctrine. There are some civil law challenges to the company from social media platforms asserting that Web scraping is an intellectual property violation. At this point, the technology can lawfully be used by a law enforcement agency except in those communities that have prohibited police use of facial recognition technology.

## SECURITY RECOMMENDATIONS FOR SEARCHING AND INTERACTING WITH CRIMINAL OR EXTREMIST SOCIAL MEDIA PLATFORMS

- ◆ Use a designated computer, particularly when “virtually undercover,” that is not used for any other law enforcement work. Each computer and device has its own Internet Protocol (IP) address to identify the device.
- ◆ Use a virtual private network (VPN) for your network connection. A VPN will:
  - Bypass geographic restrictions on websites or streaming audio and video.
  - Protect you from snooping on untrustworthy Wi-Fi hotspots.
  - Give you at least some anonymity online by hiding your true location.
  - Protect you from being logged while torrenting (downloading a large file).
- ◆ Use a browser that does not track your browsing history.
  - Tor is the most secure and is necessary for searching deep websites.
  - Firefox provides substantial secure and nontracing browsing.
- ◆ Use a search engine that is secure and does not trace searches, such as DuckDuckGo.
- ◆ Keep a log of “virtual undercover sessions” including notable results and interactions.
- ◆ Only designated users should use this computer.
- ◆ When done, clear the cache and cookies in the computer and shut the device down so it will reset when restarted.

See also the U.S. Army Identity Awareness, Protection and Management Guide, <https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Identity%20Awareness%20Protection%20Management%20Guide%20DoD.pdf>.

TABLE 12-2: EXAMPLES OF INFORMATION OBTAINABLE FROM SUBSCRIPTION DATABASE SERVICES

- ◆ Full names
- ◆ Dates of birth
- ◆ Places of birth
- ◆ Parents, spouses, siblings, and children
- ◆ Known associates
- ◆ Known phone numbers and email addresses associated with all the names
- ◆ Social security numbers
- ◆ Mortgage and lien information
- ◆ Credit reports
- ◆ Credit cards and credit card usage
- ◆ Professional affiliations
- ◆ Occupations and employers
- ◆ Licenses of all types
- ◆ Vehicle, watercraft, and aircraft registrations
- ◆ Images, address, and GPS location of residence and employment
- ◆ Images of a person, family members, and friends

**National Media Exploitation Center.** On a related point, initiatives by the Intelligence Community related to media information are worthy of note. Because of the vast amount of information that is available and easily accessible from the global news media, the National Media Exploitation Center (NMEC) was established in late 2001 at the Central Intelligence Agency (CIA).<sup>859</sup> The center’s role is to coordinate FBI, CIA, Defense Intelligence Agency, and National Security Agency efforts to analyze and disseminate information gleaned from millions of pages of paper documents, electronic media, videotapes, audiotapes, and electronic equipment.<sup>860</sup> Starting with only a small number of employees, the NMEC has about 700 employees, with around 100 linguists, today including offices overseas.<sup>861</sup> Originally focusing on news media and published open sources, the office has expanded its role to include the exploitation of captured hardware, such as laptops and cell phones.

859 Don Cryer, Special Assistant to the Director of Central Intelligence for Diversity Management. (November 5, 2003). Prepared statement, hearing before the Permanent Select Committee on Intelligence, 108th Congress.

860 Federal Bureau of Investigation. (undated). “The FBI’s Counterterrorism Program Since September 2001.” *A Report to the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: FBI, p. 16.

861 <https://www.usatoday.com/story/news/world/2018/01/31/smartphones-computers-terrorists-intelligence-agency-united-states/1079982001/>

In this venue, exploitation refers to the collection of open source information relevant to defined requirements, integrating it with other known information and deriving new knowledge from this process—that is, developing open source intelligence. The NMEC has a great deal of expertise and resources. SLTLE agencies may take advantage of the NMEC through federal partners—typically the FBI or the U.S. Department of Homeland Security (DHS)—at the primary state fusion center.

## SOCIAL NETWORKING AND ISSUES FOR OPEN SOURCE

A social network is a linked, interactive structure of people consisting of nodes that may be either an individual or group. The basis of the linkage is a shared interest of virtually any definable character—music, occupation, personal philosophy, political affiliation, sexual orientation, hobbies, and so forth. Each node may have multiple connections based on different variables.<sup>862</sup> For example, one person (i.e., a node) may be a member of multiple social networks. A person who is an accountant may also be a motorcycle enthusiast, enjoy country music, and be an avid fantasy football player. Each one of these variables could represent membership in different social networks. There are similar social network models that can be defined for people who support extremist ideologies, are gang members, or are involved in illegal activities, such as drug trafficking or money laundering. Interestingly, smugglers tend to have multiple criminal social networks because they deal with different commodities of different criminal enterprises—drugs, firearms, stolen property—where the logistics are largely the same. Online, the most visible social networks are social media platforms.

While social networks have existed in some form since the dawn of humankind, the growth of the Internet has resulted in new social networks that are virtual, notably represented by websites such as Facebook, YouTube, Instagram, Weibo, Twitter, Reddit, or Pinterest, to name a few. There are other social networking websites that are not as sophisticated or widely known but also represent diverse interests. Ironically, social network members frequently post information that is incriminating or, at the least, sufficiently strong to establish a criminal predicate as related to their behavior. While in some cases one may find gang members or supporters of the Earth Liberation Front on popular social media platforms, there are many more underground platforms that have postings indicating criminal behaviors. That is why creative search strategies—including developing the skills and tools to search the deep Web—become important. Typically, intuitive search criteria do not produce the results being sought. Rather, the use of terms and phrases unique to the social structure is required. As a result, background research to understand a social network becomes an important starting point.

Many social media sites permit the posting of video; however, YouTube is by far the most robust. The videos range from humor to personal statements about all types of issues. Included are videos related to Hamas, Hezbollah, white nationalism, neo-Nazis, Earth Liberation Front, Mexican drug cartels, street gangs, MS-13, and others. In some cases, the videos are critical while in other cases, they are supportive or promote the issue. Reviewing the videos can provide unique insights and images, including signs and symbols of the group being examined (i.e., exploited) and important indicators of the social network. Careful review of not only what is being said, but the images in the video ranging from clothing to the background, can be of substantive value for the analysis. As illustrated in one study:

Developments in the last two decades have enhanced the status and impact of gangs; namely globalization and technological advances. No longer is it the case that activities and events remain situated in a local context. To the contrary, from the seemingly benign (e.g., drug use) to the publicly violent (e.g., gang initiations), behaviors are transformed from actions witnessed by a handful of people to images and recordings posted on the Internet and broadcast to households around the world. This matter is enhanced in the gang context, in contrast to other types of criminal organizations since gangs are composed of youth where access and knowledge of Web-based applications is practically second nature. For example, anyone familiar with YouTube ([www.youtube.com](http://www.youtube.com)) can simply query “gang fight”

---

862 Knoke, D., & Yang, S. (2020). *Social Network Analysis*. 3rd ed. Thousand Oaks, CA: Sage Publications.

and well over 50,000 video clips are available for viewing. Further, websites and social networking pages (e.g., Facebook) are devoted to specific gangs, as well as communication devices and applications (e.g., cell phones, twitter), that provide the capability to mobilize people and direct their movements in a very short period of time. How technology factors into the organization of the group remains to be seen as limited research has focused on the intersection where gangs meet technology. In turn, technological advances have implications for globalization and gangs.<sup>863</sup>

To be most successful in searching a social network, the user must create an identity and become a member of the network. For purposes of intelligence inquiries, a false identity and an email address should be created by the law enforcement user. Importantly, there are certain ethical and legal limits that should be fully explored before going forward. Of particular concern is the need to be certain that statements and actions by a law enforcement employee do not induce a person to commit an act that the person would not have done otherwise without the inducement (i.e., entrapment). As a result, a law enforcement agency should develop a policy and procedures to guide the use of creating a false identity and using that identity for the intelligence process including social networking.<sup>864</sup> As noted in Chapter 7, being “virtually undercover” is lawful, although creating a false identity on a social media platform typically violates the company’s end-user agreement.

**Real-Time and Open Source Analysis<sup>865</sup> (ROSA).** ROSA is a resource guide developed by federal, state, and local partners to provide guidance in the exploitation of open sources, and particularly social media. The process is used by law enforcement and analytic personnel to (1) develop or enhance criminal intelligence (including situational awareness reports), (2) support a criminal investigation, or (3) identify public safety risks either past, present, or anticipated. During the ROSA process, law enforcement and analytic personnel gather publicly available information (otherwise known as open source) via social media resources and tools for analysis to determine whether criminal activity is occurring to support a criminal investigation or to assess risks to public safety and security. ROSA emphasizes the importance of timeliness for intercepting and analyzing online threats as well as the need for objective analysis to distinguish between expressive communications and threatening communications. The ROSA guide has resources to ensure P/CRCL protections and policy recommendations for social media analysis.

## NEWSLETTERS, BLOGS, MESSAGE BOARDS, AND WHITE PAPERS

An important part of strategic intelligence is monitoring a variety of variables related to a threat—essentially, these are standing intelligence requirements. Open source materials that are particularly useful for this purpose are newsletters, blogs, message boards, and white papers.

**Newsletters** are designed to highlight issues, trends, and developments within a specific topic area. *Blogs* are Web-based opinion discussions also frequently focused on an expressed topic area where writers and readers express opinions, perspectives, and beliefs.<sup>866</sup> A *message board*, also known as a forum, is an online discussion area in which users with similar interests discuss topics. These conversations or discussions are available in the form of posted messages. In many cases, a single source is a mixture of a newsletter, a message board, and/or a blog. For example,

---

863 Decker, S. H., & Pyrooz, D. (2013). “Gangs: A New Form of Organized Crime?” *Oxford Handbooks Online*. <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199730445.001.0001/oxfordhb-9780199730445-e-008>.

864 As a technical point, searching a social networking site is an open source. However, establishing a false identity on the site to lure an individual into making incriminating statements is surreptitious and, therefore, not an open source.

865 <https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide>

866 As an example, White Nations, <https://whitenations.com/>, is a blog and a message board for white nationalists predominantly from North America, Europe, and Australia. Understanding the white nationalist ideology with respect to its issues and trends can prove extraordinarily insightful.

a particularly useful newsletter and blog for intelligence issues is *Secrecy News*<sup>867</sup> from the Federation of American Scientists<sup>868</sup> (FAS). A *white paper* is a persuasive, authoritative, and generally detailed report on a specific topic. It is typically produced by a researcher/research organization or a commercial enterprise. Its intent is to inform and persuade the reader. For example, Cellebrite, a widely used digital intelligence company, produces a series of white papers on relevant current issues that provides insights to readers and helps market the company's services.<sup>869</sup>

In general, there are four broad categories of newsletters, blogs, message boards, and white papers:

- ◆ **Professional/academic and government**—These sources tend to be among the most objective. However, never rule out the ideological influence, even if unintentional, of an author or editor. Despite this caveat, these sources are most likely to make statements based on corroborated information and use an approach to analysis and conclusion based on logic and the scientific method rather than emotional arguments. Typically, these sources are more objective in reporting of facts and data and most commonly include attribution of facts and data.
- ◆ **Commercial sources**—As the name implies, these are profit-driven sources often intended to provide information that supports the sale of products or services. Despite the fact that the motive of the source is to make a profit, the sources can nonetheless be very reliable. Indeed, the reliability of these sources is often an important selling point for the business. While the information is typically accurate, information about alternatives is not likely to be included.
- ◆ **Advocacy groups**—These sources are agenda-driven based on the ideology and goals of the source. A newsletter from a right-wing extremist source will reflect information that supports that ideology. Similarly, discussions in a blog on environmental extremism will support the goals of that group. The reader should recognize “where the group is coming from” and factor that into his or her analysis. Using this approach, it can be quite insightful to understand an ideology or advocacy position based on these sources .
- ◆ **Pundits**—A wide range of individuals blog on the Web as critics and commentators on virtually every subject. Pundits work for a wide variety of organizations—news media, entertainment media, professional organizations, advocacy organizations, etc.—and some are independent commentators working for themselves, often not as a source of income, but as a means to discuss an interest or belief. What is important to recognize is that typically, pundits do not seek to be objective but rather to comment on a topic of interest from their particular ideology or perspective. (This is also true for pundits who blog for news organizations.) Often, their arguments and observations are persuasive and useful, but usually they are not objective. Pundits are frequently news and policy wonks; hence their research often identifies issues and sources of information that might otherwise be easily missed. As such, they are often good sources of raw information that can be corroborated through objective sources. (A caveat is to ensure that a pundit is not a conspiracy theorist—at first blush, some of pundits’ arguments can seem compelling.)

Subscribing to newsletters and monitoring blogs, message boards, and white papers on a consistent basis can provide a wealth of information on trends, issues, and anomalies. When a new issue of concern begins to emerge on a consistent basis, particularly if it is reflected in multiple sources, the issue should be proactively explored through other information sources to (a) determine its reliability and validity and (b) assess the probable impact on one’s area of responsibility.

---

867 See <https://fas.org/blogs/secrecy/>.

868 The Federation of American Scientists website contains a great deal of interesting and useful information related to intelligence issues, including downloadable documents, many of which are often difficult to access. See <http://www.fas.org>.

869 <https://www.cellebrite.com/en/whitepapers/>

## WIKIS

A *wiki* is software that allows users to easily create, edit, and link pages together. Wikis are often used to create collaborative websites and to power community websites, often also referred to as *wikis*.<sup>870</sup> These collaborations are increasingly being used by businesses to provide affordable and effective intranet sites and for knowledge management.<sup>871</sup> More specifically, the collective business knowledge of all members of an organization can be documented, refined, and shared in a dynamic virtual environment.

Wikis are generally designed with the philosophy of making it easy to correct mistakes, rather than making it difficult to make them. Thus, while wikis are open, they provide a means to verify the validity of recent additions to the body of pages. The most prominent, on almost every wiki, is the “recent changes” page—a specific list enumerating recent edits or a list of all the edits made within a given time frame.

Critics of publicly editable wiki systems argue that these systems could be easily tampered with, while proponents argue that the community of users can catch malicious content and correct it. The safe lesson on a public wiki is to use it as a pointer system and corroborate the content of interest.

Perhaps the best-known wiki is the online encyclopedia Wikipedia.<sup>872</sup> However, there are many types of wikis,<sup>873</sup> some with a very specific focus.<sup>874</sup> For example, the ODNI provides a wiki called Intellipedia that is specifically focused for Intelligence Community analysts. Wikis can be a valuable source for dealing with a topic or issue about which the information collector has limited information. Most wikis include external references to materials, which helps in the corroboration process.

From an intelligence perspective, the wiki can provide subject-matter knowledge on an issue as well as direction to more information.<sup>875</sup>

## RSS FEEDS

RSS (really simple syndication, also referred to as “rich-site summary”) is an information sharing process used online to publish frequently updated content including, but not limited to, blog entries, news headlines, and podcasts to subscribers. An RSS document (called a feed, a Web feed, or a channel) contains either a summary of content from an associated website or the full text. RSS makes it possible for people to keep up with changing Web content and new or breaking information and news that can be sent to the subscriber in an automated manner.<sup>876</sup>

From an open source perspective, the value of RSS feeds, when available on a website, is that any new information or changes in content are sent to those registered for the service without the need to check each site.<sup>877</sup> This increases both the efficiency and timeliness of information for the user.

## GREY LITERATURE AND GREY INFORMATION

Grey literature is open source information that includes a range of documents not controlled by commercial publishing organizations. This means that grey literature can be difficult to search and retrieve for review. Knowledge

---

870 <https://cft.vanderbilt.edu/guides-sub-pages/wikis/>

871 <http://en.wikipedia.org/wiki/Wiki>

872 [http://en.wikipedia.org/wiki/Main\\_Page](http://en.wikipedia.org/wiki/Main_Page)

873 For example, there are incel wikis. See [https://incels.wiki/w/Main\\_Page](https://incels.wiki/w/Main_Page) and <https://incels.wiki/w/R/HAPAS>.

874 A wide variety of wikis is available and can be searched through <http://www.wiki.com/>.

875 For example, see the crime wiki at <http://unclesam.pbwiki.com/Crime>.

876 <https://www.digitaltrends.com/computing/what-is-an-rss-feed/>

877 As an example of RSS feed in law enforcement, see <https://www.policeone.com/info/law-enforcement-police-rss-feeds/>.

and information gained through practice, but not necessarily research, is referred to grey information.<sup>878</sup> While it is open, the information is often not easily identified or retrieved. One of the greatest challenges involved with grey literature is the process of identification, since there is limited indexing, and acquisition, and availability is usually marred with uncertainty. Added to this is the absence of editorial control, raising questions about authenticity and reliability.

Traditionally, grey literature was defined as any documentary material that is not commercially published and is typically composed of technical reports, working papers, business documents, and conference proceedings. More of these types of documents are becoming available online, but they are often not discovered by traditional search engines.

From an intelligence perspective, this author views the concept of grey literature and grey information more broadly, particularly as applied to information collection. The basic idea of grey literature has three components: (1) there are documents of interest which exist; (2) the information is open; and (3) the information is not widely indexed thus not distributed and therefore difficult to locate. As a result, the concept of grey literature should not be limited to academic or scientific works but be applied to any documents characterized by these three elements.

For example, brochures printed by a right-wing extremist that are handed out at a local gun show, or flyers handed out at a demonstration that were printed by anarchists, could also be “grey.” In both cases, the documents are not commercially published but are intended to be openly disseminated as broadly as possible (the limitation often being a budgetary one). The limited supply of these unpublished materials makes them difficult to identify or locate. Collection of grey literature is a challenge and must be explored in light of the types of potential literature that exists and where it might be located, often by a human collector rather than by networking.

## THE DEEP WEB AND THE DARK WEB/DARKNET

The World Wide Web has several layers. Legitimate users are familiar with the *surface* Web, where data can be freely accessed using standard search engines, and the *deep* Web, where information (e.g., personal bank accounts) can be accessed using unique login information.

The “deep Web” or “invisible Web” refers to:

...the vast repository of information that search engines and directories don’t have direct access to, like databases. Unlike pages on the visible Web (that is, the Web that you can access from search engines and directories), information in databases is generally inaccessible to the software spiders and crawlers that create search engine indexes.<sup>879</sup>

The third layer is the *dark* Web<sup>880</sup> (also referred to as the darknet), where content is not only very hard to access, requiring unique downloadable software programs, but users and transactions remain anonymous. Although there are legitimate users on the dark Web, such as political dissidents, whistleblowers, and human rights activists, it is also a safe haven for criminal elements.<sup>881</sup>

The dark Web is attractive for criminals, since it allows them to leave hardly any trace of their illegal activities. Various types of criminals use the dark Web: Black marketeers sell all kinds of illegal goods and services, such as drugs and weapons, on dark Web marketplaces. Threat actors use botnets to create large amounts of traffic to block or suspend

---

878 Adams, J., et al. (2016). “Searching and Synthesizing ‘Grey Literature’ and ‘Grey Information’ in Public Health.” *Systematic Reviews*. Volume 5, Article 164. <https://doi.org/10.1186/s13643-016-0337-y>

879 <https://usa.kaspersky.com/resource-center/threats/deep-web>

880 It is described as “dark” not because the content is inherently criminal but because it is difficult to navigate, is inherently rich in anonymity, and requires special software.

881 *Dark Web Monitoring Challenges*. (2020). Cobweb Technologies White Paper. <https://www.cobwebs.com/>

server access, making legitimate websites unreachable. Terrorists use the dark Web to enlist services, communicate, buy weapons and explosives, and finance their operations. Hackers, fraudsters, and threat actors use the dark Web to launch their campaigns, buy and sell hacker tools, collect ransom money, and sell stolen data on various dark Web forums. Hit men, arms dealers, and gangs engaged in pornography and sex/human trafficking use the dark Web to stay under the radar of law enforcement.<sup>882</sup>

Documented criminal cases from both U.S. and European law enforcement agencies involving the dark Web as a key instrumentality have already been made for a variety of crimes, including the following:

- ◆ **Illicit drugs of all types**—This accounts for a large portion of illegal online transactions via darknet marketplaces. Vendors are even reviewed and rated by customers.
- ◆ **Weapons**—Commonly available; purchases made by persons who are unable to make legal firearms purchases; persons who want to make their weapons purchases anonymously; and persons purchasing firearms or accessories that are illegal to sell.
- ◆ **Personally identifiable information files of persons**—stolen names, addresses, phone numbers, social security numbers, and health records used for everything from fraud to identity theft.
- ◆ **Counterfeit identification**—Passports, driver’s licenses, and visas from various countries that are used in fraud, as criminal instruments for other crimes, to hide one’s true identity, and to escape detection and apprehension.
- ◆ **Illegal pornography**—While there are different forms of obscene materials that are illegal, the vast majority of illegal pornography in the darknet is child pornography.
- ◆ **Intellectual property crime**—This is predominantly counterfeiting of goods (trademark infringement and production of goods without authorization of the trademark holder) and piracy (illegal use of literary and artistic works).
- ◆ **Sale and distribution of stolen and prohibited goods**—This ranges from stolen technology devices and jewelry to stolen antiquities and sale of protected species (such as ivory).

As an illustration, Figure 12-1 shows two screenshots from the Icarus darknet market. Notice in the top screenshot the red box highlights items for sale, including such things as drugs and fraud (stolen identities). In the lower half of the figure in the second screenshot, part of the drug marketplace is displayed; the first three items are ecstasy, marijuana, and LSD, with associated descriptive information including price. Purchases are paid in cryptocurrency, and shipments are typically via UPS or FedEx (unknowingly) but also include the postal service.

Another unique aspect of the darknet has been the growth of illicit businesses on the dark Web that host a variety of hidden services and marketplaces, selling the tools of the trade for cybercriminals to rent or buy to launch cyberattacks. “Cybercrime as a service”—along with attacks as a service, malware as a service, and fraud as a service—has opened a wide digital door.<sup>883</sup> Examples include:

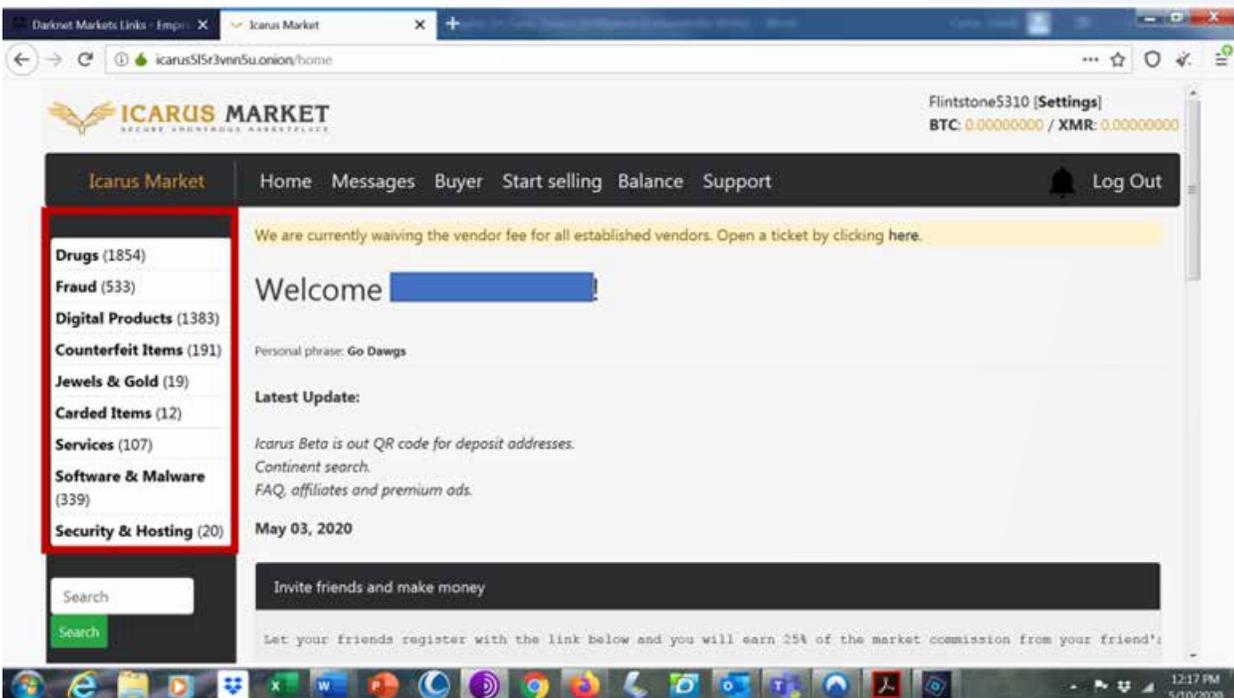
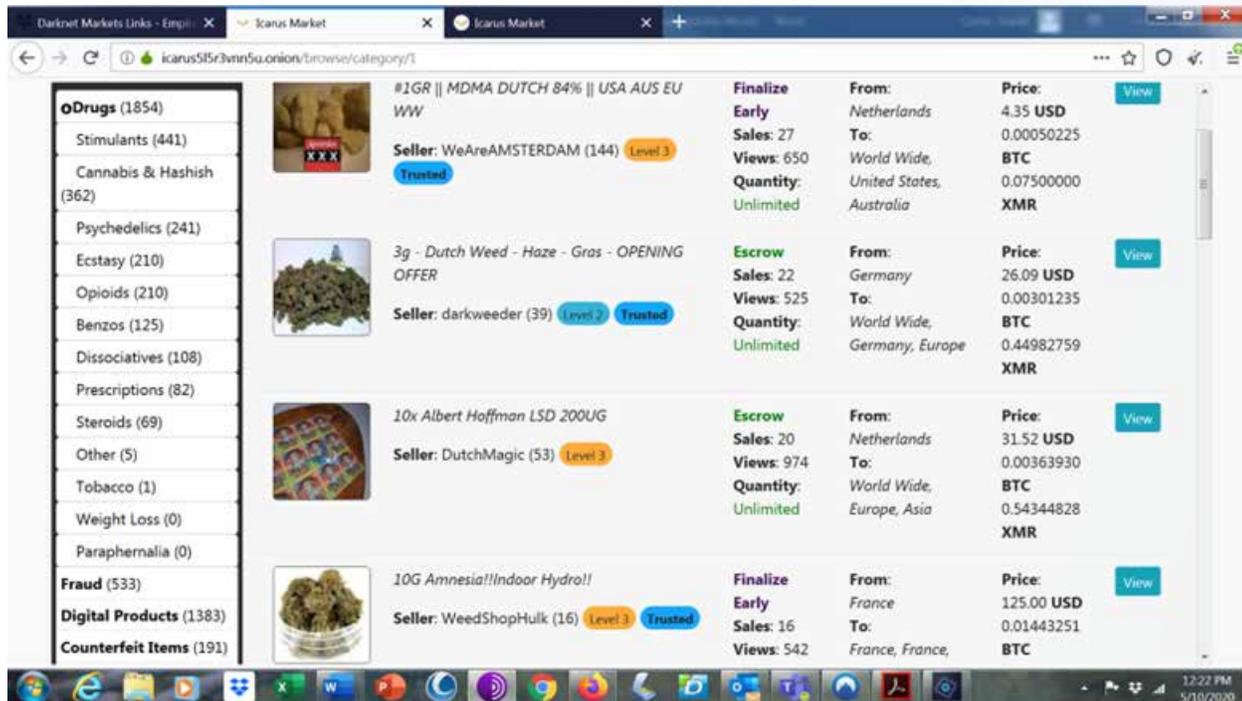
- ◆ **Malware as a service**—Cybercriminals actually license the use of malware and can receive technical support. This permits cybercriminals to conduct cyberattacks without investing in the development of the malware. Ransomware is an example.
- ◆ **Hacking for hire**—If a cybercriminal wants a website or system compromised or something stolen from the system or website but does not have the expertise, the criminal can hire a hacker, typically from a darknet job board.

---

882 Ibid.

883 “The Rise of Cybercrime as a Service.” (2017). *CSO Online – Cybersecurity Insights*. <https://www.csoonline.com/article/3205253/the-rise-and-rise-of-cybercrime-as-a-service.html>

FIGURE 12-1: EXAMPLES OF A DARKNET MARKET PLACE



- ◆ **Botnets**—“Leased” primarily for committing distributed denial of service (DDoS) attacks that can bring down a website or a network.
- ◆ **Crypting**—A service that encrypts and hides malicious software code so that it can evade detection by antivirus programs, thereby allowing malware to be installed on a computer.
- ◆ **Fraud as a service**—This has matured to the level of diversification and specialization. In the arena of cybercrime, groups have emerged into areas of specialization, with those at the top of the food chain acting as general contractors to tailor an approach to fraud that the cybercriminal wants.

The dark Web is hidden in the deep Web, which accounts for 90 percent of all Web content. The dark Web consists of IP addresses that are routable but not in use. Basically, it is a repository of hidden websites that can be accessed only with special software, such as Tor.<sup>884</sup> Common estimates suggest that the “deep Web” contains 500 times the content that is found in the visible Web. There are five broad types of content that constitute the invisible Web:

- ◆ **The content of Web-based databases.** Information stored in databases is accessible only by query to the database and are not picked up by the “Web crawlers” used by search engines. This is distinct from static, fixed Web pages, which contain documents that can be accessed directly. A significant amount of valuable information on the Web can be generated from databases.
- ◆ **Nontextual files.** These include audio and video files, graphics files, software, and documents in formats such as portable document format (PDF).<sup>885</sup> Web crawling has a limitation in searching the content of these types of files. Web crawlers can identify file names and extensions (e.g., .jpg, .wmv, .pdf) of such files but cannot identify the content of these files during the Web-crawling process—essentially, files that are not in HTML<sup>886</sup> format. Hence there is a great deal of information and data that is not picked up from these files by traditional searches.
- ◆ **Script-based Web pages.** These are Web pages that are written in script coding other than HTML and/or those with URLs<sup>887</sup> that contain a “?”.<sup>888</sup>
- ◆ **Content available on sites protected by passwords or other restrictions.** Websites protected by some degree of access through rigorous password protection or a virtual private network (VPN) do not have content identified by search engines. There is a continuum of identifiable and nonidentifiable information from these types of websites depending on what types of information the site owners elect to be publicly accessible (often for marketing purposes) as well as the degree of security applied to the site (in some instances, the website’s security is limited, and some data can be identified). Suffice it to note that a significant amount of information from these sites is not identifiable through traditional search engines. Hence part of a website may be in the surface Web and part in the deep Web. For example, a bank’s website is on the visible Web that gives information about the bank, type of accounts, locations of ATMs, interest rates, and so forth. However, the information in customers’ bank accounts is in the deep/invisible Web, protected by passwords and security from Web-crawling search engines.
- ◆ **Pages deliberately excluded by their owners.** A Web page creator who does not want his or her page captured in search engines can insert special meta tags that will cause most search engines’ crawlers to avoid the page.

Obviously, a great deal of open source information from the deep Web could be valuable to the intelligence process if it could be identified and retrieved. The deep Web is searchable, but not using standard search techniques. Hence the goal is to find tools that can locate valuable open source deep Web information.<sup>889</sup> The most effective ways to search the deep Web is to use search utilities that are designed to explore specific databases. While this still reaches only a portion of the deep Web, the information gained from these databases can be extremely valuable—although not necessarily convenient. That is, deep Web searching of databases typically requires accessing a variety of different websites to conduct a search for the desired information.

---

884 <https://www.torproject.org/>

885 These files can be located by a search engine by the file name, which is commonplace. However, a search engine cannot index the content of these types of files. For example, a search engine cannot locate a tattoo in an image or video file. However, a specialized AI search tool could locate the tattoo.

886 HTML is hypertext markup language.

887 A URL is uniform resource locator, which is the Web address.

888 <https://www.ntchosting.com/encyclopedia/scripting-and-programming/script/>

889 For a guide to assist your search strategy, see <https://guides.lib.umich.edu/c.php?g=283340&p=2126706>.

## PUTTING THE DARKNET IN CONTEXT

EXCERPTED FROM: DRUGS AND THE DARKNET: PERSPECTIVES FOR ENFORCEMENT, RESEARCH AND POLICY EUROPOL (2017)

Developments in information technology are transforming virtually all aspects of modern life; this now includes the way that illicit goods are traded and the modus operandi used by organized crime groups (OCGs). Online anonymous drug marketplaces can therefore be seen as part of a more general development for which addressing cybercrime and the use of information technology platforms for criminal purposes has become a more important policing priority across the EU. Innovation in criminal practices in this area represents a recognized challenge to established law enforcement practice and, if operational capacity is to keep pace, such innovation requires responses that are equally innovative and technologically informed. This report contributes to this objective by providing the conceptual framework necessary for understanding developments in this area, accompanied by an EU-focused analysis of darknet operations and a review of both the challenges and successes associated with darknet inquiries.

The analysis reported here supports the conclusion that drug transactions are a significant and important element of darknet market activities (although modest in value compared with the overall estimated retail drug trade in the EU), accounting for around two-thirds of all offers made on the cryptomarkets reviewed. This report has also detailed how law enforcement interventions can disrupt darknet markets. That said, overall, this new online ecosystem appears relatively resilient to disruption, with new marketplaces becoming established and vendors and buyers quickly migrating to new platforms. This resilience, as well as the relatively large scale and diversity of drug market activity, means that current operational models that are considered appropriate for addressing some other forms of hidden online criminality, such as the marketing of illegal firearms or the facilitating of crimes against children, may not be directly transferable to, or sufficient in isolation for, tackling the online drug trade. Experience to date would suggest that, to increase the effectiveness of law enforcement activities, market disruption needs to form part of a broader, more integrated set of measures implemented as part of an overall strategy to address the drug market. This implies that the identification and targeting of major vendors, in addition to market administrators, is needed to prevent simply displacing activities from the targeted marketplaces to other marketplaces. It also implies that it is equally important to target the other key elements of the supply chain, such as production, precursor sourcing and bulk trafficking, without which the online market cannot function. To some extent, this means recognizing that established intelligence led policing approaches must be brought together but conducted in a technologically informed, coordinated, and collaborative manner, if law enforcement activities are to have a sustained impact on the online drug trade.

<https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy>

There are hundreds of search engines available—many are very specialized—that can be valuable in the intelligence process. It is somewhat futile to develop a list of the engines here because there are so many, and they change so frequently. Rather, simply do an Internet search for search engine directories<sup>890</sup> to aid in finding the type of search needed. There are also resources online to aid you in developing your deep Web search strategy.<sup>891</sup>

What should be apparent is that much of the deep Web is not “hidden” in a surreptitious manner. Rather, it is hidden because it contains information in formats or architectures that are not readily identifiable by standard search engine

---

890 For example, a specialized list of search engines and directories can be found at <http://webquest.org/sdsu/searching/specialized.html> as well as at the Association of Internet Research Specialists, <https://aofirs.org/search-engines-list/>.

891 One example is <https://www.deepwebsiteslinks.com/how-to-access-the-deep-web/>.

technologies, often to maintain the security of the information. As a result, it takes specially designed search utilities and greater effort by the user to identify and capture deep Web information.

## A BROADENED PERSPECTIVE OF OPEN SOURCE FOR LAW ENFORCEMENT

The value of many Web resources—such as directories, extremist websites, and social networking sites—for law enforcement intelligence is evident. However, a wide array of data that have value for the intelligence process are less intuitively evident.

For example:

- ◆ Information about a possible threat that includes the name of a geographic feature not known to the analyst (e.g., an analyst in Arizona detects a potential threat to the Mackinac Bridge in Michigan but is unfamiliar with the massive structure connecting the state’s two peninsulas)
- ◆ Information about the demographic characteristics in a geographic area that is needed in a strategic intelligence assessment
- ◆ Information from a foreign source about money, distance, weight, temperatures, or the size of clothing (among other things) that needs to be converted to U.S. standards
- ◆ Real-time information to track either a commercial flight or private aircraft
- ◆ The GPS coordinates and legal description and/or image of a house in question
- ◆ A satellite image of a given location
- ◆ The need to convert a digital video so it can be viewed on a law enforcement computer
- ◆ The need to identify relatives of an intelligence target

These requirements, and much more, can be found in an eclectic array of Web-based open sources. (See Chapter Annex 14-1 for the descriptions and locations of these websites.) The point of note is simple: One of the important values of online open sources is easy access to information that is unique, yet critical to a comprehensive analysis.

## HOMELAND SECURITY INTELLIGENCE AND OPEN SOURCES

Beyond enforcing the criminal law, America’s law enforcement agencies have a wide range of well-established responsibilities related to public safety and order maintenance. Whenever there is a natural disaster—such as a flood, a tornado, or a hurricane—law enforcement has the responsibility to aid in the rescue and recovery of victims, protect unharmed citizens from injury, and protect property. Similarly, in a catastrophe, such as the crash of an airliner, the collapse of a building, or a public health emergency, law enforcement agencies have historically had significant public safety and order maintenance responsibilities.

With the creation of new national initiatives related to homeland security after the 9/11 attacks, many of these public safety responsibilities have become more structured. Particularly with the growth of intelligence fusion centers, most of which have an operating philosophy of all crimes, all hazards, and all threats, a new form of noncriminal intelligence has emerged: homeland security intelligence.

It should be reinforced that intelligence is based on prevention and is inherently a pre-incident function, whether that incident is criminal or all hazards/noncriminal. In the case of homeland security intelligence, information and analytic needs are much broader. They need to help law enforcement agencies understand the dynamics of a crisis, the continued threat it poses (to community members and first responders alike), to understand the likely evolution of the crisis and actions that law enforcement can take to mitigate the danger to the community.

As the reader will recall from Chapter 1, homeland security intelligence may be defined as “the analytic output of raw information that describes noncriminal threats to critical infrastructure, public health or community safety.” As a result, law enforcement needs to obtain a wide range of information to effectively prepare for any homeland security threat identified through analysis. Open sources can be particularly valuable to the intelligence process to aid in understanding the characteristics and threats posed by a pandemic,<sup>892</sup> hazardous materials, or any other direct or incidental threat posed by a homeland security emergency.

For example, a wide range of information related to hazardous materials may be found at Environmental Chemistry;<sup>893</sup> information on threats to public health can be obtained from the Centers for Disease Control and Prevention (CDC),<sup>894</sup> a wide range of diverse useful information is available from a collection of online searchable databases provided by the National Center for Biotechnology Information (NCBI)<sup>895</sup> and weather threat information from the National Weather Service.<sup>896</sup>

The broad range of homeland security threats is too exhaustive for a comprehensive discussion. The essential point to note is this: Since the responsibility of homeland security intelligence has become a part of the law enforcement intelligence process, particularly at the state fusion center level, analysts and information collectors should aggressively use open sources as the first step of collecting this critical information.

## OPEN SOURCE PROCESSES AND PROTOCOLS

A number of tools and techniques may be relied on to make the open source collection process more productive as well as to enhance the quality of information. The following discussion is intended to be a primer for insights of the process.

### USING AN OPEN SOURCE COLLECTION PLAN

As anyone knows who has browsed the Internet, the ability to search diverse information and travel down an unanticipated path of hyperlinks can easily draw one away from the original line of inquiry into an area of often interesting but frequently irrelevant information. From an intelligence perspective, this is unproductive and risks the collection of unneeded and sometimes distracting information. As a result, when using networking to seek open source information, the user is urged to develop an open source collection plan.

A collection plan is essentially a research methodology that seeks to focus the open source information collection process. Rather than relying on a dragnet approach, the collection plan focuses on source searching that is defined by specifically identified agenda items, such as:

- ◆ Determining intelligence requirements.
- ◆ Researching an emerging threat issue that has been identified.
- ◆ Identifying information in support of tips and leads that have been received.
- ◆ Researching information about a known local threat to determine its presence and effects in other geographical areas.

---

<sup>892</sup> As we learned in the 2020 novel coronavirus pandemic, there were many lessons that had to be learned “on the fly,” such as how to monitor and police executive stay-at-home orders or share information on police calls in which a person infected with the virus was within the confines of the law enforcement exemption of the privacy requirement of the Health Insurance Portability and Accountability Act (HIPAA).

<sup>893</sup> <http://environmentalchemistry.com/>

<sup>894</sup> <http://www.cdc.gov/>

<sup>895</sup> <https://www.ncbi.nlm.nih.gov/>

<sup>896</sup> <https://www.weather.gov/lwx/IdentifyThreats>

- ◆ Researching diverse and creative tactics to manage threats.
- ◆ Gaining a body of information about a specific intelligence target.
- ◆ Gaining knowledge about the current and changing nature of threat conditions in your region.

The plan should include:

- ◆ Specific types of information needed (names, locations, characteristics, or indicators of the threat or criminal behavior; signs and symbols of the threat; effects of the threat).
- ◆ Identification of the sources where the specified information is most likely to reside.
- ◆ Critical information associated with a given threat (e.g., methods, geography, modus operandi).
- ◆ Logistical information associated with threats.
- ◆ Materiel used in the commission of a crime or terrorist act and how that materiel is used.
- ◆ Unique characteristics related to the intelligence target (e.g., important dates, times, symbolism).

Developing the collection plan is an exercise in critical thinking that is best accomplished with a team approach. The significant point is that open source information collection through networking can be of the greatest utility when it has a specifically directed agenda.

## TECHNIQUES AND TOOLS

Perhaps the most important foundation skill to develop for any type of networking environment is to become adept at searching. The most common approach is to open one's search engine of choice and use the default search utility for the information that is needed. Of course, some successes are achieved with this method; however, the results can often provide a large quantity of related information but often lack the specificity needed. Narrowing the search can be more productive in seeking the information that is needed.<sup>897</sup> The first step is to develop a pre-search plan to focus on search requirements (See Chapter Annex 14-2). Beyond this plan, some tips for narrowing the search are as follows:

- ◆ Understand the **culture of the intelligence target** to both identify and accurately interpret relevant information. With a clear understanding of the culture of the target or the information that is being sought, a wider array of search terms/phrases can be developed. Moreover, narrowing the terms may assist in defining the sources or search engine to use. For example, if the threat is from MS-13, there have been a great number of news stories, investigative reports, court cases involving MS-13 members, research reports,<sup>898</sup> and even YouTube videos made by MS-13 members. The information learned from these open sources can provide valuable insight to understand the gang's culture, language, symbols, and methods.
- ◆ Based on the cultural assessment, **carefully define the types of information** that is being sought. To do this, rely on the concept of being "collectively exhaustive." That is, an attempt should be made to search all derivative terms that describe the data or phenomenon being sought in the search. For example, search for white supremacy should also include white nationalism, right-wing extremism, 88, 14 words, 13/52,<sup>899</sup> and other symbols and words.
- ◆ Once the information is defined, **dissect this information to develop alternate** terms, synonyms, jargon, symbols, abbreviations, and alternate spellings.

<sup>897</sup> A white paper on Internet search techniques is at <http://whitepapers.virtualprivatelibrary.net/SearchTips.pdf>.

<sup>898</sup> A quick search MS-13 on Google Scholar, <https://scholar.google.com/>, found thousands of research reports on the gang.

<sup>899</sup> See <https://www.adl.org/hate-symbols> for the meaning of these and other symbols of the movement.

◆ Examine **different formats of the information** being sought. For example, a search for the name *John Alexander Doe* should take several forms, such as:

- John Doe                      J Alexander Doe                      J. Doe                      Alex Doe
- Johnny Doe                      Alexander Doe                      J.A. Doe                      J. “Alex” Doe

This is particularly important for deep Web searches.

- ◆ Use the **advanced search utility** available in most search engines. As illustrated in Figure 12-2, there are a number of variables that can be controlled to narrow the search.
- ◆ **Specialty search engines**<sup>900</sup> can help focus a search by limiting searches to explicitly defined areas. For example, using a search engine that only focuses on news websites can pick up useful information from trends in terrorism or crime to the names of individuals or organizations or ideologies that may be associated with threats. Moreover, news websites often make an assessment of the quality of information easier than many other sites.
- ◆ **Language translation** from multiple languages to English is increasingly available easily online. Typically, these sites permit the copying and pasting of text for translation. Figure 12-3 provides an illustration from Google Translate.<sup>901</sup> While the translation tools are not perfect, they work surprisingly well.

**National Virtual Translation Center.** Building on this last point, when foreign language translations are necessary, the National Virtual Translation Center<sup>902</sup> (NVTC) may be an additional resource to explore. Established by Congress in 2003, the NVTC serves to provide timely and accurate translations of diverse raw information for all elements of the Intelligence Community. A virtual workplace, NVTC personnel, and linguists are located throughout the United States and connect via various networks with the NVTC program office in Washington, DC. As a member of the Intelligence Community, the NVTC is part of the Information Sharing Environment. As a result, the NVTC may become a resource for SLTLE agencies—and particularly fusion centers—on inquiries that may coincide with IC concerns. SLTLE agencies should work with their FBI or DHS fusion center partners to secure assistance with the fee-based center.

FIGURE 12-2: EXAMPLE OF FIELDS TO LIMIT SEARCH



## THE NEED TO DETERMINE ACCURACY, RELIABILITY, AND VALIDITY

As is the case with any information collected for the intelligence process, it is essential to evaluate the accuracy of facts, the reliability of the source of information, and the validity of the information’s content. These concepts are the same as for any type of information in the intelligence process:

- ◆ **Accuracy**—The information and facts are true and may be corroborated.
- ◆ **Source reliability**—The source of the information is dependable for providing accurate information.

900 A wide variety of general and specialty Internet search engines can be found at <https://kinsta.com/blog/alternative-search-engines/>

901 <https://translate.google.com/>

902 <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch/national-virtual-translation-center>

- ◆ **Information validity**—The information actually depicts or portrays what it purports.

A good method to measure these standards in open sources is to seek multisource reporting of information for validity. An important issue is to ensure that multisource reporting is not merely repetitive reporting. For example, *USA Today*, CNN, Fox News, and MSNBC may all report the same news story. If all of these news outlets are simply reporting the same facts derived solely from an Associated Press story, then this is not multisource validity. This is referred to as the “echo chamber,” which is described as:

... a group of media outlets that tend to parrot each other’s uncritical reports on the views of a single source, or that otherwise relies on unquestioning repetition of official sources.<sup>903</sup>

In the example above, if each network reports the AP story and *independently confirms it* relying on its own reporters, then this is multisource validation. A useful tool for assessing validity and reliability can also be found online through websites such as Truth or Fiction<sup>904</sup> or Snopes.<sup>905</sup> These websites contain surprisingly comprehensive and well-sourced information about rumors, legends, and information that has been quoted as fact. (They have also proven very adept at providing facts that debunk conspiracy theories.) The websites typically describe the veracity of a story, with some form of explanation.

Web content is bursting with hyperbole, innuendo, and false information. One must be diligent to ensure that collected information is accurate, reliable, and valid.<sup>906</sup>

## AVOIDING TRAFFIC ANALYSIS: BECOMING ANONYMOUS ON THE WEB

Online intelligence and investigation procedures should mask the Internet protocol (IP) address of the computer being used. This can easily be accomplished in two ways. One is to have a stand-alone computer that is used only for sensitive searches or transactions.<sup>907</sup> Ideally, the computer would not be connected to any other network with the law enforcement agency or be used for any personal activities, such as accessing any accounts requiring a user name and a password.

The other method is to use a VPN for all connections. As noted previously, the ideal would be to have a stand-alone computer and a VPN.

The reason that the IP address should be masked is that there are tools available on the Internet to trace domain names, IP addresses, connection routes, email addresses, general geographic locations of the computer, and other

903 [https://www.sourcewatch.org/index.php?title=Echo\\_chamber](https://www.sourcewatch.org/index.php?title=Echo_chamber)

904 <http://www.truthorfiction.com/>

905 <http://www.snopes.com/>

906 For a comprehensive discussion of reliability, particularly as related to the Web and open source information, see <http://sourcesandmethods.blogspot.com/2008/10/how-to-determining-source-reliability.html>.

907 This is sometimes referred to as a “hello computer,” much like a generically registered “hello telephone” used in law enforcement undercover operations.

FIGURE 12-3: GOOGLE TRANSLATION SCREENSHOT



electronic transaction information. These tools can also be effectively used by law enforcement and can be found such websites as DomainTools,<sup>908</sup> Better-Whois,<sup>909</sup> and Geektools.<sup>910</sup> It should be noted that different “Whois” websites have different databases to search; hence multiple sources may be needed. If, however, the IP being searched for has been “cleaned” through a VPN or proxy server, the Whois search will not be fruitful.

Finally, on a regular basis the computer’s cookies and Internet cache should be cleaned. This will help ensure anonymity, particularly in light of the fact that someone will inevitably use the computer for personal business. While cookies and the cache can be cleaned manually, the most effective way is to use software designed for that purpose.<sup>911</sup>

## THE INVESTMENT OF CRITICAL THOUGHT AND TIME

Despite the ease and speed of the Internet, two of the most important open source tools are *critical thought* and *time*. Both are needed to define search terms/phrases, developing the collection plan, identifying critical information needed in an inquiry, verifying the information, and interpreting it. Often, this information leads to other sources, and critical thought is needed to dissect the additional source alternatives, weighing the value of each and moving the search and collection processes forward.

The process can be laborious, particularly as one sifts through diverse blogs. Reading, consuming, interpreting, and collecting important information from the overwhelming quantity of information is labor-intensive but valuable for discovering information that can be essential in identifying and preventing threats.

Information collectors and analysts must have the wherewithal to push the process forward, particularly during searches that seem to be unproductive. Managers and administrators must develop the patience to understand these unique performance characteristics when evaluating personnel.

## CONCLUSIONS

The intent of this discussion was to provide an overview of the open source concept, the current philosophy and application of open source information, the role of open sources in law enforcement intelligence, and a primer on the use of open source techniques and tools for the intelligence process. The websites listed in this discussion are intended to serve as illustrations and are not meant to represent a comprehensive listing or an endorsement of any particular commercial or open application.

As the “source of first resort,” open source information and intelligence provide tremendous potential for law enforcement that should be exploited to increase the efficiency and effectiveness of the intelligence function.

---

908 <http://whois.domaintools.com/>

909 <http://www.betterwhois.com/>

910 <http://www.geektools.com/tools.php>

911 There is effective software available at no charge on the Internet for cleaning cookies and the cache. See a discussion of cookies, caches, avoiding spyware, maintaining your computer’s registry, recommendations for software, and additional useful information at the nonprofit site <https://www.instant-registry-fixes.org/>.

## INFORMATION THAT CAN BE LEARNED FROM YOUR COMPUTER’S INTERNET PROTOCOL ADDRESS

Information that is useful to law enforcement is also useful to those persons monitoring visitors to their websites. If a computer’s Internet protocol (IP) address is not “anonymized,” the types of information that can be gained from the IP alone include:

- ◆ City and state where the computer is accessing the Internet
- ◆ Area code
- ◆ Longitude and latitude
- ◆ Internet service provider
- ◆ Last website visited

See for yourself—visit the websites below:

- ◆ <http://www.zabasearch.com>
- ◆ <http://www.ip-address.com/>

*Importantly, using a VPN will falsely report this information if someone seeks to check the computer’s IP—that is one reason that using a VPN is urged.*

# CHAPTER ANNEX 12-1: ECLECTIC WEBSITES FOUND USEFUL FOR INTELLIGENCE

## ECLECTIC WEBSITES FOUND USEFUL FOR INTELLIGENCE

The intelligence process sometimes needs information that would not intuitively seem to be part of a law enforcement inquiry. These websites can be accessed at no charge.

The Geographic Names Information System (GNIS), developed by the U.S. Geological Survey in cooperation with the U.S. Board on Geographic Names, contains information about physical and cultural geographic features in the United States and associated areas, both current and historical (not including roads and highways). The database holds the federally recognized name of each feature and defines the location of the feature by state, county, USGS topographic map, and geographic coordinates. The Geographic Names Information System (GNIS) may be found at [https://www.usgs.gov/faqs/what-geographic-names-information-system-gnis?qt-news\\_science\\_products=0#qt-news\\_science\\_products](https://www.usgs.gov/faqs/what-geographic-names-information-system-gnis?qt-news_science_products=0#qt-news_science_products).

- ◆ The National Geospatial Intelligence Agency (NGA) GEOnet Names Server (GNS) provides access to the National Geospatial-Intelligence Agency's (NGA) and the U.S. Board on Geographic Names' (US BGN) database of foreign geographic feature names. The database is the official repository of foreign place-name decisions approved by the US BGN: <https://geonames.nga.mil/gns/html/>.
- ◆ The *Statistical Abstract of the United States* is the authoritative and comprehensive summary of statistics on the social, political, and economic organization of the United States. Sources of data include the Census Bureau, Bureau of Labor Statistics, Bureau of Economic Analysis, and many other federal agencies and private organizations: <https://catalog.data.gov/dataset/statistical-abstract-of-the-united-states>.
- ◆ The *U.S. Explore Census Data* user can obtain comprehensive population, housing, economic, and geographic data in the form of maps, tables, and reports from a variety of U.S. Census Bureau sources: <https://data.census.gov/cedsci/>.
- ◆ Sometimes, simple information is needed—such as:
  - The geographic location of an area code: <http://decoder.americom.com/>.
  - Social security numbering scheme: <https://www.ssa.gov/history/ssn/geocard.html>.
  - The definition of a word: <https://www.dictionary.com/>.
- ◆ This How Stuff Works website covers a very wide array of topics and explains the components and processes that make the topic functional: <https://www.howstuffworks.com/>.
- ◆ Significant weather events always hold the potential for law enforcement activity. Two good and slightly different sources for weather are:
  - National Weather Service: <https://www.weather.gov/>.
  - The Weather Channel: <http://www.weather.com>.
- ◆ At times, there is a need to convert U.S. dollars to a foreign currency or vice versa. To do this easily at current rates, use the currency converter: <https://www1.oanda.com/currency/converter/>.
- ◆ The need to convert information in a variety of ways often becomes essential but can be difficult. Online Conversion has made it simple by providing conversion calculators for length, temperature, speed, volume, weight, cooking, area, fuel economy, clothing, area, angles, frequency, distance, and much more: <http://www.onlineconversion.com/>.
- ◆ Real-time tracking of both commercial and private flights: <https://flightaware.com/>.

- ◆ Scalable satellite imagery—This can be used to see the layout of a target location (different sites provide slightly different satellite images):
  - Going Earth: <https://www.goingearth.com/>.
  - Google Maps: <https://www.google.com>.
- ◆ In some instances, information collected in computer files—such as images, audio, video, word processing, etc.—are in a different format that cannot be opened on law enforcement computers. These files can be converted online to a different format that can be opened on your computer: <http://media-convert.com/>.
- ◆ A wide range of unique information searches: <https://www.blackbookonline.info/>
- ◆ “Junk science” is faulty scientific data and analysis used to advance special and often hidden agendas—junk science is debunked at: <https://junkscience.com/>.
- ◆ A guide to medical quackery and health fraud: <https://quackwatch.org/>.
- ◆ Use Snap Chat Map to view snaps from all over the world by clicking on a scalable map: [https://map.snapchat.com\\_](https://map.snapchat.com_)
- ◆ Reverse phone number look-up: <https://www.usphonebook.com/>.

## CHAPTER ANNEX 12-2: THE PRE-SEARCH DEVELOPMENT PLAN

### THE PRE-SEARCH DEVELOPMENT PLAN<sup>912</sup>

1. **What UNIQUE WORDS, DISTINCTIVE NAMES, ABBREVIATIONS, or ACRONYMS are associated with your topic?**

The value of starting with these search elements is that they help define your search parameters. Be certain to include synonyms and professional terminology.

2. **Can you think of societies, organizations, or groups that might have information on your subject via their pages?**

Search these as phrases in quotes, looking for a home page that might contain links to other pages, journals, discussion groups, or databases on your subject. You may require a phrase in quotes to be in a document's title by writing **title:[no space]** before the title.

3. **What other words are likely to be in any Web documents on your topic?**

You may want to require these by joining them with **AND** or preceding each by **+ [no space]**.

4. **Do any of the words in 1, 2, or 3 belong in phrases or strings—written together in a certain order, like a cliché?**

Search these as phrases in quotes. (e.g., "world jihad" or "Aryan nation").

5. **For any of the terms in #4, can you think of synonyms, variant spellings, or equivalent terms you would also accept in relevant documents?**

You may want to allow these terms by joining them by **OR** and including each set of equivalent terms in **( )**. As an example of synonyms: "terrorists" and "jihadis." As an example of alternate spellings: "Osama" and "Usama."

6. **Can you think of any extraneous or irrelevant documents these words might pick up?**

You may want to exclude terms or phrases with **- [no space] before each term** or **AND NOT**

7. **What BROADER terms could your topic be covered by?**

When browsing subject categories or searching sites of webliographies or databases on your topic, try broader categories.

---

912 Adapted from the Regents of the University of California. Copyright 2004. All rights reserved. Created by Joe Barker, Teaching Library, University of California, Berkeley.

# CHAPTER 13

## USING FEDERAL AND NATIONAL AGENCIES AND RESOURCES TO SUPPORT THE INTELLIGENCE PROCESS AND INFORMATION SHARING



As a result of legislation, mission-related responsibilities of federal agencies guided the development of programs and products that have interstate utility. Many of these initiatives have resulted in resources and systems that support law enforcement intelligence at the state, local, and tribal levels. Some resources are designed to meet specific needs—for example, the creation of FinCEN to support financial crimes investigations. Other resources are intended to support broad law enforcement needs, such as the Federal Bureau of Investigation’s (FBI) Law Enforcement Enterprise Portal. In most cases, the resources are provided by a federal government agency (e.g., the Homeland Security Information Network). However, some resources are national and may be federally funded, but their use and/or guidance are provided by all levels of government across the country (e.g., by the High Intensity Drug Trafficking Areas or HIDTAs). The value of these diverse resources and systems to law enforcement will vary based on agency size, geographic location in the United States, and unique crime problems facing a jurisdiction.

This chapter seeks to identify resources with the greatest attention given to those that have the most value to the broadest range of law enforcement agencies. Unlike previous chapters, which sought to provide discussion of integrated issues surrounding the chapter’s topical theme, this chapter is more like a catalog. The goal is to identify the most relevant resources for state, local, and tribal law enforcement (SLTLE) agencies and provide insight with respect to what those resources or systems can provide to a law enforcement agency as well as how to use the resources, particularly with regard to sensitive information.

There are also resources available at the state and local levels. However, there was no attempt to document these because of their limited national applicability and the volume of information involved.

As will be seen, there is some overlap between resources and systems; nonetheless, exploring the materials in the following pages should provide valuable direction for the law enforcement intelligence consumer.

## WHAT IS NEEDED TO START?

From a basic perspective, certain fundamental elements need to be in place to gain access to and use many of these resources and systems. These include the following:

- ◆ Access to the Internet via a security-controlled computer(s) designated exclusively for law enforcement use (excluding undercover computers).
- ◆ The computer should have a firewall and virus and spyware protections. Operating with the use of a virtual private network (VPN) for Web-based applications is also recommended, although some websites' security protections may prohibit the connection through a VPN.
- ◆ A privacy policy should be in place that is consistent with the Global Justice Information Sharing Initiative (Global) privacy guidelines.<sup>913</sup>
- ◆ A security policy should be in place that is consistent with the Global security recommendations.<sup>914</sup>
- ◆ A fair-use operating policy for the agency's law enforcement computers may be implemented describing accepted (and prohibited) use of the law enforcement agency's computers.
- ◆ A policy should be in place to ensure accountability to monitor and supervise access external systems and resources, including stipulating the authorization process for accessing systems.

Most systems have additional requirements (including being an approved, registered user) for user access. These are simply the minimum requirements to start.

## A PERSPECTIVE ON FEDERAL LAW ENFORCEMENT INTELLIGENCE RESOURCES

Many federal agencies have reengineered their intelligence functions since the September 11, 2001 (9/11), attacks to make their intelligence products more accessible (and useful) to SLTLEs. Intelligence products have been redesigned or new products developed, dissemination methods have been revised, greater attention has been given to providing critical information that is unclassified for wide consumption by SLTLEs, and new offices and initiatives have been developed. More information is being produced and disseminated more widely than before in the history of law enforcement. Among the challenges that law enforcement now faces is accessing the needed information and using it with efficacy.

Many federal intelligence resources are in a dynamic state, responding to changes in the threat environment as well as amending policy to address these changes. As a result, it is virtually impossible to provide an exhaustive discussion of them all. This discussion, therefore, will identify those federal intelligence resources of greatest use to SLTLEs, their intelligence products, and the agencies' contact or access information. In addition, a broader discussion of the FBI and the U.S. Department of Homeland Security (DHS) than of other agencies will be provided because of their comparatively more frequent interaction with SLTLEs on intelligence matters.

While federal agencies have attempted to provide more unclassified information to America's law enforcement agencies, a significant amount of classified information remains, particularly relating to terrorism. The FBI and DHS, therefore, have made a commitment to increase security clearances for SLTLE officers. Despite this, controversies and

913 <https://it.ojp.gov/documents/d/Fusion%20Center%20Privacy%20Policy%20Development.pdf>

914 [https://it.ojp.gov/documents/Applying\\_Security\\_Practices\\_exec\\_summary.pdf](https://it.ojp.gov/documents/Applying_Security_Practices_exec_summary.pdf)

questions remain. As a result, addressing the issues of classified and sensitive information is the first place to start when discussing federal information sharing.

## CLASSIFIED INFORMATION

There is often a mystique about classified information, leading many people to say, “That’s it?” after seeing it. While there are a number of explicit elements required for information to be classified, often the distinction between classified and unclassified information with respect to the law enforcement community is that the classified information contains information about the sources and methods used in the collection of information. There are extensive rules and processes associated with all aspects of classified information. These are based on federal law and regulations that are intended to protect national security information. When this information involves domestic criminal threats, classified information becomes relevant for law enforcement.

Some of the rules governing classified information are unique to the specific missions of some federal agencies, their responsibilities, and the types of information they collect and retain. The current discussion is limited to issues and questions that typically arise about classified information as specifically related to how SLTLE agencies will most commonly interact with the classified information environment.

The federal agency responsible for managing classified information is the *Information Security Oversight Office*<sup>915</sup> (ISOO) of the *National Archives and Records Administration* (NARA). The ISOO is responsible to the President for policy and oversight of the governmentwide security classification system and the *National Industrial Security Program*. The ISOO receives its authority from:

- ◆ Executive Order 12958 “Classified National Security Information”<sup>916</sup>
- ◆ Executive Order 12829 “National Industrial Security Program”<sup>917</sup>

The classified information environment is highly controlled. For example, there are explicit categories of information which are subject to being classified (See Table 13-1). Similarly, as illustrated in Table 13-2, there are certain types of information or circumstances wherein information may *not* be classified. Despite these regulations, concerns are still expressed that the federal government tends to overclassify too much information. Overclassification is a complaint registered not only by anti-secrecy advocates<sup>918</sup> but also by law enforcement officials and members of

915 <https://www.archives.gov/isoo>

916 <https://www.archives.gov/isoo/policy-documents/cnsi-eo.html>

917 <https://www.archives.gov/isoo/oversight-groups/nisp>

918 See, for example, <https://fas.org/blogs/secrecy/2013/10/overclass/>.

## TERMS AND CONCEPTS RELATED TO CLASSIFIED INFORMATION

Agencies dealing with classified information often use the following terms and concepts as related to SLTLE:

**Tear Line or Tear Line Report:** The place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination of the information below the tear line, in accordance with the right-to-know and need-to-know principles.

**Write for Release (Write for the Consumer):** Prepare intelligence reports and products at the unclassified level to the greatest extent possible or use tear line reporting to facilitate the dissemination of releasable information to individuals who do not have a clearance.

**Markings:** Classified Information and information that has been declassified has an explicit set of comprehensive rules for the proper marking of documents to ensure that notice is given about classification and safeguarding. The extensive set of markings guidelines is available from the Office of the Director of National Intelligence in the document titled “Authorized Classification and Control Markings Register” (available on the ODNI website at [https://www.dni.gov/files/documents/FOIA/Public\\_CAPCO\\_Register%20and%20Manual%20v5.1.pdf](https://www.dni.gov/files/documents/FOIA/Public_CAPCO_Register%20and%20Manual%20v5.1.pdf)).

**Sources and Methods:** This refers to how information was obtained. “Sources” refers to who or where the information was collected (for example, a confidential informant), and “methods” refers to the means used to collect the information (for example, a wiretap).

Congress.<sup>919</sup> Suffice it to note that the issue of overclassification between federal law enforcement and SLTLE is often frustrating.<sup>920</sup>

According to Executive Order 12958,<sup>921</sup> information at the federal level may be classified at one of three levels:

- ◆ **“Top Secret”** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- ◆ **“Secret”** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- ◆ **“Confidential”** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

In addition, there are two major categories of classified information that require additional handling and access restrictions—Sensitive Compartmented Information<sup>922</sup> (SCI), which includes intelligence sources, methods, and processes, and Special Access Programs (SAPs), which are highly sensitive projects and programs (such as a prototype analytic program to monitor threats made on social media).<sup>923</sup>

TABLE 13-1: INFORMATION CATEGORIES FOR CLASSIFIED INFORMATION<sup>924</sup>

Information to be classified must fall within one or more of the following prescribed categories:

- ◆ Military plans, weapons systems, or operations
- ◆ Foreign government information
- ◆ Intelligence activities (including special activities), intelligence sources or methods, or cryptology
- ◆ Foreign relations or foreign activities of the United States, including confidential sources
- ◆ Scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism
- ◆ United States government programs for safeguarding nuclear materials or facilities
- ◆ Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
- ◆ Weapons of mass destruction

919 As a result, Congress passed and President Obama signed the “Reducing Over-Classification Act.” <https://obamawhitehouse.archives.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act>.

920 As an illustration, there have been instances in which a police department has placed information in the unclassified eGuardian system, and the information is migrated to the classified Guardian system. The police department then loses control over its own information. In another illustration, a researcher wrote a report for the FBI that was later classified, even though the report was based on research that had already been published.

921 <https://www.archives.gov/isoo/policy-documents/cnsi-eo.html> Section 1.2

922 For example, a terrorism threat to a major U.S. city is detected by the National Security Agency and is confirmed by human intelligence (HUMINT) from the source country overseas. Given the sensitivity of the sources and methods, a local investigator with a Top Secret clearance on the JTTF may not receive details of the intelligence unless given SCI access.

923 <https://fas.org/sgp/crs/secrecy/R43216.pdf>

924 <https://www.cdse.edu/documents/student-guides/IF105-guide.pdf> Section 1.4

TABLE 13-2: INFORMATION CATEGORIES PROHIBITED OR LIMITED FOR CLASSIFICATION<sup>925</sup>

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

1. Conceal violations of law, inefficiency, or administrative error;
2. Prevent embarrassment to a person, organization, or agency;
3. Restrain competition; or
4. Prevent or delay the release of information that does not require protection in the interest of national security.
  - a. Basic scientific research information not clearly related to the national security shall not be classified.
  - b. Information may not be reclassified after declassification and release to the public under proper authority.

Classified information, including databases and computer memory that contain classified information or are connected to a classified information system, must be located in a sensitive **compartmented information facility**<sup>926</sup> (**SCIF**). A SCIF is an accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures, which are explicitly stipulated in federal government regulations, prevent the free access of persons unless they have been authorized with an appropriate security clearance.

## SECURITY CLEARANCES FOR SLTLE PERSONNEL

Before any individual may be given access to classified information, he or she must first have the appropriate security clearance of Top Secret, Secret and Confidential. Beyond the clearance levels that establish a person's right to know, an individual must have the need to know the classified information. Hence just because a law enforcement employee has a security clearance does not mean that he or she will be given broad access to classified information.

Beyond access to classified information, security clearances are also often required for access to certain facilities, such as a SCIF. Similarly, there are certain intelligence training programs that require people to have a clearance before attending the training, either because of the location for the training (i.e., in a secured facility) or the content of the training.

A number of different federal agencies can authorize clearances.<sup>927</sup> The process begins with the applicant completing a comprehensive questionnaire—*Form SF-86, Questionnaire for National Security Positions*<sup>928</sup>—wherein a person must provide extensive information on his or her personal background. A federal agency uses the information on this form to conduct a comprehensive personal security investigation. (Fingerprints must also be submitted and

925 <https://www.archives.gov/isoo/policy-documents/cnsi-eo.html> Section 1.7

926 <https://www.dni.gov/files/NCSC/documents/Regulations/ICS-705-1.pdf>

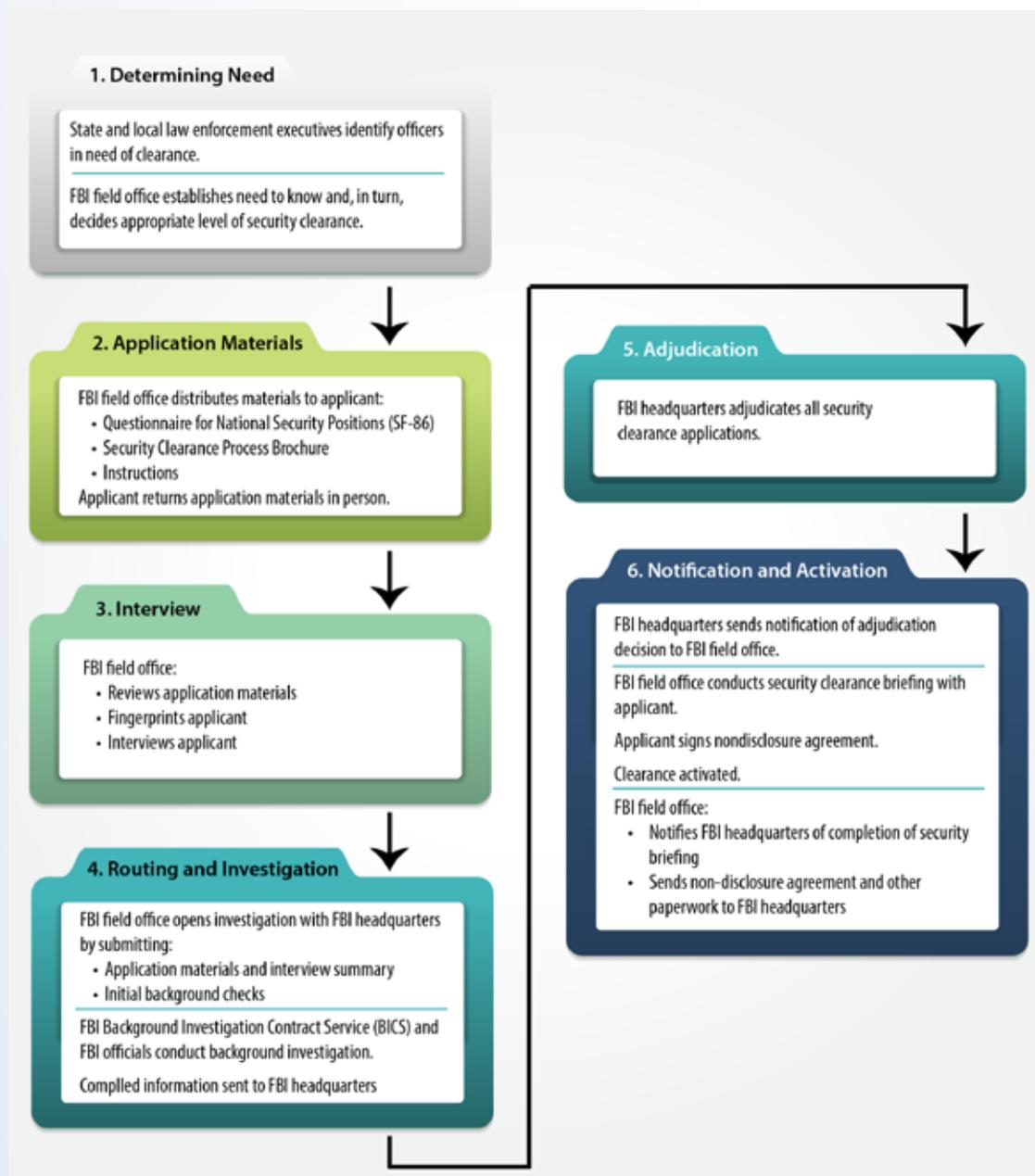
927 Ironically, security clearances are not universal. For example, a person may be an officer in the National Guard and have a Top Secret clearance from the U.S. Department of Defense, but the clearance may not automatically be recognized by a federal law enforcement agency.

928 Form SF-86 is available as a form that may be filled out on the computer from the General Services Administration at [http://www.opm.gov/Forms/pdf\\_fill/sf86.pdf](http://www.opm.gov/Forms/pdf_fill/sf86.pdf). Applicants should check with the agency from which they are seeking the clearance for special instructions. For example, the SF-86 asks for the applicant's employment history over the past seven years; however, some agencies request the employment history for the past ten years.

privacy waivers signed.) Following the investigation, the findings are “adjudicated” by a separate body that makes a determination about the issuance of a clearance. The adjudication process is an administrative examination of a sufficient period of a person’s life to make an affirmative determination that the individual, based on his or her past behavior and associations, is eligible for a security clearance. The process is the careful weighing of a number of variables. In particular, a person’s conduct is reviewed to determine that he or she has high integrity and is reliable and trustworthy. When questionable conduct is identified, the adjudication will consider such factors as:

- ◆ The nature, extent, and seriousness of the conduct.
- ◆ The circumstances surrounding the conduct, to include knowledgeable participation.
- ◆ The frequency and how recently the conduct occurred.
- ◆ The individual’s age and maturity at the time of the conduct.

FIGURE 13-1: STEPS IN THE FBI SECURITY CLEARANCE PROCESS FOR SLTLE PERSONNEL<sup>929</sup>



929 From: *Security Clearances*. (2004). GAO-04-596. Washington, DC: U.S. General Accountability Office, p. 8. <https://fas.org/sgp/gao/gao-04-596.pdf>

- ◆ The voluntariness of participation.
- ◆ The presence or absence of rehabilitation and other pertinent behavioral changes.
- ◆ The motivation for the conduct.
- ◆ The potential for pressure, coercion, exploitation, or duress.
- ◆ The likelihood of continuation or recurrence.

The factors are balanced to determine whether the clearance should be granted (basically, whether the person can be trusted not to abuse or release national security information). Once a clearance is issued, the applicant must be briefed on the regulations associated with the clearance and sign a nondisclosure agreement.<sup>930</sup>

As noted previously, different agencies issue clearances and there is some variability in processes. The most common clearances for SLTLE are from the FBI and DHS. The clearance process is labor-intensive and expensive. For these reasons, as well as operations security concerns, typically there must be a substantial reason to issue a clearance to an SLTLE employee. Moreover, conducting a large number of clearance investigations slows the process, so it takes longer to process clearances for those persons who may be in more critical positions. Hence, not all requests for clearances by SLTLE may be honored by the federal agency.

In most cases, the FBI will begin consideration of a clearance investigation for an SLTLE officer by examining local issues on a case-by-case basis.<sup>931</sup> (See Figure 13-1 for the steps in the FBI process.) For those who seek to apply for a security clearance, the appropriate forms and fingerprint cards can be obtained from the local FBI field office. Chapter Annex 12-1 describes the process for gaining a clearance and provides a list of frequently asked questions and their answers.

For some people, receiving a security clearance is viewed as achieving a form of professional status. However, for most analysts and investigators working for an SLTLE agency, a federal security clearance is not needed.

## SENSITIVE BUT UNCLASSIFIED (SBU) AND CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Dissemination refers to the types of information about threats, suspects, and indicators of criminality that a law enforcement agency or government entity wants to purposely share. However, because of the sensitivity of some information, policies have been created to protect the information from being shared with persons who do not have the right to know and need to know the information, even if it is unclassified—at least, that is the idea, but it has not been overly effective.

The management of information that is deemed “sensitive” but does not meet the requirements to be classified is going through a change at the federal level, albeit somewhat slowly. These changes are predicated by initiatives of the Information Sharing Environment to be compliant with provisions of the *Intelligence Reform and Terrorism Prevention Act*. Because a multiyear transition process is in place transitioning Sensitive But Unclassified (SBU) to Controlled Unclassified Information (CUI), a discussion of both will be provided.

---

<sup>930</sup> The general nondisclosure agreement can be found at <https://www.archives.gov/files/isoo/security-forms/sf312.pdf>.

<sup>931</sup> The FBI provides the following guidance: Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. Local FBI field offices can help determine whether or not a security clearance is needed, and, if so, what level is appropriate. <https://www.fbi.gov/resources/law-enforcement/security-clearances-for-law-enforcement>

## SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION

Since it is not feasible (or necessary) for every law enforcement officer to have a security clearance and not all information meets the standards for classification, there is a mechanism to get critical information into the hands of officers that does not involve the classified information framework. The traditional approach has been to use various document markings or labels that designate the information as some form of “Sensitive But Unclassified” information. A variety of SBU labels are placed on intelligence products and other information by the originator of the information to indicate that it should not be broadly shared—dissemination is intended to only those persons indicated by the SBU label.

There are no statutory mandates for designating information as SBU—rather, agencies have developed policies and practices to identify and designate SBU information, and these processes have generally been adopted by agencies at all levels of government by policy.<sup>932</sup> Generally, this unclassified information is withheld from the public for a variety of reasons, but it needs to be accessible to law enforcement and other persons who have the right to know and need to know the information (for example, a potential threat on social media about violence at a school would require this sensitive information to be shared with school officials). Agencies have discretion to define SBU in ways that serve their particular needs to safeguard information. Since there is little uniformity in implementing rules throughout the various levels of government on the use of SBU, the specific applications of the markings may vary between agencies.<sup>933</sup> There is an intuitive understanding but no formal process to control the information. Some guidance has been provided by DHS, which issued a directive for safeguarding “For Official Use Only” (FOUO) information.<sup>934</sup> Recognize, however, that this is policy and does not carry the force of law as classified information does.

**“For Official Use Only” (FOUO) Information.** The FOUO label is used within DHS “. . .to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of a federal program, or other programs or operations essential to the national interest.”<sup>935</sup> FOUO is not classified information, but information that should be distributed only to persons who need to know the information to be aware of conditions that will help keep the homeland and, hence, the community, secure. Within DHS, the caveat “For Official Use Only” will be used to identify SBU information within the DHS community that is not otherwise governed by statute or regulation. In sum, FOUO information may be shared with *anyone* who has the right to know and need to know the information in the report or product.

**“Law Enforcement Sensitive” (LES) Information.** The second most common SBU label is “Law Enforcement Sensitive.” This label is more restrictive than FOUO because it is intended to limit dissemination to anyone (sworn or nonsworn) in the law enforcement community who has the right to know and the need to know the information. Hence, the additional qualifier was that the recipient had to be a law enforcement employee. One of the reasons for the distinction was that some information containing personally identifiable information (PII) had to stay within the law enforcement community as precautions relating to civil rights and privacy.

---

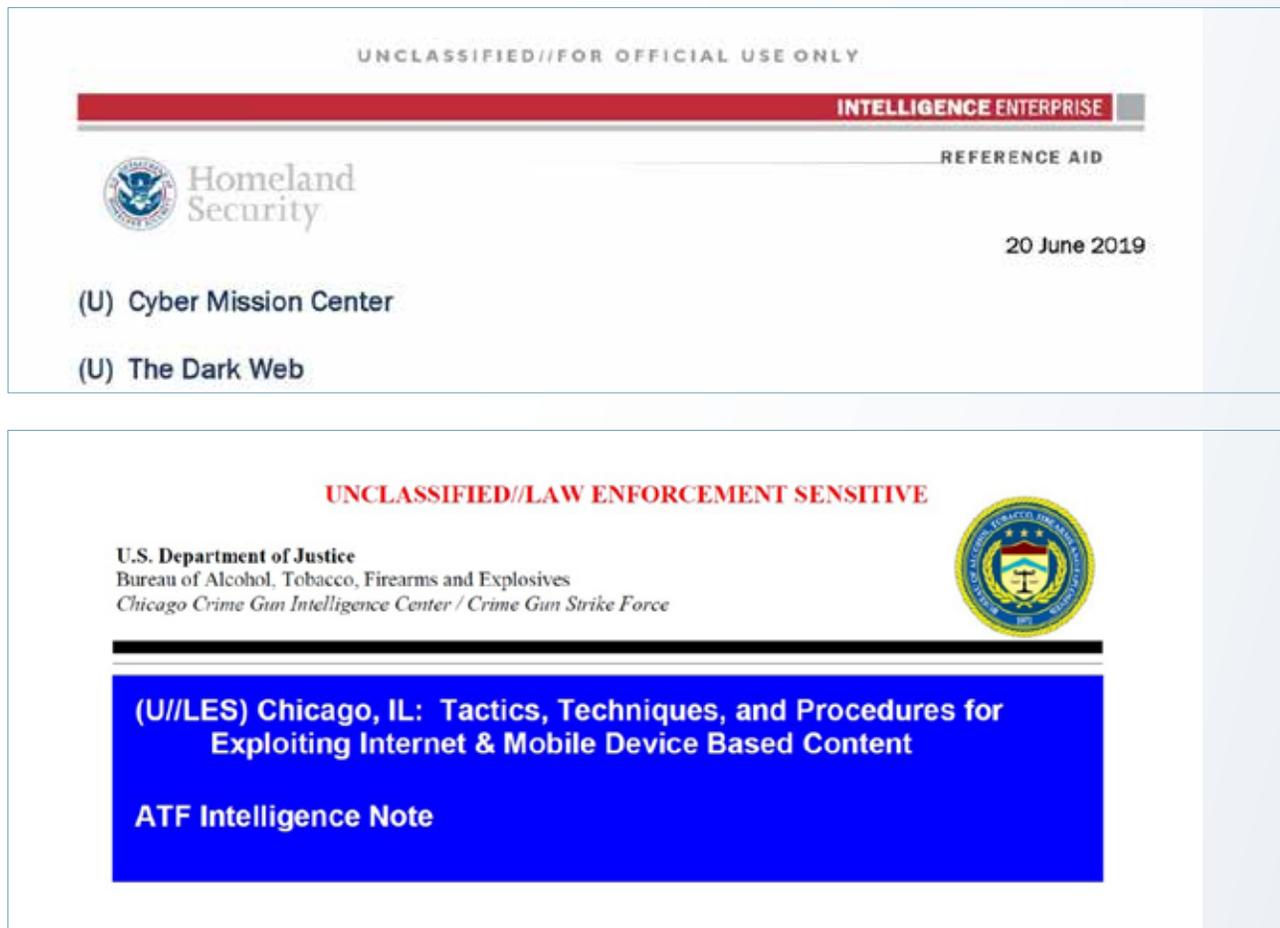
932 Just as there has been overclassification of national security information, there has been overlabeling of information designated as SBU. Some intelligence units, for example, label all of their products, even though the information may already be in the public domain. In reality, these practices tend to devalue the intent of the label.

933 For a detailed review of the SBU meaning and how it is defined and used by different statutes and regulations, see Knezo, G. J. (2006). *“Sensitive But Unclassified” and Other Federal Security Controls on Scientific and Technical Information*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/secretcy/RL33303.pdf>

934 [https://www.dhs.gov/xlibrary/assets/foia/mgmt\\_directive\\_110421\\_safeguarding\\_sensitive\\_but\\_unclassified\\_information.pdf](https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf)

935 Department of Homeland Security, Management Directive System, MD Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*. May 11, 2004.

FIGURE 13-2: ILLUSTRATIONS OF FOUO DOCUMENT MARKINGS



While these descriptions reflect the intent of the FOUO and LES labels—and because there are no national standards or any national policies on the explicit types of information that is deemed SBU—individual agencies at all levels of government began making their own rules and adaptations of rules as they labeled SBU information. For example, some agencies have used both the FOUO and LES dissemination labels on a document—this basically eliminates the original distinctions between the labels.

There are no sanctions if SBU information is widely distributed, including to the media, and no guidelines to ensure that the information is secured. In many ways, particularly for SLTLE agencies, SBU markings reflected a professional agreement to limit the dissemination of certain types of information.

There is a federal effort under way that seeks to standardize the identification, labeling and dissemination of SBU information by using a system called *Controlled Unclassified Information*. While designed to be applicable to federal agencies, SLTLE agencies could choose to adopt the process, since here are no statutory restrictions or mandates as there is with classified information.

## CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Among the mandates of *the Intelligence Reform and Terrorism Prevention Act of 2004* was to develop policies and practices that enhance the ability of rapid information sharing among the Intelligence Community (IC), law enforcement, the private sector, and foreign partners. One of the information sharing obstacles was the lack of consistency in policies regulating SBU information. At the federal level alone, the Program Manager for the

Information Sharing Environment observed:

Among the twenty departments and agencies we have surveyed, there are at least 107 unique markings and more than 131 different labeling or handling processes and procedures for SBU/CUI information. Even when SBU information carries the same label marking (e.g., For Official Use Only), storage and dissemination are inconsistent across Federal agencies and departments. Because such markings are agency-specific, recipients of SBU information in a different agency must understand the processes and procedures of the originating Federal agency for handling the information, even if their agency uses the same marking. The result is an unmanageable collection of policies that leave both the producers and users of SBU information unable to know how a piece of information will be controlled as it moves through the Federal government and therefore reducing information sharing.<sup>936</sup>

Established by Executive Order 13556, the *Controlled Unclassified Information* program standardizes the way the Executive Branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with regulations and governmentwide policies. The policies set forth in the Presidential Memorandum for the designation, marking, safeguarding, and dissemination of CUI are mandatory for all CUI originated by the Executive Branch of the federal government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal.

It is important to note that the Presidential Memorandum also encourages the adoption of the CUI Framework by state, local, tribal, and private sector entities. Frequent consultations with individuals and organizations from these entities during the development of this framework suggest that there is some support for moving in the direction of a common, or mostly common, CUI framework. As necessary, departments and agencies may agree with foreign partners to ensure that they protect shared CUI in “a like manner,” similar to what is now done for sharing classified information. Of course, this provision only applies to the federal government, not SLTLE.

The National Archives and Records Administration (NARA) is responsible for administering all policies and regulations associated with the CUI framework.<sup>937</sup> Once fully implemented, this framework is intended to end confusion about proper access, handling, and control of unclassified information that needs protection. Moreover, the new system will instill confidence that identical rules apply to everyone using the CUI markings and provide clear guidance to SLTLE partners that are now confused about SBU markings with respect to safeguarding and disseminating the sensitive information.<sup>938</sup>

FIGURE 13-3: ILLUSTRATION OF THE CUI MARKING



## SUMMARY

To be clear, there are federal laws and rigorous processes for designating classified information, authorizing access to classified information, and transmitting and storing classified information. A person violating any of the classified information requirements may be disciplined, terminated, or even criminally prosecuted.

Conversely, unclassified information that is marked as FOUO, LES, or CUI has no legal implications for its marking,

storage, transmission, or release. Essentially, the markings are largely advisory as determined by the originator of the information.

<sup>936</sup> McNamara, T. (April 26, 2007). Statement for the Record before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Committee on Homeland Security.

<sup>937</sup> <https://www.archives.gov/cui>

<sup>938</sup> McNamara, T. E. (2008). *Annual Report to the Congress*, op cit., p. 36.

Since SLTLE agencies will encounter these labels when receiving federal intelligence products, it is useful to know the framework from which they arise. At a practical level, the rule of thumb for law enforcement officers is to use good judgment when handling such materials. This does not mean that SLTLE officers may not disseminate this information further unless prohibited from doing so as indicated on the document. Rather, officers should use the information in a manner that meets community safety needs, including disseminating portions of the information to those segments of the community that would benefit from the information contained in the report.

Despite the caveats of SBU/CUI marked information, the materials often find their way to the news media or websites<sup>939</sup> where they may be viewed by the public.

## FEDERAL AND NATIONAL INTELLIGENCE RESOURCES

There are a number of federal agencies and initiatives that provide support, information sharing, and resources to SLTLE to aid in the intelligence process and investigations. Many of these have a focus on international terrorism because of statutory mandates and limitations. However, change is occurring with an increasing focus on domestic terrorism (notably right-wing extremism) as well as targeted violence. The other noted area of federal concentration is in illicit drug trafficking and crimes associated with national and international drug trafficking organizations (DTOs), such as money laundering. Other growing areas of federal involvement are in human trafficking and cybercrimes. While the primary focus of federal agencies and resources remains federal crimes and national security, there has been a notable increase of cooperation and resources for SLTLE agencies. While many federal resources and sources of information are available to law enforcement, the best way to maximize access and use of them is through the primary state fusion centers. While the line between the IC and domestic law enforcement remains intact, new lawful avenues have also been developed for information sharing in cases that serve the needs of both. The following discussion identifies these entities and provides a summary discussion of the responsibilities and services.

Of the wide range of information systems available to law enforcement agencies to aid the intelligence function, some are specifically for intelligence purposes, while others have a much broader purpose but have applications for intelligence. Resources and information systems were designed for diverse purposes; hence a brief understanding of these purposes can provide insight about their use and applicability.

For clarity, some of the resources are federal, meaning they are provided as part of the mission of a federal agency. Yet other resources are national, which means they provide services and resources to state, local, and tribal law enforcement on a nationwide basis. Although a national organization may not be a federal agency, in most cases, the agency receives federal funding to provide its service.

As a place to begin, resources and systems may be described in six broad categories. Information found in some of the categories overlaps a resource in another category. The intent of this typology is to help provide a perspective of the different types of resources and systems that are available for state, local, and tribal law enforcement.<sup>940</sup>

1. **Situational awareness**—Documents and technologies that provide information on threats, incidents, indicators and other short-term or real-time information needed for planning or operational responses.
2. **Public records**—Depending on statutes and policies, various types of information collected or recorded by diverse public agencies may be available. Land transactions, driving records, registered sexual offenders, addresses, phone numbers, and all types of licenses are illustrations.

---

939 As an example, see <https://publicintelligence.net/>.

940 Based on: Shaw, L. (Inspector, Florida Department of Law Enforcement.) (July 2008). *Information Systems and Technologies*. Presentation at the BJA-Funded Intelligence Commanders' Course, Norwalk, CA.

3. **Criminal justice**—Whenever anyone has an encounter with the criminal justice system, it is going to be in a record. Computer-aided dispatch calls, arrest records, field interview reports, court records, probation and parole records, and institutional corrections records are examples.
4. **Intelligence**—Any records system or network that is explicitly designated to handle intelligence, such as RISSNET, Law Enforcement Online, and the Homeland Security Data Network. (While many of the networks are not exclusively for intelligence, they all contain intelligence products.)
5. **Resource and communications systems**—A number of systems that have emerged post-9/11 are explicitly designed to provide diverse types of intelligence resources and/or provide secure e-mail communications for SLTLE. Examples are the National Criminal Intelligence Resource Center, the Law Enforcement Enterprise Portal, and the Homeland Security Information Network.
6. **Open sources**—The previous chapter comprehensively addressed open source information as publicly available information that anyone can lawfully obtain by request, purchase, or observation.

There are many information systems that can potentially provide support to the law enforcement intelligence function; it is not feasible to include them all here. This is particularly true when one considers state and local systems that are in use. Rather, the goal is to provide a snapshot of those systems that SLTLE officers across the United States are most likely to encounter as well as a brief listing of other federal intelligence information systems that SLTLE personnel may occasionally encounter. The goal of this discussion is to develop an awareness of the systems and resources. In many cases, the information from the resources and systems in the following discussions will not be classified but will be SBU/CUI. In all cases, the sensitivity of the information and appropriate safeguarding of the information will be clearly marked.

## DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INTELLIGENCE AND ANALYSIS (DHS I&A)

I&A's<sup>941</sup> staff of intelligence analysts and other professionals are responsible for providing relationship building and intelligence and information sharing across the range of DHS components, federal partners, fusion centers, law enforcement agencies, and, as applicable, to the private sector. The office also provides information collection, intelligence analysis, and reporting in support of SLTLE partners, the DHS Intelligence Enterprise (IE), the IC, and other homeland security partners to ensure a homeland that is safe, secure, and resilient against terrorism and other threats.

I&A field personnel are responsible for three primary functions:

- ◆ Lead, manage, or support intelligence cycle execution in their areas of responsibility (AORs) and in concert with I&A, SLTLE, DHS IE, or other homeland security partners as appropriate.
- ◆ Lead, manage, or support threat-related information sharing to and from SLTE, DHS IE, and the IC to inform the national threat picture.
- ◆ Support state and major urban area partners in developing, maintaining, and applying IC tradecraft skills, tools, and resources necessary to effectively execute the intelligence cycle.

**DHS I&A Partner Engagement<sup>942</sup> (PE).** The office manages strategic relationships with key partners across federal, state, local, tribal, territorial, and private sector stakeholders. I&A PE systematically establishes and leverages these partnerships to facilitate multidirectional intelligence and information sharing; collaborates with key partners to build mutually beneficial relationships; facilitates the identification of partner requirements and needs; facilitates partner access to I&A products and resources; and advocates partner equities across I&A in support of their respective

941 <https://www.dhs.gov/office-intelligence-and-analysis>

942 <https://www.dhs.gov/office-intelligence-and-analysis-partner-engagement>

homeland security missions. Essentially, partner engagement reflects the processes that DHS uses for outreach and cooperative working relationships.

**Homeland Security Information Network (HSIN).** HSIN<sup>943</sup> is DHS's official system for trusted sharing of Sensitive But Unclassified information among federal, state, local, territorial, tribal, international, and private sector partners. Mission operators use HSIN to access homeland security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe. Homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and, in general, share the information they need to do their jobs.

- ◆ **HSIN-Intel**—Facilitates the sharing, dissemination, and notification of key Sensitive But Unclassified intelligence information among federal, state, local, and tribal stakeholders supporting the DHS Office of Intelligence and Analysis.
- ◆ **HSIN Exchange**—A centralized request for information (RFI) management system serving analysts and professionals working in analytic and information sharing entities, fusion centers, federal agencies, and the broader Homeland Security Enterprise.
- ◆ **HSIN SitRoom and CINAware**—Provides 24/7 virtual Adobe Connect room to exchange critical information during a physical crisis (SitRoom) or cybercrisis (CINAware).
- ◆ **HSIN-Intel Planned Production Tool**—Provides a location for analysts to deconflict and collaborate on planned intelligence products.

## FEDERAL BUREAU OF INVESTIGATION (FBI) INTELLIGENCE INITIATIVES

The FBI<sup>944</sup> has 56 field offices (also called divisions) with 380 resident agencies located in smaller cities and towns across the United States. The bureau also has 64 legal attaché offices—commonly known as “legats”—and more than a dozen smaller suboffices in key cities around the globe, providing coverage for more than 200 countries, territories, and islands. The expressed priorities of the FBI are to:

- ◆ Protect the United States from terrorist attack.
- ◆ Protect the United States against foreign intelligence operations and espionage.
- ◆ Protect the United States against cyber-based attacks and high-technology crimes.
- ◆ Combat public corruption at all levels.
- ◆ Protect civil rights.
- ◆ Combat transnational/national criminal organizations and enterprises.
- ◆ Combat major white-collar crime.
- ◆ Combat significant violent crime.

**FBI Office of Partner Engagement<sup>945</sup> (OPE).** Much like DHS, the FBI engages partners through offices and programs that strengthen the quality of their working relationships with law enforcement agencies to maximize information sharing and intelligence/investigative support at all levels of government. The goal is to have clear processes and substantive operational relationships to maximize the quality of their engagement. The FBI's Office of Partner Engagement builds bridges, creates new partnerships, and strengthens and supports relationships between the FBI and other federal agencies, as well as with state, local, tribal, and campus law enforcement; national and international law enforcement associations; and others within the broad public safety, law enforcement, and homeland security

943 <https://www.dhs.gov/homeland-security-information-network-hsin>

944 <https://www.fbi.gov/>

945 <https://www.fbi.gov/about/partnerships/office-of-partner-engagement>

communities. As part of the Intelligence Branch,<sup>946</sup> the OPE serves as the FBI's primary liaison for the law enforcement community, representing the perspectives of chiefs, sheriffs, and law enforcement associations within the FBI.

The OPE also manages outreach programs, including FBI support to state and local fusion centers, along with the Countering Violent Extremism, Active Shooter, and Police Executive Fellowship programs. The office implements national-level initiatives and strategies that support engagement, communication, coordination, and cooperation efforts with law enforcement, intelligence, and public agencies and partners in a continuous effort to enhance the FBI's capabilities.

The **Enhanced Engagement Initiative** of the OPE represented several specific assignments or practices to enhance partner relationships primarily for terrorism prevention and investigations. These include:

- ◆ **Integration:** FBI personnel embedded full-time at the fusion center.
- ◆ **Clearances and Access:** Co-location of personnel and systems in field offices and fusion centers.
- ◆ **Joint Terrorism Task Force (JTTF) Participation and Coordination:** Fusion center leadership, the Homeland Security Advisor, and other relevant partners are members of and participate in the JTTF Executive Board.
- ◆ **Suspicious Activity Reporting:** Development of fusion center policy/standard process detailing how SAR information is managed and evaluated.
- ◆ **Guardian threats:** When feasible, JTTF investigations are assigned to task force officers (TFOs) whose home agencies have a connection to the Guardian (the FBI's classified information system).
- ◆ **Intelligence analysis, production, and dissemination:** Fusion centers provide tailored, timely, and relevant intelligence products to their law enforcement, public safety, private sector, and designated community partners.
- ◆ **Special event and critical incident coordination:** Special events are worked collaboratively with regular meetings, updates, and Guardian reviews leading up to and through events.
- ◆ **Threat Review and Prioritization (TRP) Process:** Fusion center and other relevant partners (JTTF Executive Board members, DHS, NCTC, U.S. Attorney's Office) participate in appropriate TRP meetings.

**Emerging Threat and Incident Notifications Processes.** The FBI and DHS provide state and local partners with a general overview of actions they may take in response to specific/credible threats and/or critical incidents associated with international or domestic terrorism, significant criminal activity, or cybersecurity.

Within 6 to 8 hours of a critical incident, the FBI and DHS I&A will initiate communications to coordinate and deconflict outreach and engagement with appropriate partners. Within 8 to 12 hours of a critical incident, DHS I&A and the FBI will provide state and local partners with an alert/notification of the issue at hand and an estimated communications plan, including any planned calls. The communications will allow state and local partners to anticipate further outreach and engagement from DHS I&A and the FBI. If the incident appears likely to be ongoing, a conference call or secure video teleconference (SVTC) is scheduled. Issues discussed during the conference call will include information about such issues as:

- ◆ The status of the current threat or incident reporting.
- ◆ Intelligence gaps and information needs.
- ◆ Immediate operational actions and updates (e.g., enhanced screening at select ports of entry).
- ◆ Information that can and should be shared with elected officials and the public.
- ◆ Potential preventive and protective actions that can be taken by state and local partners.

946 <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch>

- ◆ Placeholders for any anticipated conference calls or SVTCs.
- ◆ Currently planned intelligence production schedules, associated timelines, distribution mechanisms, and distribution restrictions.

Following a critical incident, DHS I&A will utilize the National Situation Room (SitRoom), a HSIN Connect session (essentially a video conference over the Homeland Security Information Network), to facilitate real-time, incident-specific information sharing and related requests for information (RFIs) among federal, state, and local partners. Pertinent intelligence products will be shared with partners via the Homeland Security Information Network's Intelligence Community of Interest (HSIN-Intel). Subsequent updates to production schedules, associated timelines, and other messaging will be provided at regular, announced intervals as needed, depending on the nature of the threat or updates or changes in available information.

**Terrorist Screening Center (TSC).** The Terrorist Screening Center,<sup>947</sup> established in 2003, is a multiagency center administered by the FBI. The TSC is the U.S. government's consolidated counterterrorism watchlist and is responsible for the management and operation of the Terrorist Screening Database, commonly known as "the watchlist."

The TSC watchlist is connected to the National Crime Information Center (NCIC) and will create alerts when a known or suspected terrorist (KST) has his or her name checked in the system by law enforcement across the country, at border entry points, or after having made flight reservations; is an applicant for government positions; or purchases firearms.

**National Domestic Communications Assistance Center (NDCAC).** Law enforcement uses a variety of communications surveillance techniques. Live or real-time surveillance allows law enforcement to capture information while it is being transmitted. There is also stored information, such as email or communications transaction logs, which may be from an Internet service provider or wireless provider. Many of the technologies are sophisticated and most require work with the private sector. The National Domestic Communications Assistance Center<sup>948</sup> was established in 2013 and designed as a resource to enhance law enforcement's ability to lawfully collect and analyze this array of communications data. NDCAC is a hub for technical knowledge management that facilitates the sharing of solutions and know-how among law enforcement agencies, as well as strengthening law enforcement's relationships with the communications industry. The center shares collective technical knowledge and resources with law enforcement on issues involving real-time and stored communications to address challenges posed by advanced communications services and technologies. NDCAC is not an operational organization but a technical knowledge and referrals clearinghouse that responds to requests for assistance from any member of the law enforcement community related to law enforcement coordination of technology use, industry relations, technology sharing, and assistance in implementing requirements of the Communications Assistance for Law Enforcement Act<sup>949</sup> (CALEA).

**Law Enforcement Enterprise Portal (LEEP).** The FBI's Law Enforcement Enterprise Portal<sup>950</sup> (LEEP) is a gateway that provides law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources that can strengthen case development for investigators, enhance information sharing between agencies, be accessible in one centralized location, and provide a portal that affords admission to a host of information systems such as real-time event collaboration and management tools, nationwide criminal justice records, and counterterrorism threat tracking. Among the applications on LEEP are:

- ◆ **JusticeConnect**—An online collaboration service accessible via LEEP. Through online forums and blogs, partners can communicate with experts, share information and ideas, and receive feedback with criminal investigations.

947 <https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc>

948 <https://ndcac.fbi.gov/>

949 <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>

950 <https://www.fbi.gov/services/cjis/leep>

- ◆ **Active Shooter**—An outgrowth of a White House initiative to assist law enforcement and first responders, the FBI Active Shooter Resources library contains valuable resources to aid in the management of the chaos often surrounding active shooter/multiple-victim incidents.
- ◆ **Intelink**—A secure portal for integrated intelligence dissemination and collaboration efforts.
- ◆ **Internet Crime Complaint Center (IC3)**—The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.
- ◆ **Malware Investigator**—Malware Investigator is a tool that provides users with the ability to submit suspected malware files and, within as little as an hour, receive detailed technical information about what the malware does and what it may be targeting.
- ◆ **Repository for Individuals of Special Concern (RISC)**—This tool allows officers on the street to use a mobile identification device to perform a rapid search of a limited repository of fingerprint records. It provides law enforcement with an enhanced capability to quickly identify persons who present special risks to the public or to law enforcement officers themselves. Specifically, this capability enables officers and agents in the field to screen detainees and criminal suspects against a repository of wanted persons, sex offenders, registry subjects, known or suspected terrorists, and other persons of special interest for rapid identification. The handheld identification devices can be used nationwide and decrease risk to officers dealing with subjects presenting false or no identification. The matching process is entirely automated, enabling an officer to receive a response within seconds.

**FBI Violent Criminal Apprehension Program (ViCAP).** This program is part of the FBI’s National Center for the Analysis of Violent Crime (NCAVC). The mission of the ViCAP is to assist law enforcement agencies across the country and around the world in identifying and apprehending violent criminals. Initially created to study the behavior of serial killers and rapists, ViCAP has grown to include solved and unsolved homicides, kidnappings, missing persons, sexual assaults, and unidentified persons. ViCAP-Web, the nation’s largest repository of criminal cases that involved violence. In 2008, the FBI granted access to ViCAP-Web to all authorized law enforcement agencies at the national, state, and local levels, further enabling closer collaboration and cooperation among these organizations. While not an intelligence-related program, per se, its use as a tool to link death investigations, possibly identifying murders that involve the same suspect, can provide value to the intelligence process.

**FBI National Data Exchange (N-DEx).** The N-DEx system is an unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records. N-DEx is also a strategic investigative information sharing system that fills information gaps and provides situational awareness. Essentially, the system is designed to provide SLTLE agencies with a tool to collect, process, and disseminate criminal and investigative data to be used as a pointer system for nationwide information sharing. The N-DEx system complements other well-known FBI systems, such as the National Crime Information Center (NCIC), Interstate Identification Index (III), and Next Generation Identification (NGI), which provide critical information to the criminal justice community. The information that would not be contained in the other systems—i.e., incident and case reports, full U.S. Department of Justice (DOJ) case files, and corrections data—is available in N-DEx.

- ◆ Available 24/7 from any secure Internet-capable device.
- ◆ Data covers the entire life cycle, from initial contact to release from prison, to include:
  - Incidents
  - Arrests
  - Bookings

- Holdings
- Federal case reports
- Incarcerations
- Probation
- Parole
- Warrant investigations
- Service calls

**eGuardian.** The eGuardian<sup>951</sup> system was developed to help meet the challenges of collecting and sharing information on potential terrorism-related activities among law enforcement agencies across various jurisdictions. The eGuardian system is a Sensitive But Unclassified information-sharing platform hosted by the FBI's Criminal Justice Information Services (CJIS) Division as a service on the Law Enforcement Enterprise Portal.

The eGuardian system allows law enforcement agencies to combine new suspicious activity reports (SARs) of incidents such as these with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel and analysts directly supporting law enforcement. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force for any further investigative action.

## DRUG ENFORCEMENT ADMINISTRATION (DEA)

Through its 221 domestic offices in 21 divisions throughout the United States and its 90 foreign offices in 69 countries, the Drug Enforcement Administration's (DEA) mission is to enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support nonenforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets. In carrying out its mission as the agency responsible for enforcing the controlled substances laws and regulations of the United States, the DEA's primary responsibilities include:

- ◆ Investigation and preparation for the prosecution of major violators of controlled substance laws operating at interstate and international levels.
- ◆ Investigation and preparation for prosecution of criminals and drug gangs that perpetrate violence in our communities and terrorize citizens through fear and intimidation.
- ◆ Management of a national drug intelligence program in cooperation with federal, state, local, and foreign officials to collect, analyze, and disseminate strategic and operational drug intelligence information.
- ◆ Seizure and forfeiture of assets derived from, traceable to, or intended to be used for illicit drug trafficking.
- ◆ Enforcement of the provisions of the Controlled Substances Act as they pertain to the manufacture, distribution, and dispensing of legally produced controlled substances.
- ◆ Coordination and cooperation with federal, state, and local law enforcement officials on mutual drug enforcement efforts and enhancement of such efforts through exploitation of potential interstate and international investigations beyond local or limited federal jurisdictions and resources.
- ◆ Coordination and cooperation with federal, state, and local agencies, and with foreign governments, in programs designed to reduce the availability of illicit abuse-type drugs on the United States market through nonenforcement methods such as crop eradication, crop substitution, and training of foreign officials.

951 <https://www.fbi.gov/resources/law-enforcement/eguardian>

- ◆ Responsibility, under the policy guidance of the Secretary of State and U.S. Ambassadors, for all programs associated with drug law enforcement counterparts in foreign countries.
- ◆ Liaison with the United Nations, INTERPOL, and other organizations on matters relating to international drug control programs.

**DEA Intelligence.**<sup>952</sup> DEA, in coordination with other federal, state, local, and foreign law enforcement organizations, has been responsible for the collection, analysis, and dissemination of drug-related intelligence. The role of intelligence in drug law enforcement is critical. The DEA Intelligence Program helps initiate new investigations of major drug organizations, strengthens ongoing ones and subsequent prosecutions, develops information that leads to seizures and arrests, and provides policymakers with drug trend information upon which programmatic decisions can be based. DEA is recognized for its significantly robust global intelligence operations and its willingness to work closely with and share intelligence with SLTLE. DEA divides intelligence into three broad categories:

- ◆ **Tactical intelligence** is evaluated information on which immediate enforcement action—arrests, seizures, and interdictions—can be based.
- ◆ **Investigative intelligence** provides analytical support to investigations and prosecutions to dismantle criminal organizations and gain resources.
- ◆ **Strategic intelligence** focuses on the current picture of drug trafficking from cultivation to distribution that can be used for management decision making, resource deployment, and policy planning.

DEA also manages the El Paso Intelligence Center<sup>953</sup> (EPIC), which was originally created to monitor drug trafficking threats along the Southwest border but has evolved to include all threats to the United States in the Western Hemisphere. EPIC offers tactical, operational, and strategic intelligence support to federal, state, local, tribal, and international law enforcement organizations.

Also, part of the intelligence division is a Web-based case pointer system called the *National Drug Pointer Index* (NDPIX), which is integrated with the Nationwide Deconfliction System. The purpose of the system is to assist federal, state, and local law enforcement agencies investigating drug trafficking organizations (DTOs) and to enhance officer safety by preventing duplicate investigations. Recognizing that the development of this system would require a truly cooperative effort, the DEA drew from the experience of state and local agencies not only to make certain that their concerns were addressed, but also to ensure that they had unrestricted input and involvement in the pointer system's development.

**Organized Crime Drug Enforcement Task Force<sup>954</sup> (OCDETF).** The Organized Crime Drug Enforcement Task Force (OCDETF) Program was established in 1982 to mount a comprehensive attack against and reduce the supply of illegal drugs in the United States and diminish violence and other criminal activity associated with the drug trade. OCDETF is headquartered in Washington, DC, but operates nationwide and combines the resources and the expertise of the DEA and numerous federal agencies to target drug trafficking and money laundering organizations. The DEA has been a decades-long partner with OCDETF. Since its inception, tens of thousands of arrests have been made, and hundreds of tons of narcotics and billions in currency, real property, and conveyances have been seized. In OCDETF's coordinated attack against drug trafficking and money laundering organizations, OCDETF formulated the Consolidated Priority Organization Target (CPOT) list. The CPOT list is a multiagency target list of command-and-control elements of the most prolific international drug trafficking and money-laundering organizations. Through the combined efforts of DEA and other law enforcement agencies under the OCDETF umbrella, CPOTs are targeted with the goal of disrupting or dismantling their operations.

952 <https://www.dea.gov/intelligence>

953 <https://www.dea.gov/el-paso-intelligence-center-epic>

954 <https://www.dea.gov/organized-crime-drug-enforcement-task-force-ocdetf>

## BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (ATF)

ATF<sup>955</sup> has a key responsibility of disrupting the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism, and the illegal diversion of alcohol and tobacco products. The agency proactively partners with communities, industries, law enforcement, and public safety agencies to safeguard the public through investigations, intelligence, information sharing, training, research, and use of technology.

**The Office of Strategic Intelligence and Information** focuses on gathering and assembling information on major complex, conspiratorial-type (multidefendant) investigations of such targets as firearms and narcotics trafficking organizations, arson rings, traditional and nontraditional organized crime groups, and equivalent criminal conspiracies. In doing so, it applies the principles and techniques of inductive and deductive reasoning and the knowledge of either a geographical area or a functional area to produce finished intelligence products. Intelligence research specialists interpret and project existing data to fill gaps in information and review and evaluate finished intelligence reports from the point of view of their specific subject-matter field(s). ATF has historically had a strong relationship with SLTLE for both information sharing and joint investigations.

As noted in Chapter 1, ATF has also been the leader in developing Crime Gun Intelligence Centers,<sup>956</sup> which are designed to disrupt the shooting cycle by using forensic science and data analysis to identify, investigate, and prosecute shooters and their sources of crime guns.

## OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

The core mission of the ODNI<sup>957</sup> is to lead the IC in intelligence integration, forging a community that delivers the most insightful intelligence possible. That means effectively operating as one team: synchronizing collection, analysis, and counterintelligence so that they are fused. This integration is the key to ensuring that national policymakers receive timely and accurate analysis from the IC to make educated decisions. Despite the ODNI's role in the IC, there are also programs and relationships relevant to SLTLE intelligence, notably as related to counterterrorism.

The ODNI has two field-based programs focused on the sharing of counterterrorism information, including fusion centers.

- ◆ Domestic DNI Representative (DDNIR), wherein FBI executives from 12 regions around the country serve as DNI representatives to help facilitate the coordination of IC resources within their assigned regions.
- ◆ National Counterterrorism Center<sup>958</sup> (NCTC) Domestic Representative program, wherein NCTC representatives are assigned to 12 regions to support counterterrorism information sharing and connectivity to the NCTC.

**National Security Partnerships, Federal, State, Local Tribal Information Sharing (FSLT-IS), formerly Partner Engagement—Information Sharing Environment (PE-ISE).** Established in 2004 by the Intelligence Reform and Terrorism Prevention Act (IRTPA) as the Program Manager—Information Sharing Environment (PM-ISE), the PE-ISE is granted the authority to plan, oversee, and manage the Information Sharing Environment to ensure access to all information in the ISE by all information sharing partners as permitted by law. Partners include the IC, law enforcement at all levels of government, and the private sector, notably critical infrastructure. Most importantly for SLTLE, the PE-ISE provides guidance for connectivity of intelligence systems and databases and guidelines for information sharing that ensure confidentiality, security, and the protection of privacy and civil rights.

---

955 <https://www.atf.gov/>

956 <https://www.atf.gov/resource-center/fact-sheet/fact-sheet-crime-gun-intelligence-centers-cgic>

957 <https://www.odni.gov/index.php/who-we-are/mission-vision>

958 <https://www.odni.gov/index.php/nctc-home>

One of the factors affecting the development of a “domestic approach to national intelligence”<sup>959</sup> was a recognition that SLTLE agencies make critical contributions to the security of the United States. With this recognition of state and local law enforcement and a need for vertical integration of information sharing, the DNI created the Homeland Security and Law Enforcement Partners Board. This group of nonfederal leaders assists the DNI in understanding the responsibilities, requirements, and capabilities of the law enforcement and homeland security communities, especially at the state, local, and tribal levels of government.

**National Counterterrorism Center<sup>960</sup> (NCTC).** The center was established in 2003 as the Terrorism Threat Integration Center (TTIC) and in 2004 was renamed the National Counter Terrorism Center under the ODNI. NCTC provides analysis, maintains the authoritative database of known and suspected terrorists, shares information, and conducts strategic counterterrorism operational planning. Among the center’s many responsibilities is operating a secure website, NCTC CURRENT, which serves as a dissemination mechanism for terrorism information produced by NCTC and other counterterrorism mission partners. NCTC CURRENT is directly available to a broad audience to include U.S. government partners with an operational focus, such as the FBI’s Joint Terrorism Task Forces. As such, state and local law enforcement officers assigned to a JTTF have access to threat information directed toward their communities.

**Joint Counterterrorism Assessment Team<sup>961</sup> (JCAT).** The Joint Counterterrorism Assessment Team’s mission is to improve information sharing and enhance public safety in coordination with the FBI, DHS, and the IC. The team collaborates with other members of the IC to research, produce, and disseminate counterterrorism intelligence products for federal, state, local, tribal, and territorial law enforcement as well as private sector partners. The JCAT also helps articulate counterterrorism intelligence requirements and needs of these partners throughout the IC. The JCAT is staffed not only by federal counterterrorism officers but also by law enforcement officers from across the country who are on temporary fellowship assignments to work on the team. This not only brings an important perspective from local law enforcement information needs; it provides officers a unique experience and a network of counterterrorism contacts for information sharing.

## REGIONAL INFORMATION SHARING SYSTEMS (RISS)

The Regional Information Sharing Systems<sup>962</sup> (RISS) has been in operation since 1973. RISS is a congressionally funded program, administered by DOJ, that provides services supporting the investigative and prosecution efforts of law enforcement and criminal justice agencies. The RISS Secure Cloud (RISSNET) was founded in response to transjurisdictional crime problems and the need for cooperation to secure information sharing among law enforcement agencies as well as to provide technical assistance for investigations and intelligence. RISS’s mission is to assist local, state, federal, and tribal criminal justice partners by providing adaptive solutions and services that facilitate information sharing, support criminal investigations, and promote officer safety.

Today, RISS is a national network comprising six multistate centers operating regionally.

- ◆ **Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network<sup>963</sup> (MAGLOCLEN):** Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia. The center also has member agencies in England, the Canadian provinces of Ontario and Quebec, and Australia.
- ◆ **Mid-States Organized Crime Information Center<sup>964</sup> (MOCIC):** Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. The center also has member agencies in Canada.

---

959 <https://www.dni.gov/files/documents/Newsroom/DomesticApproachtoNationalIntelligence.PDF>

960 <https://www.dni.gov/index.php/nctc-what-we-do/overview>

961 <https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team>

962 <https://www.riss.net/>

963 <https://www.riss.net/centers/magloclen/>

964 <https://www.riss.net/centers/mocic/>

- ◆ **New England State Police Information Network<sup>965</sup> (NESPIN):** Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The center also has member agencies in Canada.
- ◆ **Regional Organized Crime Information Center<sup>966</sup> (ROIC):** Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia, Puerto Rico, and the U.S. Virgin Islands.
- ◆ **Rocky Mountain Information Network<sup>967</sup> (RMIN):** Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. The center also has member agencies in Canada.
- ◆ **Western States Information Network<sup>968</sup> (WSIN):** Alaska, California, Hawaii, Oregon, and Washington. The center also has member agencies in Canada, New Zealand, and Guam.

The regional approach allows each center to offer support services tailored to the needs of member agencies, although the centers also provide services and products that are national in scope and significance. Typical targets of RISS-member agencies' activities are initiatives against terrorism, drug trafficking, violent crime, cybercrime, gang activity, and organized crime. While the RISS Program is congressionally funded and administered by the U.S. Bureau of Justice Assistance (BJA), it is controlled by its member agencies. As a result, state and local law enforcement agencies play a critical role in helping the RISS Centers establish priorities related to services, such as specially tailored information systems and investigative resources.

Traditional support services provided to law enforcement member agencies from the RISS Centers include the following:

- ◆ Information-sharing resources and deconfliction
- ◆ Analytical services
- ◆ Loan of specialized investigative equipment
- ◆ Confidential funds
- ◆ Training conferences
- ◆ Technical assistance

**RISSNET.** RISS operates the RISS Secure Cloud, known as RISSNET, to facilitate law enforcement communications and information sharing nationwide. RISS local, state, federal, and tribal law enforcement member agency personnel have online access to share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. There is a comprehensive array of resources and subsystems within RISSNET; of particular interest to the current discussion is the RISS Criminal Intelligence Database (RISSIntel).<sup>969</sup> This system provides for a real-time, online federated search of more than 75 RISS and partner intelligence databases, including state intelligence systems, fusion centers, and systems connected via the National Virtual Pointer System (NVPS). RISSIntel permits federated searching across many systems without requiring the RISSNET user to have a separate user account for each partner system. Millions of intelligence records are available via RISSIntel and between connected partner systems. Records include individuals, organizations, and associates, as well as locations, vehicles, weapons, and telephone numbers.

965 <https://www.riss.net/centers/nespin/>

966 <https://www.riss.net/centers/roic/>

967 <https://www.riss.net/centers/rmin/>

968 <https://www.riss.net/centers/wsin/>

969 <https://www.riss.net/rissintel/>

## FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

The Financial Crimes Enforcement Network<sup>970</sup> is designed to bring agencies, investigators, and information together to fight the complex problem of money laundering. Since its creation in 1990, FinCEN has worked to maximize information sharing among law enforcement agencies and its other partners in the regulatory and financial communities. Through cooperation and partnerships, FinCEN's network approach encourages cost-effective and efficient measures to combat money laundering domestically and internationally.

The network supports federal, state, local, tribal, and international law enforcement by analyzing information required under the Bank Secrecy Act (BSA), one of the nation's most important tools in the fight against money laundering. The BSA's record keeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities, and their assets. Over the years, the FinCEN staff has developed expertise in adding value to the information collected under the BSA by uncovering leads and exposing unknown pieces of information contained in the complexities of money laundering schemes.

Illicit financial transactions can take many routes—some complex, some simple, but all increasingly inventive—with the goal being to disguise the source. The money can move through banks, check cashers, money transmitters, businesses, and casinos and is often sent overseas to become “clean.” The tools of the money launderer can range from complicated financial transactions, carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

Intelligence research specialists and law enforcement support staff members research and analyze this information and other critical forms of intelligence to support financial criminal investigations. The ability to network with a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country. Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its employees—a responsibility that strongly imprints all of its data management functions and operations.

FinCEN's information sources fall into three categories:

- ◆ **Financial database:** The financial database consists of reports that the BSA requires to be filed, such as data on large currency transactions conducted at financial institutions or casinos, suspicious transactions, and international movements of currency or negotiable monetary instruments. This information often provides invaluable assistance for investigators because it is not readily available from any other source and preserves a financial paper trail for investigators to track criminals' proceeds and assets.
- ◆ **Commercial and public records databases:** Information from commercially available sources plays an increasingly vital role in criminal investigations. Commercial databases include information such as state, corporation, property, and people locator records, as well as professional licenses and vehicle registrations.
- ◆ **Law enforcement databases:** FinCEN is able to access various law enforcement databases through written agreements with each agency.

**High Risk Money Laundering and Related Financial Crimes Areas<sup>971</sup> (HIFCA).** Part of the FinCEN program, HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high-intensity money laundering zones. HIFCAs may be defined geographically or can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

---

970 <https://www.fincen.gov/>

971 <https://www.fincen.gov/hifca-regional-map>

The HIFCA program is intended to concentrate law enforcement efforts at the federal, state, and local levels to combat money laundering in designated high-intensity money laundering zones. To implement this goal, a money-laundering action team will be created or identified within each HIFCA to spearhead a coordinated federal, state, and local anti-money laundering effort. Each action team will: (1) be composed of all relevant federal, state, and local enforcement authorities, prosecutors, and financial regulators; (2) focus on tracing funds to the HIFCA from other areas, and from the HIFCA to other areas, so that related investigations can be undertaken; (3) focus on collaborative investigative techniques, both within the HIFCA and between the HIFCA and other areas; (4) ensure a more systemic exchange of information on money laundering between HIFCA participants; and (5) include an asset forfeiture component as part of its work.

## HIGH INTENSITY DRUG TRAFFICKING AREAS (HIDTAS)

The HIDTA program, created by Congress with the Anti-Drug Abuse Act of 1988, provides assistance to federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States. This grant program is administered by the Office of National Drug Control Policy (ONDCP). The HIDTA<sup>972</sup> Intelligence System has more than 1,500 law enforcement personnel, mostly criminal intelligence analysts, participating full time in more than 60 intelligence initiatives in the 28 HIDTA designated areas throughout the United States. While HIDTA is a counterdrug program, the intelligence centers operate in a general criminal intelligence environment, thereby leveraging all criminal intelligence information for the program's primary mission.

The HIDTA Intelligence System, a core element in the creation and growth of many SLTLE intelligence programs, largely depends on HIDTA program mandates. Each HIDTA must establish an intelligence center co-managed by a federal and a state or local law enforcement agency. The core mission of each individual HIDTA Intelligence Center is to provide tactical, operational, and strategic intelligence support to its HIDTA executive board, a group of participating law enforcement agency principals responsible for the daily management of their respective HIDTAs, HIDTA-funded task forces, and other regional HIDTAs. Developing regional threat assessments and providing event and target deconfliction are also among the centers' core missions. These core functions are critical to building trust and breaking down parochialism between and among the local, state, and federal participating law enforcement agencies.

The **National HIDTA Assistance Center**<sup>973</sup> provides resources and information to aid the HIDTA centers, including training, financial services, and media and technology services. In addition, the center has three national initiatives: the National Emerging Threats Initiative, the National Marijuana Initiative, and Domestic Highway Enforcement.

## CRIMINAL INTELLIGENCE COORDINATING COUNCIL (CICC)

The CICC<sup>974</sup> was created after the 9/11 attacks as a mechanism to develop and enhance the sharing of intelligence and critical information among and between law enforcement agencies of all levels. The council advises Global, a formally constituted advisory committee to DOJ. Through its evolution, the CICC has also become an important partner with DHS I&A as well as DHS Partner Engagement. The CICC has representatives appointed from different law enforcement organizations and groups as well as federal agencies with leadership coming from state and local law enforcement. In its early days, the CICC was instrumental in developing policies and practices of sharing terrorism-related information. Its reach has broadened significantly providing guidance in a wide range of technological applications in the intelligence process to privacy and civil rights. The council strives to ensure that every chief, sheriff, and law enforcement executive has a stake in its effort so that all law enforcement and homeland security agencies understand their role in the development and sharing of information and intelligence while also collaborating with federal partners.

---

972 <https://www.dea.gov/hidta>

973 <https://www.nhac.org/>

974 <https://it.ojp.gov/global/working-groups/cicc>

The coordination that the CICC strives for has far-reaching effects, the most significant being the continued active involvement of SLTLE and homeland security agencies in nationwide criminal intelligence sharing efforts. It is only through the institutionalization of coordination and collaboration among all agencies—regardless of size and jurisdiction—that agencies can effectively and efficiently develop and share criminal intelligence, resulting in a safer nation. This is the CICC’s continuing mission.

## DECONFLICTION

Deconfliction is the process of determining when law enforcement personnel, particularly from different jurisdictions or assignments, are conducting an event, often at high risk, in proximity to one another during the same time frame. When certain variables—such as date, time, and location—are matched between two or more different law enforcement operations, a conflict is the result. Deconfliction is a mechanism to compare operations and notify participating agencies and personnel of the conflict. There is also subject or target deconfliction, wherein agencies determine whether there are multiple investigations of the same person or criminal enterprise so that information can be compared and no investigation is compromised.

Event deconfliction helps support and protect law enforcement officers in a variety of ways. Officers partaking in high-risk operations are able to enhance their personal safety and the safety of those around them. The use of an event deconfliction system also helps to reduce risk and liability, improve the wellness of officers, and safeguard citizens. Using an event deconfliction system enables officers to identify operational conflicts and collaborate with other law enforcement agencies and officers. Officers are able to leverage each other’s information and successfully apprehend criminals. Often, after entering information about an event into an event deconfliction system, officers discover that they are investigating the same subject as another law enforcement agency or officers. There is no cost to use any of the participating systems.<sup>975</sup>

- ◆ **Nationwide Officer Safety Event Deconfliction**<sup>976</sup>—Using a map interface, the site identifies event deconfliction systems (Case Explorer, SAFETNet, and RISSafe™) available in each state and U.S. territory. When a state is selected from the drop-down menu or map, deconfliction systems and contact information for the state or territory are listed. The system with the greatest number of users (in a state) is listed first.
- ◆ **Case Explorer**<sup>977</sup>—A Web-based deconfliction program with access provided through the Washington/Baltimore HIDTA.
- ◆ **SAFETNet**<sup>978</sup>—Access is provided by the appropriate regional HIDTA Investigative Support Center.
- ◆ **RISSafe**<sup>979</sup>—Access is provided through the appropriate RISS Center and is available to all law enforcement agencies even if an agency is not a RISS member.
- ◆ **DEA Internet Connectivity Endeavor**<sup>980</sup> (**DICE**)—DICE enables participating federal, state, local, tribal, and territorial law enforcement agencies to deconflict investigative information.

---

975 <https://www.ncirc.gov/Deconfliction/>

976 <https://www.ncirc.gov/Deconfliction/Map.aspx>

977 <http://caseexplorer.net/>

978 [https://www.ncirc.gov/Deconfliction/Documents/SAFETNet\\_Informational\\_Card.pdf](https://www.ncirc.gov/Deconfliction/Documents/SAFETNet_Informational_Card.pdf)

979 <https://www.riss.net/rissafe/>

980 <https://dice.usdoj.gov/>

## A UNIFIED MESSAGE ON LAW ENFORCEMENT INFORMATION SHARING<sup>981</sup>

The 2019 Global Call to Action, titled *Strategic Solutions to Transform Our Nation's Justice and Public Safety Information Sharing*,<sup>982</sup> recommended more effective, efficient, and coordinated technical, policy, and funding activities for information technology (IT) solutions and practices. The recommendations have not changed, even though IT and sharing capabilities have evolved. The CICC established a multipartner Criminal Intelligence/Information Technology Crossroads Committee (CI/IT) to better coordinate the actions of agencies and associations facing similar IT and policy challenges and issues that have emerged from modern IT. The Crossroads Committee developed and approved the information sharing best practices described in this call to action to help address the complex information sharing environment.

Data owners should prioritize information interoperability (e.g., the ability of computer systems to access and exchange information) to share data efficiently, in accordance with applicable laws. This will allow better allocation of resources to plan and implement technical solutions and increase connectivity and information sharing among partners. Actions include developing:

- ◆ Information sharing policies and practices.
- ◆ Enhancements to existing data sharing capabilities and partnerships.
- ◆ A three- to five-year information sharing plan.

Data owners are encouraged to incorporate lessons learned and information sharing best practices to improve access to data while ensuring privacy, civil liberties, and civil rights protection and data security. Specific lessons learned include the following:

- ◆ Ensure that new technology applications are implemented in conjunction with agency policy.
- ◆ Remain cognizant of vendor motivations; your data has value. Also ensure data storage location and ownership when purchasing a new IT product.
- ◆ Develop and apply national data information sharing standards (e.g., NIST, NIEM/LEXS, NIEF/GFIPM/ SAML) as appropriate to enhance interoperability.
- ◆ Ensure that new vendor products support data owners' information sharing objectives.
- ◆ Research partner capabilities to avoid duplication and/or incompatible data repositories.
- ◆ Consider participation in the CI/IT Crossroads Committee to remain aware of current issues and concerns.

Beyond the information sharing platforms discussed previously, the unified message urges law enforcement agencies to use additional systems that will aid in enhancing community safety and officer safety. While these are not intelligence systems, per se, they have value in the intelligence process.

- ◆ **Bomb Arson Tracking System<sup>983</sup> (BATS)**—A Web-based case management system that provides state and local arson and explosives investigators with access to up-to-date arson and explosives investigative data from across the nation.
- ◆ **eTrace<sup>984</sup>**—An Internet-based system that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center (NTC). Authorized users can receive firearm trace results via this same website, search a database of all firearm traces submitted by their individual agencies, and perform analytical functions.

981 <https://it.ojp.gov/GIST/1208/A-Global-Unified-Message-Regarding-Information-Sharing>

982 [https://it.ojp.gov/documents/d/Transforming%20Our%20Nation\\_Call%20to%20Action.pdf](https://it.ojp.gov/documents/d/Transforming%20Our%20Nation_Call%20to%20Action.pdf)

983 <https://www.atf.gov/explosives/bomb-arson-tracking-system-bats>

984 <https://etrace.atf.gov/etrace/>

- ◆ **FirstNet<sup>985</sup>**—A high-speed, nationwide, wireless broadband network dedicated to public safety.
- ◆ **National Incident-Based Reporting System<sup>986</sup> (NIBRS)**—An incident-based reporting system for crimes known to police departments. For each crime incident coming to the attention of law enforcement, a variety of data is collected about the incident. These data include the nature and types of specific offenses in the incident, characteristics of the victim(s) and offender(s), types and value of property stolen and recovered, and characteristics of persons arrested in connection with the incident.
- ◆ **National Missing and Unidentified Persons System<sup>987</sup> (NamUS)**—A national information clearinghouse and resource center for missing, unidentified, and unclaimed person cases across the United States.
- ◆ **National Seizure System<sup>988</sup> (NSS)**—A repository for information on drug, clandestine laboratory, and other contraband seizures such as chemical precursors, currency, and weapons. The system also contains information on methods of concealment, seizure locations, people, organizations, and transportation.
- ◆ **Nationwide Suspicious Activity Reporting (SAR) Initiative<sup>989</sup> (NSI)**—A collaborative effort by DHS, the FBI, and SLTLE partners to permit the reporting and sharing of suspicious behaviors related to terrorism and targeted violence.
- ◆ **Overdose Detection Mapping Application Program<sup>990</sup> (ODMAP)**—The program provides near real-time suspected overdose surveillance data across jurisdictions to support public safety and public health efforts to mobilize an immediate response to a sudden increase, or spike, in overdose events. It links first responders and relevant record management systems to a mapping tool to track overdoses to stimulate real-time response and strategic analysis across jurisdictions.

## INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)

While this chapter has focused on national and federal resources for law enforcement intelligence, it is useful also to look beyond U.S. borders for another law enforcement information sharing resource. INTERPOL is the International Criminal Police Organization,<sup>991</sup> founded in 1923 to serve as a clearinghouse for information on transnational criminals. It receives, stores, analyzes, and disseminates criminal data in cooperation with its 181 member countries on a 24/7/365 basis in its four official languages (English, French, Spanish, and Arabic). INTERPOL deals only with international crimes. It provides four core functions to member states:

- ◆ **Secure global police communication services.** INTERPOL operates a global police communications system called I-24/7, which provides police agencies around the world with a common platform through which to share crucial information about criminals and criminality.
- ◆ **Operational data services and databases for police.** INTERPOL's databases and services ensure that police agencies worldwide have access to the information and services they need to prevent and investigate crimes. Databases include data on criminals such as names, fingerprints, and DNA profiles, and stolen property such as passports, vehicles, and works of art.
- ◆ **Operational police support services.** INTERPOL supports law enforcement officials in the field with emergency support and operational activities, especially in its priority crime areas of fugitives, public safety and terrorism, drugs and organized crime, trafficking in human beings, and financial and high-tech crime. A Command and Coordination Centre operates 24 hours a day, seven days a week.

985 <https://www.firstnet.com/>

986 <https://www.fbi.gov/services/cjis/ucr/nibrs>

987 <https://www.namus.gov/>

988 <https://esp.usdoj.gov>

989 <https://www.dhs.gov/nsi>

990 <http://www.odmap.org/>

991 The INTERPOL General Secretariat site is <https://www.interpol.int/>.

- ◆ Police training and development. INTERPOL provides focused police training initiatives for national police forces and offers on-demand advice, guidance, and support in building dedicated crime-fighting components. The aim is to enhance the capacity of member countries to effectively combat serious transnational crime and terrorism.

Criminal intelligence analysts at INTERPOL are uniquely placed to recognize and detect patterns and criminal trends from a global perspective, as well as having the resources to assist with specific international crime cases.

In the United States, the contact point for INTERPOL is the U.S. National Central Bureau (USNCB), which operates within the guidelines prescribed by the Department of Justice, in conjunction with the DHS. The mission of the U.S. National Central Bureau is to facilitate international law enforcement cooperation as the U.S. representative to INTERPOL.

U.S. law enforcement officers can gain access to INTERPOL reports and make international inquiries by contacting their state points of contact (usually within state law enforcement or intelligence agencies or fusion centers), who will then query the USNCB.<sup>992</sup>

## SUMMARY

As demonstrated through the above discussions, the amount of information and intelligence being generated by federal law enforcement agencies and national law enforcement entities is significant. If that information is not being used, then its value is lost. Not only are these resources responsible for making information available to SLTLE agencies in an accessible and consumable form, but nonfederal law enforcement must develop the mechanisms for receiving the information and being good consumers of it.

One of the ongoing controversies is the problem of dealing with classified information. This chapter explained the classification process as well as the initiatives that are being undertaken to deal with this issue. One measure is to increase the number of security clearances for SLTLE personnel. The other is for federal agencies to write intelligence products so that they are unclassified but remain as SBU/CUI to give SLTLE personnel access.

By gaining access to secure networking (e.g., LEEP, HSIN, RISSNET), interacting on a regular basis with fusion centers, and proactively interacting with other federal law enforcement intelligence offices, SLTLE agencies can have access to the types of critical intelligence necessary to protect their communities.

## CONCLUSIONS

If effective information sharing is one of the critical goals of contemporary law enforcement intelligence, then networks and systems are the critical tools to reach that goal. As has been seen throughout this chapter, there has been significant growth in the capability for law enforcement agencies to share information. This growth has been a product of new initiatives following 9/11, the availability of new networking technologies that reduce interoperability conflicts, and the commitment of American law enforcement at all levels of government to facilitate information-sharing processes. These factors are in a dynamic state at this writing. Systems and networks will change; therefore, it is incumbent on intelligence managers to carefully monitor trends to stay current.

---

992 <https://www.justice.gov/interpol-washington>

# CHAPTER ANNEX 13-1: FBI PROCESS AND INFORMATION FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT PERSONNEL TO OBTAIN A SECURITY CLEARANCE

## SECURITY CLEARANCE PROCESS FOR THE FBI<sup>993</sup>

It is the policy of the Federal Bureau of Investigation (FBI) to share with Law Enforcement personnel pertinent information regarding terrorism. In the past, the primary mechanism for such information sharing was the Joint Terrorism Task Force (JTTF). In response to the terrorist attack on America on September 11, 2001, the FBI established the State and Local Law Enforcement Executives and Elected Officials Security Clearance Initiative. This program was initiated to brief officials with an established need to know on classified information that would or could affect their areas of jurisdiction.

Most information needed by state or local law enforcement agencies can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. This brochure describes when security clearances are necessary and the notable differences between clearance levels. It also describes the process involved in applying and being considered for a clearance.

State and local officials who require access to classified material must apply for a security clearance through their local FBI field offices. Candidates should obtain from their local FBI field offices a Standard Form 86 (SF 86), Questionnaire for National Security Positions; and two FD-258 (FBI applicant fingerprint cards). One of two levels of security clearance, Secret or Top Secret, may be appropriate. The background investigation and records check for Secret and Top Secret security clearance are mandated by Presidential Executive Order (EO). The EO requires these procedures for a security clearance to be granted; the FBI does not have the ability to waive them.

## SECRET CLEARANCES

A Secret security clearance may be granted to those persons who have a need to know national security information, classified at the Confidential or Secret level. It is generally the most appropriate security clearance for state and local law enforcement officials who do not routinely work on an FBI Task Force or in an FBI facility. A Secret security clearance takes the least amount of time to process and allows for escorted access to FBI facilities.

The procedure is as follows:

- ◆ The FBI performs record checks with various federal agencies and local law enforcement, as well as a review of credit history.
- ◆ The candidate completes forms SF-86<sup>994</sup> and FD-258.<sup>995</sup>
- ◆ Once favorably adjudicated for a Secret security clearance, the candidate will be required to sign a nondisclosure agreement.

## TOP SECRET CLEARANCES

A Top Secret clearance may be granted to those persons who have a need to know national security information, classified up to the Top Secret level, and who need unescorted access to FBI facilities, when necessary. This type of clearance will most often be appropriate for law enforcement officers assigned to FBI Task Forces housed in FBI facilities. In addition to all the requirements at the Secret level, a background investigation, covering a ten-year time

<sup>993</sup> <http://www.fbi.gov/clearance/securityclearance.htm>

<sup>994</sup> [http://www.opm.gov/Forms/pdf\\_fill/sf86.pdf](http://www.opm.gov/Forms/pdf_fill/sf86.pdf)

<sup>995</sup> This form is the FBI applicant fingerprint card, available at any FBI office. Two cards are required. A sample of the FD-258 is at <https://www.fbi.gov/file-repository/identity-history-summary-request-fd-258-110120/view>.

period, is required. Once favorably adjudicated for a Top Secret security clearance, the candidate will be required to sign a nondisclosure agreement.

## QUESTIONS AND ANSWERS (Q&A):

### Q: WHO SHOULD APPLY FOR A SECURITY CLEARANCE?

**A:** State or local officials whose duties require that they have access to classified information and who are willing to undergo a mandatory background investigation.

### Q: WHAT IS THE PURPOSE OF A BACKGROUND INVESTIGATION?

**A:** The scope of the investigation varies with the level of the clearance being sought. It is designed to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information. Applicants must meet certain criteria relating to their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals.

### Q: IF AN INDIVIDUAL OCCUPIES AN EXECUTIVE POSITION WITH A LAW ENFORCEMENT AGENCY, MUST HE OR SHE STILL UNDERGO A BACKGROUND INVESTIGATION TO ACCESS CLASSIFIED INFORMATION?

**A:** An Executive Order (EO), issued by the President, requires background investigations for **all** persons entrusted with access to classified information. The provisions of the EO are mandatory, cannot be waived, and apply equally to all federal, state, and local law enforcement officers. This is true of both Secret and Top Secret security clearances.

### Q: HOW LONG DOES IT NORMALLY TAKE TO OBTAIN A SECRET SECURITY CLEARANCE?

**A:** It is the goal of the FBI to complete the processing for Secret security clearances within 45 to 60 days once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity.

### Q: HOW LONG DOES IT NORMALLY TAKE TO OBTAIN A TOP SECRET SECURITY CLEARANCE?

**A:** It is the goal of the FBI to complete the processing for Top Secret security clearances within six to nine months once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity.

### Q: WHAT KINDS OF INQUIRIES WILL THE FBI MAKE INTO MY BACKGROUND?

**A:** Credit and criminal history checks will be conducted on all applicants. For a Top Secret security clearance, the background investigation includes additional record checks, which can verify citizenship for the applicant and family members, verification of birth, education, employment history, and military history. In addition, interviews will be conducted with persons who know the candidate and of any spouse divorced within the past ten years. Additional interviews will be conducted, as needed, to resolve any inconsistencies. Residences will be confirmed, neighbors interviewed, and public records queried for information about bankruptcies, divorces, and criminal or civil litigation. The background investigation may be expanded if an applicant has resided abroad or has a history of mental disorders or drug or alcohol abuse. A personal interview will be conducted with the candidate.

- Q:** IF I HAVE A POOR CREDIT HISTORY, OR OTHER ISSUES IN MY BACKGROUND, WILL THIS PREVENT ME FROM GETTING A SECURITY CLEARANCE?
- A:** A poor credit history or other issues will not necessarily disqualify a candidate from receiving a clearance, but resolution of the issues will likely take additional time. If the issues are significant, they may prevent a clearance from being approved.
- Q:** IF I CHOOSE NOT TO APPLY FOR A SECURITY CLEARANCE, WILL I STILL BE INFORMED ABOUT COUNTERTERRORISM ISSUES IMPORTANT TO MY JURISDICTION?
- A:** Absolutely. If the FBI receives information relevant to terrorism that may impact your jurisdiction, you will be informed by your local field office through the Law Enforcement Enterprise Portal and other available mechanisms approved for the transmission of unclassified information. Most terrorism-related information can be provided in an unclassified form.
- Q:** ARE THERE ANY OTHER ADVANTAGES OR DISADVANTAGES TO RECEIVING UNCLASSIFIED OR CLASSIFIED TERRORISM- RELATED INFORMATION?
- A:** An additional advantage of receiving unclassified terrorism-related information is that there may be fewer restrictions on your ability to further disseminate it within your jurisdiction. Classified information may be disseminated only to other cleared persons who also have a need to know.
- Q:** WHAT IS THE DIFFERENCE BETWEEN AN INTERIM AND A FULL SECURITY CLEARANCE?
- A:** Interim clearances are granted in exceptional circumstances in which official functions must be performed before completion of the investigative and adjudicative processes associated with the security clearance procedure. There is no difference between an interim and a full security clearance as it relates to access to classified information. However, when such access is granted, the background investigation must be expedited, and, if unfavorable information is developed at any time, the interim security clearance may be withdrawn.

If you have any additional questions and/or wish to apply for a security clearance, please contact your local FBI field office. (See <https://www.fbi.gov/contact-us/field-offices> to locate the nearest field office.)

# CHAPTER 14

## MANAGEMENT AND HUMAN RESOURCE ISSUES FOR THE INTELLIGENCE FUNCTION



The basic principles and applications of management—leadership, accountability, supervision, span of control, chain of command, labor relations, budgeting, etc.—apply to the intelligence function in the same manner as they would apply to any other unit within a law enforcement agency. Hence, the extensive literature of police administration and management serves as a solid resource for these issues of managing an intelligence unit. As a result, this chapter will focus on selected issues relating to the development and management of the intelligence function.

Of course, police departments range in size from a single officer in a small community to the plus or minus 36,000 officers and nonsworn personnel in the New York Police Department (NYPD). An intelligence capacity in a single-officer department may be the officer receiving intelligence bulletins by email and occasionally submitting a SAR to the fusion center. NYPD's Intelligence Bureau not only contains two different sections with significant amounts of sophisticated technology for information collection and analysis, but also posts officers as intelligence liaisons in police departments in major cities around the world.<sup>996</sup> The term "intelligence capacity" can have a significantly different meaning depending not only on an agency's size but also on the character of a jurisdiction and the threats it faces.

The intelligence function in an agency also varies depending on the police executive's vision and leadership of the agency. In some agencies, the intelligence unit is narrowly limited; for example, focusing only on gangs and criminal extremism. In a different agency, the chief executive may embrace intelligence-led policing, with a larger number of

<sup>996</sup> <https://www1.nyc.gov/site/nypd/bureaus/investigative/intelligence.page>

analysts focusing on all crimes. Regardless of the size or intelligence philosophy, there will be management issues. The intent of this chapter is to provide a broad look at intelligence management issues and processes to provide the reader with a buffet of factors to consider, including those that are most applicable to his or her agency's intelligence philosophy and needs. It is doubtful that any agency will need to address every issue discussed in this chapter. It is likely, however, that every issue addressed will be relevant to different agencies across the country.

When a new, unfamiliar activity is introduced into an organization—such as intelligence—an important management task is helping the organization *adapt to change*. Law enforcement has experienced this in the past: problem-oriented policing, community policing, and the use of CompStat are illustrations. For example, as community policing was growing in the 1980s, there were significant challenges: It was a conceptually different way of policing a community and required new tasks and responsibilities of officers. It was uncomfortable, requiring a new learning curve of police responsibilities as well as organizational change. There was criticism, resistance, and skepticism that this “new way of policing” would work. Three decades later—essentially a generation—community policing is the norm, although its path to normalcy was challenging. intelligence-led policing (ILP), which complements community policing, is following a similar path and requires adept management skills to reach its goal.

## FOUNDATION

Most American law enforcement agencies do not have a formal intelligence unit but still have an intelligence function to manage. With the growing symbiosis among agencies at all levels of government, adoption of the *National Criminal Intelligence Sharing Plan* (NCISP), and the growth of networked intelligence information systems, along with the responsibility to keep the homeland secure, virtually every law enforcement agency in the country should have some capacity to share threat information and suspicious activities. That capacity may be a full-scale unit or one person who serves part time as an agency's point of contact to receive and disseminate critical information. As an initial artifact of the September 11, 2001 (9/11), attacks, expanding with the violence associated with drug trafficking, including the devastating effects of the opioid crisis, targeted mass violence, human smuggling, and other transjurisdictional criminal enterprises, in some form an intelligence capacity has become a de facto requirement for American law enforcement agencies. As a result, new intelligence processes for law enforcement present challenges such as the following:

- ◆ Reengineering some of the organization's structure and processes.
- ◆ Developing a shared vision of the criminal extremist or criminal threats within the community, as well as the broader law enforcement community.
- ◆ Participating in intelligence processes and following through with information sharing and suspicious activity reporting.
- ◆ Developing a “culture of information sharing” so that the new information sharing processes are consistently used.
- ◆ Committing resources, time, and energy to the intelligence function.
- ◆ Developing a proactive spirit and creative thought to identify “what we do not know” about terrorism and criminal enterprises in the community.
- ◆ Developing a culture within the law enforcement agency that is able to think globally and act locally.
- ◆ Providing vigilance, patience, and entrepreneurial leadership to address complex criminality that threatens a community.

To operationalize these components into a functional intelligence capacity, state, local, and tribal law enforcement (SLTLE) agencies *of all sizes*, as recommended by the NCISP, should have, at a minimum, fundamental operational components. These include:

- ◆ A person designated as the intelligence point of contact to whom external agencies may direct inquiries, warnings, and advisories and from whom information and questions may be sent. This person must have sufficient training to understand the language, processes, and regulations incumbent on the law enforcement intelligence community.
- ◆ A secure electronic communications system for sending and receiving information that is Sensitive But Unclassified (SBU). Several systems are available, including the Law Enforcement Enterprise Portal<sup>997</sup> (LEEP) and the Regional Information Sharing Systems (RISS) Secure Cloud<sup>998</sup> (RISSNET)—some of which are available at no charge to the user. With the growth of the National Information Exchange Model<sup>999</sup> (NIEM), access to these systems will be essential for the most accurate information sharing.
- ◆ Established policies for information collection, reporting, and dissemination.
- ◆ The ability to determine the kinds of information and intelligence that is needed to effectively prevent terrorism and disrupt criminal enterprises. This is a difficult challenge requiring a significant labor investment. Understanding the threats and targets within a community and developing responses to neutralize those threats is essential. American law enforcement must discover the evidence of threats that may be in its backyard.
- ◆ An established relationship with the primary state fusion center.

Beyond these factors, a number of management factors may be considered when developing an intelligence capacity. A common question asked by law enforcement executives and those responsible for developing an intelligence capacity, is “Where do I start?” Providing a succinct response is not easy because the starting place will vary depending on agency size, the chief executive’s vision, the geographic location of the jurisdiction, the presence of factors that make the jurisdiction a terrorist or criminal target, and other variables unique to the jurisdiction and the agency. As a result, the first part of the answer is to provide a list of factors to be considered in developing—or reengineering—the intelligence capacity in a law enforcement agency. The second part of the answer is to develop a concept of operations (ConOps) for the intelligence unit to refine how the intelligence function is envisioned to integrate with the agency’s other activities. Finally, attention will be given to selected intelligence management issues.

## A CHECKLIST OF CONSIDERATIONS FOR DEVELOPING OR REENGINEERING THE LAW ENFORCEMENT INTELLIGENCE CAPACITY

For ease, the following is a list of questions and variables to consider in developing the intelligence capacity. As noted previously, not every factor will apply to every agency, although collectively all of these factors will give a perspective on the intelligence function as it exists within the organizational environment. The intent of the list is to provide food for thought and a straightforward perspective on the management responsibilities required to accomplish the task. Many of the factors will be discussed in greater detail later in the chapter.

### ADMINISTRATION AND MANAGEMENT

- ◆ The chief executive must have a vision for the role of the intelligence function.
  - What activities are expected of the intelligence function?
    - A clearinghouse of information?
    - Tactical analysis?
    - Strategic analysis/forecasting?
    - Threat assessments?

997 <https://www.fbi.gov/services/cjis/leep>

998 <https://www.riss.net/>

999 For information on the National Information Exchange Model, see <https://it.ojp.gov/initiatives/niem>.

- Pointer and deconfliction activities?
- Other? Make sure this is articulated.
- Does the chief executive’s vision include incorporating the ILP philosophy throughout the law enforcement agency?
  - If not, what is the envisioned relationship of intelligence to other departmental activities?
  - This should be clearly articulated by the chief executive.
- If intelligence is one of several responsibilities assigned to one person or unit, what is its priority/relationship to other responsibilities?
- What crimes are to be the focus (i.e., strategic priorities) of the intelligence function?
- Will an all-threats and all-hazards orientation be included?
  - If so, how will all threats and all hazards be defined for the intelligence function?
- What outputs and activities are expected of the intelligence function?
- Question: Does the chief executive and/or command staff need to be briefed (i.e., training) on contemporary law enforcement intelligence?
  - If so, how is this to be accomplished?
- ◆ The chief executive must demonstrate commitment and support for the intelligence function.
  - This includes allocation of people and adequate resources.
- ◆ Obtain budget parameters.
  - How much funding will be available to establish the intelligence unit?
- ◆ Will the intelligence supervisor be organizationally responsible directly to the chief executive or to another commander (e.g., the Criminal Investigations Division (CID) commander or the Operations Division commander)?
  - There are advantages to both direct reporting to the chief executive and reporting to another commander.
    - If the intelligence unit supervisor answers directly to the chief executive:
      - Advantage: More direct information flow and operational responses regarding threats.
      - Disadvantage: There may be jealousies among those of higher rank with respect to the intelligence supervisor’s access to the chief executive.
      - Disadvantage: In a large agency, this may make the chief executive’s span of control too broad.
    - If the unit is assigned under another division commander:
      - Advantage: It helps shield the unit from criticisms of secrecy, which often becomes an issue.
      - Disadvantage: A filtering effect of critical information can occur.
  - While there are other advantages and disadvantages, all of these will depend on the culture of the law enforcement organization.

## DEVELOP THE INTELLIGENCE UNIT’S INFRASTRUCTURE

- ◆ The mission, goal(s), and objectives of the intelligence function must be articulated.
- ◆ Develop necessary policies and procedures (See Table 14-1 for a sample list of areas in which to consider developing policy for the intelligence function. The need for policy will be directly related to the mission, goals, and objectives.)
  - Develop a privacy policy that is consistent with federal privacy guidelines.<sup>1000</sup>
  - Develop a policy and procedures for the criminal intelligence records system that is 28 CFR Part 23-compliant.
    - The *Law Enforcement Intelligence Unit (LEIU) File Guidelines*<sup>1001</sup> serves as a court-tested model.
    - The criminal intelligence records policy should include:

1000 <https://it.ojp.gov/documents/d/7%20steps%20to%20a%20privacy,%20civil%20rights,%20and%20civil%20liberties%20policy.pdf>

1001 <http://www.leiu.org/sites/default/files/Criminal%20Intelligence%20File%20Guidelines.pdf>

- Positions/personnel assignments of persons who have access to the criminal intelligence records system.
  - Positions/personnel authorized to enter information into the system.
  - Positions/personnel authorized to review and purge information from the system.
- Collection standard of a criminal predicate.
  - Positions/personnel responsible for reviewing information prior to entering it into the system.

TABLE 14-1: SAMPLE ISSUES FOR INTELLIGENCE UNIT POLICY DEVELOPMENT<sup>1002</sup>

- ◆ Intelligence Unit Organization, Role, and Responsibilities
- ◆ Intelligence Unit Staff Position Requirements, Selection, and Training
- ◆ Privacy Policy (consistent with the federal *ISE Privacy Guidelines*)
- ◆ Intelligence Unit Records Management
  - 28 CFR Part 23-Compliant File Guidelines (including standards and processes collection, retention, review, purging, and dissemination)
  - Quality Control Procedures for Data and Information Accuracy
- ◆ Handling of SBU/CUI Information
- ◆ Access, Documentation, Dissemination, and of Use of Information From
  - Intelligence Records Systems (e.g., RISSNET, LEO, HSIN)
  - Contacting other agencies and jurisdictions (i.e., fusion centers, Federal Bureau of Investigation [FBI] Field Intelligence Group [FIG], and other law enforcement agencies)
  - Contacting the International Criminal Police Organization (INTERPOL)
  - Contacting the El Paso Intelligence Center (EPIC)
- ◆ Types of Intelligence Products to Be Produced
  - Marking and Dissemination Policy for Intelligence Products
- ◆ Intelligence Unit Reporting Procedures and Dissemination
- ◆ Suspicious Activity Reporting and Field Interview Procedures and Reporting
- ◆ Classification and Security System for the Agency and/or Intelligence Unit
  - Rules for Violations of the Security System
- ◆ Procedures and Accountability When Operating Under a Memorandum of Agreement (MOA)
- ◆ Intelligence Unit Processes and Responsibilities During Critical Incidents
- ◆ Surveillance Operations (processes, documentation, limitations)
- ◆ Access to Equipment and Resources in Support of Intelligence Activities
- ◆ Use of Criminal Informants
  - Guidelines for Payments to Criminal Informants
- ◆ Undercover Operations in Support of the Intelligence Function
  - Undercover Reporting Procedure
  - Investigative and Undercover Expense Fund Accountability
  - Consumption of Alcoholic Beverages During Undercover Operations and Surveillance
  - Narcotics Simulation During Undercover Narcotics Investigations
- ◆ Information Release and Media Policy
- ◆ Intelligence Unit Performance Evaluation and Review

1002 Model and sample policies and resources are available at the National Criminal intelligence Resource Center, <https://www.ncirc.gov/Policies.aspx>.

- Retention guidelines.
  - Temporary files should have a time limit for retention of information and standards for review and purging.
    - Process and timeline for the review of records in the criminal intelligence records system.
    - Purging requirements and processes.
    - Dissemination criteria.
    - Nondiscrimination statement.
- ◆ Select an office location.
  - Will the unit be co-located with CID, narcotics, organized crime, or another unit?
    - If so, be certain that the physical location will be able to meet the security requirements needed for intelligence records.
  - If the intelligence unit is at an off-site location, it is preferable to have a “stand-alone” office, not one shared with other businesses.
  - Ideally, the intelligence unit’s office will be centrally located.
  - Develop the work environment.
    - Get access to intelligence products and networks.
    - Lockable filing cabinets.
    - Dedicated computers and files.
    - All personnel, supplies, and services necessary to fulfill the vision.
- ◆ Purchase or obtain the unit’s unmarked vehicle(s).

## STAFFING

There is a wide array of staffing models used in intelligence units. Some units have sworn officers who are information collectors and some, sworn analysts. The knowledge they bring about crime and the community can be very valuable. Conversely, investigative experience tends to narrow their focus from an analytic perspective. Another issue often raised is that a sworn officer is likely to be promoted and transferred out of the unit; thus the unit will lose the officer’s knowledge and experience.

The majority of analysts are nonsworn and tend to bring a broader, more creative perspective to analytic problems. Recruiting analysts permits focusing on their research and technical skills, opening a broader candidate pool than might be possible compared with sworn officers. Nonsworn analysts may have a steeper learning curve with respect to crime in the community and criminal justice processes. Importantly, nonsworn analysts should never be viewed as clerical or support personnel; rather, they should be viewed and treated as practicing professionals. With these factors in mind, the following are staffing considerations:

- ◆ Select personnel: Sworn intelligence officers
  - Consider education, analytic skills, and languages if relevant to the jurisdiction.
  - Consider how the officers get along with other agencies.
  - Consider a past officer/deputy with diverse law enforcement experience.
  - Consider policing style.
    - A person who is operationally aggressive in making arrests typically is not a good fit in an intelligence unit that requires a more contemplative approach to analysis.
  - Personal characteristics most suited to the intelligence unit include:
    - Maturity
    - Dependability
    - Independent thinker
    - Strong technology skills
    - A person who works well without supervision

- Self-motivated
- A good writer
- Good communication skills
- A team player
- In selecting officers for the intelligence unit, be certain they are able to obtain a security clearance, if required for the position.
  - For law enforcement officers, one of the more common factors that prohibits them from receiving a clearance is poor credit.
- Consider knowledge of your special needs, such as gangs, computers, surveillance techniques, tactical surveillance equipment knowledge, etc.
- ◆ Select personnel: Analysts
  - The analyst should be viewed as a practicing professional of equal organizational stature to officers, not treated as support staff.
  - Desirable characteristics of an analyst include:
    - College education
    - Research skills
    - Creative thinker
    - Highly motivated
    - Strong computer skills
    - Willing to help with all cases
    - If applicable, a background that will enable the analyst to obtain a security clearance
- ◆ If applicable to the job assignment, once personnel have been selected, contact the local FBI office to apply for security clearances for your new personnel.<sup>1003</sup>
  - In most cases, a Secret level clearance will be sufficient. (NOTE: The process typically takes several months.)

## TRAINING

- ◆ Training
  - Get the added training needed to further the strategic plan.
    - Includes training on an agency's specific policies/procedures.
  - Remember, training includes both the intelligence discipline and training on crimes that are the focus of the intelligence unit.
- ◆ Ensure that all training meets the standards of:
  - *Minimum Criminal Intelligence Training Standards*<sup>1004</sup>
  - *National Criminal Intelligence Sharing Plan*<sup>1005</sup>
- ◆ Conduct a training needs assessment and enroll personnel in training programs they need (see examples below—training will be discussed later in the chapter).
  - Training in the discipline and processes of intelligence, including the Foundations of Intelligence Analysis Training (FIAT).
  - Analytic training.
  - Intelligence records management, including 28 CFR Part 23.
  - Analysts will need many other courses to become proficient.
    - Certified Intelligence Analyst certificates
    - Crime mapping
    - HIDTA programs (Analytical Investigative Techniques I & II)

1003 See <https://www.fbi.gov/resources/law-enforcement/security-clearances-for-law-enforcement>.

1004 [https://it.ojp.gov/documents/minimum\\_criminal\\_intel\\_training\\_standards.pdf](https://it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf)

1005 <https://it.ojp.gov/gist/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>

- FinCEN
- Join open source networks.
- ◆ Be certain to monitor the National Criminal Intelligence Resource Center’s training page for programs and topics.<sup>1006</sup>
- ◆ Attend the annual joint meeting of the LEIU and the International Association of Law Enforcement Intelligence Analysts (IALEIA) for training and presentations of emerging issues and techniques.

## INFORMATION MANAGEMENT AND INFORMATION SHARING

- ◆ In light of the chief executive’s vision of intelligence products:
  - Identify the types of intelligence products that are to be produced.
  - Identify the dissemination table of intelligence products.
    - Internal dissemination only?
    - If external dissemination is to be included, define:
      - Dissemination criteria (i.e., what are the characteristics of recipients who receive the products?)
      - Will the Third Agency Rule be applied?
      - Must products be approved for dissemination prior to being sent?
      - What is the mechanism for disseminating products?
      - Will there be an audit trail for disseminated products?
      - What types of products will not be disseminated outside of the agency?
- ◆ Select computer databases to store information and intelligence records:
  - Must be separated from the agency’s regular records management system (RMS).
  - Must be able to purge records from the system so they are destroyed and not accessible in the future.
  - Secure and audited access to computers and systems.
- ◆ Obtain individual computers for intelligence personnel.
  - Analysts need computers with fast processors and more memory to run analytic software.
  - Basic software needs:<sup>1007</sup>
    - Word processing program
    - Spreadsheet program
    - Relational database
    - Presentation software
    - Flowcharting software
    - Link analysis software
    - Database reporting/visualization software
    - Mapping software
    - Photo enhancement software
    - Telephone analysis software
    - Analytic charting
    - Portable document format (PDF) creation software
    - Security software (virus, adware, spyware software; firewall and virtual private network [VPN] security)
    - Publication software
    - Statistical analysis software
    - Text mining software
  - Budget for analytical tools and commercial databases, including membership in the RISS Program and commercial database search system.

1006 <https://www.ncirc.gov/Training.aspx>

1007 *The Analyst Toolbox*, Global Intelligence Working Group, [https://it.ojp.gov/documents/analyst\\_toolbox.pdf](https://it.ojp.gov/documents/analyst_toolbox.pdf)

- Full Internet access with VPN.
- Stand-alone computer for virtual undercover work as well as for accessing the dark net, extremists, and websites that have a potential criminal nexus.
  - An access log, including the names of those who use this computer as well as dates, times, and purpose, is advisable.
- ◆ Develop a report and intelligence product numbering system.
  - Keep an audit and control log of issued numbers that can be accessed by unit members.
  - Develop a system that easily permits identification of unit, date, and application of the bulletin.
- ◆ Organize monthly meetings among all the area analysts to discuss and share issues and analytic methods.
- ◆ Organize and host a monthly intelligence meeting with other area law enforcement agencies.
  - Meetings should include analysts and officers.
    - Creates a trusting environment with others.
    - Face-to-face contact is critical.
    - Sharing information is critical.
    - Create a contact list to quickly handle situations.
  - Also invite specific vetted individuals from appropriate private sector companies that can assist in reaching your goals, as applicable.
  - Invite federal agencies such as the Joint Terrorism Task Force, U.S. Immigration and Customs Enforcement, etc.

## IMPLEMENTATION AND ASSESSMENT

- ◆ Start the process.
  - Test the system and be prepared to adjust/refine it.
  - Identify critical processes and procedures to collect data for assessment.
  - Ask the consumers of the intelligence function whether it is working.
  - Seek suggestions for improvement.
- ◆ Implement an audit process.
  - Intelligence Guide Audit Model
  - LEIU Audit Checklist
- ◆ Strive for continuous quality improvement.

The points in this list are food for thought in developing an agency's intelligence structure. These factors are intended to help identify issues that need to be addressed in planning for the intelligence function. The next step is to integrate these factors into a cohesive vision of how the intelligence structure will actually operate within an agency. This is accomplished by molding these factors in a ConOps.

## DEVELOPING THE CONCEPT OF OPERATIONS

The ConOps is a user-oriented document that describes the characteristics for a proposed program, an initiative, or a system from the viewpoint of how staff members and users will interact with the proposed initiative.<sup>1008</sup> The ConOps is used to communicate overall characteristics of the new organizational entity—in this case, a new intelligence structure—to management, staff members, and users. Ideally, the ConOps is prepared in conjunction with a business plan. While the ConOps describes the organization, mission, and organizational objectives from an integrated systems point of view, the business plan describes the proposed system or situation from an investment and process point

<sup>1008</sup> A descriptive guide to ConOps can be found at <https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/concept-development/concept-of-operations>. A sample ConOps can be found at [https://www.dhs.gov/sites/default/files/publications/NICS\\_CONOPS\\_508-v2.pdf](https://www.dhs.gov/sites/default/files/publications/NICS_CONOPS_508-v2.pdf).

of view. Whether designed for a complex program or a relatively small unit, the ConOps serves as a mechanism to effectively plan the way the new initiative will work.

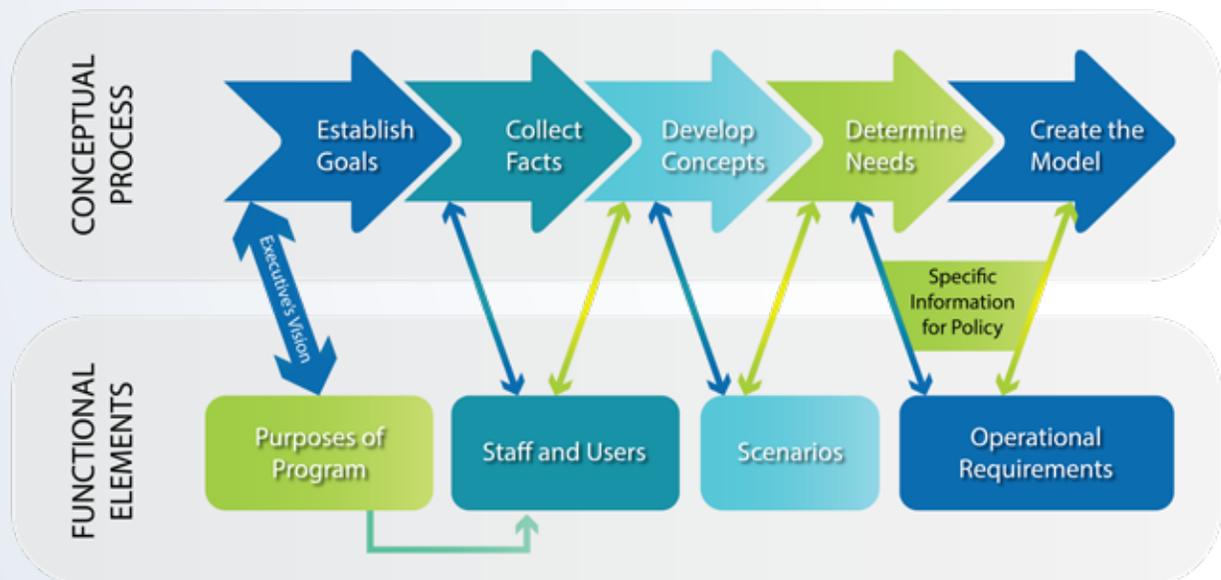
The ConOps provides an analysis that bridges the gap between operational needs and visions and the technical aspects of a functioning organization, in this case an intelligence unit. The ConOps should also document a program's characteristics and the users' operational needs in a manner that can be confirmed by users without requiring any technical knowledge beyond that required to perform normal job functions. For example, management and users need to understand how the intelligence unit will function and the products it will produce but do not need to know how to conduct specific types of analysis or access specific systems.

The ConOps documents the visions and expectations of management and users alike without requiring the provision of quantified, testable specifications until later in the system life cycle. The ConOps also provides a mechanism for management and users to express thoughts and concerns on possible issues, strategies, and processes before actual implementation of the system.

The ConOps represents a process for developing a new functional concept of an organizational activity. It seeks to represent the needs of the organization and the needs of the users/consumers of intelligence while embracing the lessons learned or best practices of other organizations, all tailored to meet the needs of the law enforcement agency.

Figure 14-1 illustrates the development process. The series of progressive activities, illustrated on the top row of Figure 14-1, are intended to clarify the operational concept of a new organizational activity, in this case a new intelligence structure. The bottom row represents functional components required to develop the concept. Specifically, to establish goals, one needs to know the intended purpose of the program, which will be strongly directed by the chief executive's vision of the program. This vision must be shared with the staff members who will develop and operate the program. Once the goals are clear, the ConOps can evolve to develop an intelligence structure that can accomplish those goals.

FIGURE 14-1: PROCESS FOR THE DEVELOPMENT OF A CONCEPT OF OPERATIONS



The next conceptual step is to gather information related to the goals—for example, national standards (such as the NCISP and the *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector* [Fusion Center Guidelines]), lessons learned, and best practices from other agencies, as well as legal issues and other factors that may be idiosyncratic to the jurisdiction. The latter information often has to be gained from staff members and potential users of the new (or reengineered) intelligence structure. Based on the collective analysis of these facts, the

concept of how the new intelligence structure will work begins to take shape. Once again, two-way discussion with staff members and users is essential to ensure that the concept will work. One of the effective mechanisms to test this is to develop different information sharing and analytic scenarios to illustrate the concept. For example, if a new SAR process is to be part of the new intelligence structure, different scenarios of how the system would work can be developed with feedback sought from staff members and users on the strengths, weaknesses, and constraints of the system.

By developing scenarios for all aspects of the new intelligence enterprise, specific changes to or needs of the system can be identified and built into the concept. These needs will help define the operational requirements for the new intelligence structure to be successful—everything from office layout to training to new report forms. Once these have been identified, the final model, represented by the ConOps, can be prepared for review and consideration. The culmination of this process needs to be expressed in written form to fully communicate the new operational concept.

## CONTENTS OF A CONCEPT OF OPERATIONS

There are different models of ConOps, each of which will always need to be adapted to meet the unique needs of any given agency or fusion center. The following model, broadly based on a model used by the U.S. Department of Health and Human Services<sup>1009</sup> (HHS), provides a blending of the more common elements found in a ConOps as used by a law enforcement agency.

### Title Page

### Table of Contents

### List of Figures

### List of Tables

#### 1. Introduction

Summarize the purpose of the document, the scope of activities that resulted in its development, its relationship to other relevant plans or standards, the intended audience for the ConOps, and expected evolution of the document. Also describe any security or privacy considerations associated with use of the ConOps.

#### 2. Referenced Documents

Provide identifying information for all documents referenced within the ConOps (e.g., NCISP, *Fusion Center Guidelines*, 28 CFR Part 23, as well as legislation, feasibility studies, or any other relevant documentation).

#### 3. Current System or Situation

This section describes the intelligence structure as it currently exists. If there is no current intelligence structure on which to base changes, then describe the situation that motivates development of the proposed intelligence unit.

##### 3.1. Background, Objectives, and Scope

Provide an overview of the current intelligence structure, including, as applicable, background, mission, goals, objectives, scope, and responsibilities for the current intelligence structure.

##### 3.2 Operational Policies and Constraints

Describe the operational policies and constraints affecting the operations of the current intelligence

### RELEVANT DEFINITIONS

- ◆ **Concept of Operations**—Articulates the concept and vision of a new organizational entity.
- ◆ **Business Plan**—Takes the ConOps to the next step. The business plan establishes functional processes, implementation strategies, and daily operations of the organizational entity.
- ◆ **Implementation**—The process of making the concept a reality through the use of the business plan.

1009 <https://www.hhs.gov/sites/default/files/ocio/eplc-lifecycle-framework.pdf>

structure. Operational policies are predetermined management decisions regarding the operations of the current system, normally in the form of general statements or understandings that guide or limit decision-making activities, but they allow for some discretion. Operational constraints are limitations placed on the operations of the current system (e.g., available hours of intelligence unit operation, available number of personnel to work in the unit, networking constraints).

### **3.3. Description of Current System or Situation**

Provide a description of the current intelligence structure or situation that is simple and clear enough that all intended readers of the document can fully understand it. Provide a graphical overview of the current system or situation in the form of a context diagram, a top-level object diagram, or some other type of diagram that depicts the system and its environment. The description should include the following as appropriate:

- The operational environment and its characteristics (e.g., facilities, equipment, computing hardware, software, communications links, personnel, and operational procedures used to operate the existing system)
- Major system components and the interconnection among those components
- Interfaces to external systems or procedures
- Capabilities, functions, and features of the current intelligence structure, including types of products that are produced
- Charts and accompanying descriptions depicting inputs, outputs, data flows, control flows, and manual and automated processes sufficient to understand the current system or situation from the user's point of view
- Cost of system operations
- Operational risk factors
- Performance characteristics, such as speed, throughput, volume, and frequency of intelligence products
- Quality attributes, such as availability, correctness, efficiency, expandability, flexibility, interoperability, maintainability, portability, reliability, reusability, supportability, survivability, and usability
- Provisions for safety, security, privacy, integrity, and continuity of operations in emergencies that exert influence on the operation or operational environment of the current system

### **3.4. Current Modes of Operation**

Describe the various modes of operation for the current intelligence structure (e.g., normal, imminent threat, emergency event, natural disaster, etc.), including strengths and weaknesses.

### **3.5. Current Users and Stakeholders**

A user class is distinguished by the ways in which users interact with the current intelligence structure. Include descriptions of both internal and external intelligence users, how these users were identified, feedback from the users, and demands from users to which the intelligence structure is currently unable to respond.

### **3.6. Current Support Environment**

Describe the support environment for the current intelligence structure, including support organizations or units; facilities; equipment; support software; and any other aspect of support. For external partners of the intelligence structure, describe the roles and responsibilities and whether a memorandum of understanding (MOU) is in place.

## **4. Justification and Description of Changes**

Briefly describe the shortcomings or limitations of the current intelligence structure or the circumstances that motivated development of a new or modified intelligence structure.

If there is no current intelligence structure on which to base changes, then so indicate and provide justification for the new structure.

#### **4.1 Justification of Changes**

Briefly summarize new or modified aspects of the intelligence unit's operations, including the types of analysis, products, changes, or modified mission and the reasons for those changes. Changes may be based on new national standards, a new MOU, new strategic priorities of the executive, external funding requirements, legislation, or any of a variety of other factors.

It is important to articulate the reasons for change to ensure that the explicit conditions or mandates for the change are being met.

#### **4.2. Description of Desired Changes**

Summarize the new or modified capabilities, functions, processes, products, and other changes needed to respond to the factors identified in 4.1. Changes should be based on the current intelligence structure described in Section 3 above. If there is no existing intelligence structure on which to base changes, then summarize the capabilities to be provided by a new structure. This description should include the following, as appropriate:

- Capability changes
- Information processing changes
- Product changes
- Personnel changes
- Priority changes
- Partnership changes
- Support changes
- Other changes

#### **4.3 Priorities Among Changes**

Identify priorities among the desired changes and new features. Each change should be classified as essential, desirable, or optional and a reason provided for the classification.

#### **4.4. Changes Considered But Not Included**

Identify desired changes and new features considered but not included in Section 4.2 and the rationale for not including them.

### **5. Proposed System or Situation**

Describe the concepts for the proposed intelligence structure that results from the desired changes specified in Section 4 above. The description should be at a high level, indicating the operational features that are to be provided without specifying design details. The description should be of sufficient detail to fully explain how the proposed system is envisioned to operate in fulfilling users' needs and the law enforcement agency's business requirements. The ConOps may contain some examples of typical design strategies for the purpose of clarifying operational details of the proposed system but should not contain design specifications.

#### **5.1 Background, Objectives, and Scope**

Provide an overview of the proposed intelligence structure, including, as applicable, background, mission, goals, objectives, scope, business drivers, and motivation for the proposed structure.

#### **5.2 Operational Policies and Constraints**

Describe the operational policies and constraints affecting the operations of the proposed system. Operational policies are predetermined management decisions regarding the operations of the proposed system, normally in the form of general statements or understandings that guide or limit decision-making activities, but they allow for some discretion.

Operational constraints are limitations placed on the operations of the proposed system (e.g., available hours of system operation, available number of personnel to operate the system, computer hardware, and operational facilities constraints).

### 5.3 Description of the Proposed Intelligence Structure

Provide a description of the proposed intelligence structure that is simple and clear enough that all intended readers of the document can fully understand it. Provide a graphical overview of the proposed structure in the form of a context diagram, a top-level object diagram, relationship to other intelligence entities (particularly as applied to fusion centers), structure within an agency of governmental entity, or some other type of diagram that depicts the structure and its environment. The description should include the following as appropriate:

- The intelligence unit's environment and its characteristics (e.g., facilities, equipment, computing hardware, software, communications links, personnel, and operational procedures used for the unit's operations)
- Major law enforcement intelligence systems for which access is needed (e.g., RISS.NET, LEEP, HSIN, NLETS)
- Capabilities, functions, and features of the analytic capability including skills of analysts, analytic software and special skills needed)
- Charts and accompanying descriptions depicting inputs, outputs, data flows, control flows, and manual and automated processes sufficient to understand the two-way information flow for the intelligence structure
- Cost of intelligence structure's operations
- Operational risk factors (including civil rights and privacy issues)
- Performance characteristics, such as speed, throughput, volume, frequency
- Quality attributes, such as availability, correctness, efficiency, expandability, flexibility, interoperability, reliability, and usability of intelligence products
- Provisions for security, privacy, integrity, accuracy, and continuity of operations in emergencies for the new intelligence structure

### 5.4 Proposed Modes of Operation

Describe the various modes of operation for the proposed intelligence structure (e.g., normal, emergency, special threat). The intelligence structure's processes, procedures, and capabilities or functions should be related to each mode, as appropriate, perhaps using a cross-reference matrix.

### 5.5 Anticipated Users and Stakeholders

A user class is distinguished by the ways in which users interact with the proposed intelligence structure. Factors that distinguish a user class include common responsibilities, skill levels, work activities, and modes of interaction with the system.

In this context, a user is anyone who interacts with the proposed intelligence structure, including analysts, research specialists, reports officers, investigators, management decision makers, patrol officers, trainers, and perhaps certain segments of the private sector.

Specify the planned user class for the intelligence structure.

### 5.6 Proposed Support Environment

Describe the support concepts and support environment for the intelligence structure, including partner organizations; facilities; equipment; support software; and the information sharing environment of the intelligence structure.

## 6. Operational Scenarios

Provide step-by-step descriptions of how the intelligence structure should operate and interact with its users under a diverse set of circumstances (e.g., development of specific intelligence products as a result of a user's request; how Suspicious Activity Reports (SARs) are processed through the intelligence structure; how and to whom imminent threat information should be confirmed and disseminated). The scenarios should be described in a manner that will allow readers to walk through them and gain an understanding of how all the various parts of the proposed intelligence structure function.

The scenarios tie together all parts of the system, the users, and other entities by describing how they interact and may also be used to describe what the system should not do. The scenarios can be presented in several different ways: (1) for each major intelligence activity or function of the proposed structure; (2) thread-based, where each scenario follows one type of transaction type through the proposed structure; or (3) following the information flow through the system.

## 7. Summary of Impacts

Describe the anticipated operational and organizational impacts of the proposed intelligence structure on staff members, users/consumers, and management. Also, describe the temporary impacts on the staff, users/consumers, and management during the period of time when the new intelligence structure is under development and being implemented and when training is being provided. This information will allow all affected organizations and organizational units to prepare for the changes that will be brought about by the new structure and to plan for the impacts during development and transition to the new structure.

### 7.1 Operational Impacts

Describe the operational impacts of the proposed system on the users, system developers, and support and maintenance organizations. The impacts to consider include the following:

- Information sharing with primary or alternate information sources and/or systems
- Changes in procedures
- Use of new analytic methods and resources
- Changes in quantity, type, and timing of data to be input into the system
- Changes in intelligence requirements
- New modes of operation based on imminent threats and emergencies
- New processes for responding to user analytic requests
- Changes in the operational budget

### 7.2 Organizational Impacts

Describe the anticipated organizational impacts of the proposed intelligence structure, in comparison with current impacts on staff members, management, personnel, partners, and other users of the intelligence structure.

### 7.3 Impacts During Development

Describe the anticipated impacts on staff members, management, personnel, partners, and other users of the intelligence structure during the development of the new intelligence structure. The impacts to consider include the following:

- Involvement in studies, meetings, and discussions prior to implementation of the new structure
- User and support involvement in testing and review of new processes and methods, including training
- Parallel operation of the new and existing structure during transition

## 8. Analysis of the Proposed Intelligence Structure

Provide an analysis of the benefits, limitations, advantages, disadvantages, and alternatives and trade-offs considered for the proposed intelligence structure.

### 8.1 Summary of Improvements

Provide a qualitative (and, to the extent possible, quantitative) summary of the benefits to be provided by the proposed intelligence structure.

### 8.2 Disadvantages and Limitations

Provide a qualitative (and, to the extent possible, quantitative) summary of the disadvantages and/or limitations of the proposed intelligence structure. Disadvantages might include the need to retrain personnel or change to a new style of information sharing. Limitations might include products and services desired by users but not included as part of the new intelligence structure.

### 8.3 Alternatives and Trade-Offs Considered

Describe major alternatives considered, the trade-offs among them, and rationale for the decisions reached. In the context of the ConOps, alternatives are operational alternatives; for example, using shared or contract intelligence analysts; limiting the intelligence structure to only strategic or tactical analysis; and co-locating the new structure with another agency.

## Appendices

Utilize appendices to facilitate ease of use and maintenance of the ConOps. Each appendix should be referenced in the main body of the document where that information would normally have been provided; for example, samples of new report forms, new policies and procedures, etc.

## Glossary

Provide clear and concise definitions for terms used in the ConOps that may be unfamiliar to readers of the document.

## THE CONOPS NEXT STEP

As the name implies, the ConOps is intended to describe how the intelligence vision of the chief executive is conceptualized in an operational form—that is, the ConOps translates the vision into a functional model. The intent is to permit stakeholders—staff members, users, management, and relevant external parties—to understand the intended dynamics and comment on different aspects of the envisioned operations. Feedback by stakeholders may be used to fine-tune the concept, as long as it stays true to its vision. The next step is to use the ConOps as a road map to implement the new intelligence structure.

## IMPLEMENTING AND MANAGING THE INTELLIGENCE STRUCTURE

As noted previously, the principles of management apply to the intelligence function of an agency just as they apply to any other organizational entity. As such, the following management discussion focuses on selected elements related to the intelligence function. As will be seen, many of the issues in the following discussions will be applicable to preparing the ConOps.

### ESTABLISHING AN ORGANIZATIONAL FRAMEWORK

Just as any other function in a law enforcement agency, organizational attention must be given to the administrative structure of the intelligence function. Administrators and managers must examine:

- ◆ The need for the intelligence function as related to strategic priorities of the agency.
- ◆ How the intelligence structure functions on a daily basis.
- ◆ Issues of resource acquisition, deployment, and management.
- ◆ Future agency requirements for the intelligence function.

Properly organized and staffed, the intelligence function serves as an internal consultant to management for resource deployment. It should be designed as an integrated and organic element of the law enforcement organization, not a distinct function. Indeed, this approach supports the effective implementation of ILP. Intelligence defines the scope and dimensions of complex criminality—including terrorism—facing the jurisdiction and provides alternatives for policy responses to those problems. Importantly, it also serves as a focal point for information sharing and dissemination to maximize community safety.

Some law enforcement agencies have been reluctant to fully develop an intelligence structure—including both tactical and strategic activities—for several reasons. Perhaps at the top of the list are the past abuses and subsequent lawsuits from poorly organized and managed intelligence activities. In many cases, law enforcement executives eliminated the intelligence function to reduce liability and to minimize criticism from persons in the community who did not understand the intelligence role and/or generally opposed law enforcement intelligence for philosophical reasons. Similarly, the need for and value of an intelligence function has not been fully recognized by managers who often do not understand that the intelligence function can be an important resource for agency planning and operations. For example, intelligence analysts are frequently assigned clerical tasks—e.g., responding to requests to check names or doing a records search of a person’s background—in addition to their analytic duties, largely because the manager does not understand the value that is lost to the organization if the analyst does not have the time to devote to his or her function.

As a consequence of several factors, the zeitgeist—or spirit of the times—is now present for American law enforcement to embrace law enforcement intelligence of the 21st century. Many SLTLE agencies have established a legacy of proactive law enforcement through the use of community policing and its activities of problem solving, CompStat, crime analysis, effective internal and external communications, multidisciplinary responses to crime, and a “bottom-up” approach for operational direction. Moreover, since the 9/11 attacks, there has been a greater development of resources and training to make intelligence activities more easily adapted and functional. Finally, the law enforcement intelligence function has become professionalized through greater involvement of academic institutions, federal initiatives, and long-standing activities by groups such as the IALEIA and the LEIU.<sup>1010</sup>

## “CHARTERING” AN INTELLIGENCE UNIT

One of the first steps in creating an intelligence structure is to “charter” the function. This includes:

- ◆ Determining its organizational structural priority and placement.
- ◆ Resource allocation.
- ◆ Defining its mission and goals.
- ◆ Establishing the unit’s authority and responsibility.

A number of publications describe these processes.<sup>1011</sup> The current discussion will identify specific points related

---

1010 For more information on these organizations, see their respective Web pages at <http://www.ialeia.org> and <http://www.leiu-homepage.org>.

1011 Most police management textbooks describe these processes in detail. Perhaps of particular value are publications available from the International City Management Association, <https://icma.org/publications>.

o the intelligence function. The creation of an intelligence function should be based on a needs assessment.<sup>1012</sup> This includes identifying *current* intelligence-related competencies of the law enforcement agency and *desired* competencies. One of the main outcomes of an effective needs assessment is identifying how an intelligence structure can influence the drive toward greater efficiency and responsiveness. Importantly, the needs assessment will also define personnel and resource needs.

Resource allocation is always a difficult process because it typically involves diminishing one function to develop another. In most cases, the creation of a new unit will not come with a new appropriation of funding to fully staff and operationalize it. Therefore, part of the resource allocation process is to determine where the intelligence function fits into the organizational priorities of the law enforcement agency.

The mission of the intelligence function is the *role* that the unit fulfills in support of the agency's overall mission. It specifies in general language *what* the unit intends to accomplish and articulates the *direction and responsibility* of the intelligence structure, which all other administrative actions and activities are designed to fulfill. Table 14-2 presents a sample mission statement for a law enforcement agency's intelligence unit.

A goal is the end to which all activity in the unit is directed. It is broad-based, yet *functionally* oriented. Importantly, the goal must be *mission-related*; that is, accomplishing goals supports the broader mission of the law enforcement agency. Moreover, the goals will give the unit direction in support of the mission. Since the mission of an intelligence unit will be comprehensive and incorporate diverse functions, several goals will be stipulated. The purpose of goals is not only to provide operational direction but also to serve as performance standards.<sup>1013</sup> The environment of the community will change over time, as will crime patterns and problems; therefore, the law enforcement agency should review goal statements annually and change or revise them to reflect current issues and trends. (Table 14-2 also includes an illustration of intelligence *goals* for a law enforcement agency.)

Authority is the right to act or command others to act toward the attainment of organizational goals. Operational authority includes decisions that must be made concerning the degree and types of activities the intelligence function may perform without seeking administrative authorization, financial flexibility of the unit to fulfill its objectives, and the degree of direction or precedence the intelligence structure can exercise over other departmental units. Each of these factors has significant organizational implications and must be developed conceptually and stipulated by policy.

**Responsibility** reflects how the authority of a unit or individual is used for determining whether goals have been accomplished and the mission fulfilled in a manner consistent with the defined limits of authority. The unit and its members must be held accountable for its charge, and administrative mechanisms must be set in place to assess the degree to which the unit is meeting its responsibilities.

**IACP Model Policy on Criminal Intelligence.** The International Association of Chiefs of Police (IACP) has taken a proactive role in all aspects of developing a contemporary intelligence capacity in America's law enforcement agencies. The IACP *Model Policy*<sup>1014</sup> *on Criminal Intelligence* provides a policy statement and procedures that are of particular benefit to a small agency. As in the case of all models, the language of the IACP policy needs to be adjusted to meet the needs of different jurisdictions. Nonetheless, it provides a sound foundation for starting the process.

---

1012 An illustration of a needs assessment can be found at the National Highway Traffic Safety Administration, [https://one.nhtsa.gov/people/injury/alcohol/Community%20Guides%20HTML/Book2\\_NeedsAssess.html](https://one.nhtsa.gov/people/injury/alcohol/Community%20Guides%20HTML/Book2_NeedsAssess.html).

1013 Performance standards are often characterized as effectiveness and efficiency, wherein effectiveness is "doing the right job" and efficiency is "doing the job right."

1014 [https://www.ncirc.gov/documents/public/criminal\\_intelligence\\_model\\_policy.pdf](https://www.ncirc.gov/documents/public/criminal_intelligence_model_policy.pdf)

TABLE 14-2: SAMPLE MISSION STATEMENT AND GOALS OF AN LEIU

### SAMPLE INTELLIGENCE MISSION STATEMENT

The mission of the Intelligence Unit of the Hypothetical Police Department is to collect, evaluate, analyze, and disseminate intelligence data regarding criminal activity in this city/county and any criminal activity in other jurisdictions that may adversely affect this city/county. This includes providing processes for collating and analyzing information collected by operational units of the law enforcement agency. The Intelligence Unit will furnish the chief of police with the necessary information so that Operations Units charged with the arrest responsibility can take the necessary enforcement action.

### SAMPLE INTELLIGENCE GOALS

1. The Intelligence Unit shall supply the chief of police with accurate and current strategic intelligence data so that the chief will be kept informed of changing criminal activity in the jurisdiction.
2. The Intelligence Unit shall provide a descriptive analysis of organized crime systems operating within the jurisdiction to provide operational units with the necessary data to identify organized crime groups and individuals working as criminal enterprises.
3. The Intelligence Unit will concentrate its expertise on the following crimes:
  - a. **Islamic extremists in support of terrorism**—activities, participants, funding, and logistical support, all of which are of a criminal nature.
  - b. **Domestic extremists in support of criminal acts**—activities, participants, funding, and logistical support, all of which are of a criminal nature.
  - c. **Labor/strike activity**—monitor and gather strategic intelligence to be supplied to the Operations Bureau with regard to this activity.
  - d. **Organized crime**—identify crimes and participants, including new and emerging criminal enterprises.
  - e. **Major narcotics traffickers**—provide tactical intelligence and information analysis to the Operations Bureau on persons identified as being involved in narcotics trafficking enterprises.

The Intelligence Unit recognizes the delicate balance between the individual rights of citizens and the legitimate needs of law enforcement. In light of this recognition, the unit will perform all of its intelligence activities in a manner that is consistent with and upholds the civil rights, privacy, and lawful expressive activity of all persons.

## AUDITING THE INTELLIGENCE FUNCTION

An important tool for managing the intelligence function is performing regular audits. An audit provides an accountability mechanism that can help maximize efficiency and effectiveness while verifying adherence to policies and procedures. In addition, the audit can serve as a benchmarking tool to measure changes in performance of the intelligence function which, in turn, leads to continuous quality improvement.

The audit is not only an important management tool; it can also serve as a means to demonstrate accountability to the community. It is a structured method to track and measure critical issues related to the intelligence function and provide assurances that the intelligence function is operating in a manner that is consistent with good management practices and within lawful constraints.

There are different types of audits, depending on the needs or issues associated with the intelligence function. In all likelihood, a law enforcement agency should perform diverse types of audits on a periodic basis. The types of audits include the following:

- ◆ **Financial audit**—to ensure that the expenditure of funds is consistent with policy and allowable expenses, including appropriated funds and grant funds. In addition, if there is an undercover/informant budget, this should be audited on a regular basis.
- ◆ **Process audit**—to ensure that all intelligence activities are being performed in a manner that is consistent with the law enforcement agency’s internal policies and procedures. This audit includes not only the activities of line personnel but also those of supervisors, demonstrating whether they are adequately performing their supervisory functions.
- ◆ **Compliance audit**—to ensure that intelligence operations are consistent with law and regulations that are external to the organization, such as 28 CFR Part 23, legal mandates, grant regulations, etc.
- ◆ **Outcome audit**—to ensure that the intelligence function is accomplishing its goals and objectives.
- ◆ **Service audit**—to ensure that the intelligence function is meeting the needs of its consumers.

The person(s) conducting the audit may be somewhat dependent on the nature of the issues associated with the intelligence function, both internal and external to the law enforcement agency, associated with the intelligence function. If there are no controversies associated with the intelligence function, then an audit by a supervisor should suffice. However, if there are controversial issues related to intelligence operations, an external auditor would be preferable. For example, someone who has recognized integrity, such as a retired judge or a recognized businessperson who is a community leader, would serve well as an auditor. While the intelligence staff will need to provide the raw information to the auditor, an independent party asking questions, making judgements, and drawing conclusions about performance can serve an important role.

Appendix C contains an audit checklist developed by the author and used at law enforcement agencies to ensure compliance with court orders. Appendix D is the audit checklist developed by the LEIU.

## ESTABLISHING AND MANAGING PARTNERSHIPS

The nature of the intelligence function requires that a law enforcement agency enter into partnerships. Critical information is shared through collaboration, typically with other law enforcement agencies, but often with other organizations ranging from the private sector (as discussed in Chapter 9) to non-law enforcement government agencies, such as public health, the fire service, or emergency operations. These various relationships have different dynamics related to needs, responsibilities, and limitations on access to information. As such, the parameters of each formal partnership should be articulated in a formal partnership agreement.

Broadly speaking, two types of partnerships are related to the intelligence function. These are:

- ◆ **Users:** Organizations and individuals with which information and/or intelligence products are shared. Users are consumers.
- ◆ **Participants:** Organizations and individuals that provide resources and actively contribute to the intelligence activity, such as a regional fusion center. Participants have a shared responsibility for operations.

A formal agreement is sound management because it articulates mutually agreed-on operational provisions related to resource management; clear identification of responsibilities and accountability; adherence to legal standards; and conditions associated with liability. Certainly, these agreements apply to a wide range of law enforcement activities or services; however, the current discussion is limited to the intelligence function. While the language varies between states, as a general rule there are three forms of written partnerships:

- ◆ **Memorandum of agreement (MOA):** Users/consumers of an intelligence unit or system, including a records system, that use the system on an ongoing basis would typically sign the MOA. Essentially, the MOA acknowledges that the user will abide by the rules established for the system or activity, aid in cost recovery,

and adhere to legal and accountability standards. Obviously, the character of the activity will dictate more detail. As an example, if one agency's intelligence records system can be accessed by another agency, the user may have to agree to pay a monthly fee, adhere to 28 CFR Part 23, and agree to the Third Agency Rule. Failure to meet these standards will result in losing access to the system.

- ◆ **Mutual aid pact (MAP):** The MAP is an agreement that is in place to deal with special circumstances, rather than an ongoing service, and establishes the agreed-on conditions for which one agency will provide assistance to another. Often, assistance is reciprocal, except for real costs that may be incurred in extended activities. As an intelligence-related example, two law enforcement agencies may agree to aid each other when conducting a surveillance.
- ◆ **Memorandum of understanding (MOU):** The MOU is more detailed and involves a partnership in an activity. Essentially a contract, the MOU specifies all obligations and responsibilities and typically shares liabilities in the endeavor. For example, if multiple agencies agree to develop a fusion center, the MOU may be a fairly detailed document outlining all aspects of governance, management, structure, funding, accountability, and operations of the center.

A key element to understand is that, regardless of the nature of the agreement, its content and detail is to ensure that all parties understand their obligations. Table 14-3 identifies some of the provisions that may be included in a partnership agreement. While not all of these provisions will be required of every agreement, it is important to have a formal document that clearly defines expectations and responsibilities.

**TABLE 14-3: SAMPLE PROVISIONS FOR A PARTNERSHIP AGREEMENT**

◆ Activities	◆ Operating procedures
◆ Civil liability/indemnification	◆ Payments and costs
◆ Dispute resolution	◆ Personnel assignment
◆ Funding	◆ Personnel evaluation
◆ Governance	◆ Personnel removal
◆ Information—access and use	◆ Physical plant considerations
◆ Information—adherence to 28 CFR Part 23	◆ Property—purchase and maintenance
◆ Information—dissemination to Third Agency	◆ Reports to be prepared
◆ Information—entry into a system	◆ Security clearances of staff
◆ Information—ownership	◆ Security of information
◆ Location	◆ Security of the facility
◆ Mission, purpose, goals	◆ Time limit/term of the agreement

## PROGRAM EVALUATION

Just like any organizational entity, the intelligence function needs to be evaluated to aid in the improvement and accountability of intelligence processes and services. Since a goal of the intelligence function is to prevent crime, some argue that it cannot be accurately evaluated because it is impossible to measure crime that has been prevented. While measuring crime prevented is an unreliable metric, there are other factors that can be measured and evaluated.

The intent of program evaluation is to measure effectiveness and efficiency. Effectiveness measures whether objectives are being accomplished—this is outcome evaluation. As a simple example, an objective of a fusion center may be to have “80 percent of the law enforcement agencies in the state consistently participating in the suspicious activity reporting program.” Within this objective, there must be operational definitions. For purposes of this objective, does “law enforcement agencies” include tribal law enforcement, conservation agents, alcoholic

beverage control agents, federal agencies with offices/agents in the state, etc.? What is meant by “consistently”? What is meant by “participate”? While a person may have an intuitive understanding of these terms and phrases, for purposes of measurement they must be explicitly defined.

Efficiency measures whether the intelligence unit is using resources wisely—this is process evaluation. For example, an intelligence unit purchases five site licenses for the use of I2 Analyst Notebook software, which is powerful, yet expensive, analytic software. For purposes of efficiency, questions may include the following: Are all five site licenses being consistently used? Are analysts using the full capacity of the software? Is the software providing the types of tools and outputs needed to accomplish its objectives? Again, definitions are needed for “consistently used,” “full capacity,” and “outputs needed” because these are the variables being measured to determine efficiency. The results may show that only three site licenses are needed, thereby saving money. The results may also show that the software is not being used to full capacity, indicating a need for further training of the analysts. If the software is not meeting “outputs needed,” this could be a software issue, a training issue, or a reexamination of the objectives. All of these are factors that can be measured to ensure that resources and expenditures are being used wisely to maximize their results.

It is important to remember that any evaluation must be performed as measured against true objectives, not assumed objectives. For example, the Congressional Research Service (CRS) examined fusion centers from an overall comprehensive perspective. However, the CRS report criticized fusion centers as being:

...parochial—by focusing largely on criminal intelligence relevant to the state and locality alone—and not issues pertaining to federal homeland security concerns.<sup>1015</sup>

In reality, this criticism—often referred to as “mission creep”—was inaccurate because the CRS assessed the wrong criteria. As discussed in Chapter 8, fusion centers are the creation of state and local government and have a primary responsibility defining the threats to their community—which are usually criminal threats, not homeland security threats. The primary responsibility of fusion centers is not federal homeland security concerns, although they contribute to homeland security. This CRS assessment brought significant, unwarranted criticisms to fusion centers from the news media as well as from civil liberties organizations such as the American Civil Liberties Union (ACLU),<sup>1016</sup> many of which extrapolated from the comment to make erroneous assumptions. This illustrates the importance of evaluating a program or initiative against stated criteria, not assumed or inaccurate criteria.

The methodologies for program evaluation are essentially the same as for any type of applied research and can be either quantitative or qualitative. The key is to have operational variables based on the stated objectives of the intelligence function. Examples of methods and measures include the following:

- ◆ Real versus expected outcomes of intelligence products and activities.
- ◆ Before-and-after comparisons of outcomes related to intelligence products and activities.
- ◆ Assessment of quantitative actions and results to intelligence outputs by consumers.
- ◆ Assessment of administrative expectations compared with intelligence accomplishments.
- ◆ Assessment of the intelligence function’s contributory value to law enforcement agency’s mission.
- ◆ Assessment of the quality, accuracy, and utility of the intelligence function’s outputs.
- ◆ Efficiency of the intelligence function’s processes and intelligence production.

---

1015 *Fusion Centers; Issues and Options for Congress*. (2008). Washington, DC: Congressional Research Service, p. 45. <https://fas.org/sgp/crs/intel/RL34070.pdf>

1016 [https://www.aclu.org/sites/default/files/pdfs/privacy/fusion\\_update\\_20080729.pdf](https://www.aclu.org/sites/default/files/pdfs/privacy/fusion_update_20080729.pdf)

While these illustrations serve as a foundation, the key is to measure the intelligence function's work against the expectations defined by the objectives. The results may not be as satisfying as attempting to measure prevented crime; however, this approach can help identify strengths, successes, and weaknesses that need to be addressed.

## SOURCES FOR INTELLIGENCE MANAGEMENT AND RESOURCE TRENDS

Effective management of an intelligence unit requires that the manager be constantly informed of emerging issues, technologies, and trends. This is a difficult process; however, one of the more effective methods is to monitor online newsletters and resources of reliable organizations. Topics can range from emerging issues to best practices to new products and new policy and legislation. As an illustration (not an endorsement), some of the more substantive online resources (in alphabetical order) include the following:

- ◆ Bureau of Justice Assistance (BJA) Open Source Analysis: <https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide>.
- ◆ BJA, National Criminal Intelligence Resource Center: <https://www.ncirc.gov/>.
- ◆ Computerworld—Computer Forensics Resources: <https://www.computerworld.com/article/2577697/security0/computer-forensics-resources.html>.
- ◆ Criminal Intelligence Coordinating Council (CICC): <http://it.ojp.gov/global/working-groups/cicc/resources>.
- ◆ CICC Five in 5 Newsletter Subscription: <https://confirmsubscription.com/h/t/240A298327414519>.
- ◆ Criminal Intelligence Resources Guide: [https://www.it.ojp.gov/documents/d/criminal%20intelligence%20resources%20guide\\_compliant.pdf](https://www.it.ojp.gov/documents/d/criminal%20intelligence%20resources%20guide_compliant.pdf).
- ◆ Cryptome: <http://cryptome.org/>.
- ◆ Department of Homeland Security (DHS) Newsletters: <https://www.dhs.gov/publication/newsletters>.
- ◆ DHS Combating Cyber Crime Resources: <https://www.dhs.gov/topic/combating-cyber-crime>.
- ◆ DHS Information Sharing: <https://www.dhs.gov/topic/cybersecurity-information-sharing>.
- ◆ DHS State and Major Urban Area Fusion Centers: <http://www.dhs.gov/state-and-major-urban-area-fusion-centers>.
- ◆ Department of Justice (DOJ) Information Sharing: <https://www.justice.gov/otj/information-sharing>.
- ◆ DOJ, Justice Technology Information Center: <https://www.justnet.org/>.
- ◆ Domestic Security Alliance Council: <https://www.dsac.gov/topics/cyber-resources>.
- ◆ Electronic Privacy Information Center (EPIC) Privacy Concerns for Intelligence: <http://epic.org/privacy/fusion/>.
- ◆ Federal Computer Week: <https://fcw.com/home.aspx>.
- ◆ Federation of American Scientists—a rich resource of open source documents on a wide range of issues not readily or easily available from other sources: <http://fas.org/>.
- ◆ Federation of American Scientists Secrecy News: <http://www.fas.org/sgp/news/secrecy/>.
- ◆ Foundation for Defense of Democracies Weekly Update: <https://www.fdd.org/>.
- ◆ Global Intelligence Working Group, Fusion Centers and Intelligence Sharing Resources: <https://it.ojp.gov/initiatives/fusion-centers>.
- ◆ Global Justice Information Sharing Initiative, Privacy and Civil Rights Resources for Intelligence: <http://it.ojp.gov/PrivacyLiberty>.
- ◆ Government Computer News: <https://gcn.com/Home.aspx>.

- ◆ Government Executive News and Newsletters: <https://www.govexec.com/>.
- ◆ Government Technology Magazine and Newsletters: <https://www.govtech.com/>.
- ◆ Homeland Security Today Newsletter: <https://www.hstoday.us/>.
- ◆ IACP Center for Social Media: <http://www.iacpsocialmedia.org/>.
- ◆ INFOSEC Institute—Privacy Implications for License Plate Readers: <https://resources.infosecinstitute.com/privacy-implications-automatic-license-plate-recognition-technology/#gref>.
- ◆ IntelTechniques: <https://inteltechniques.com/>.
- ◆ International Association of Law Enforcement Intelligence Analysts (IALEIA): <http://www.ialeia.org/>.
- ◆ Internet Crime Complaint Center: <https://www.ic3.gov/default.aspx>.
- ◆ Law Enforcement Information Sharing: <https://www.ise.gov/law-enforcement-information-sharing>.
- ◆ National Fusion Center Association: <https://nfcausa.org/>.
- ◆ National White Collar Crime Center (NW3C) Cyber Crime Links: <http://www.nw3c.org/services/research/cyber-crime-links>.
- ◆ New York Police Department Shield: <https://www.nypdshield.org/public/>.
- ◆ Open Source Solutions: <http://www.oss.net/>.
- ◆ PoliceOne.com (Law Enforcement News): <https://www.policeone.com/>.
- ◆ RAND Emerging Technology Trends and Their Impact on Criminal Justice: [https://www.rand.org/pubs/research\\_briefs/RB9996.html](https://www.rand.org/pubs/research_briefs/RB9996.html).
- ◆ SEARCH High-Tech Crime Investigation: <http://www.search.org/solutions/high-tech-crime-investigation/>.
- ◆ Smart Policing Initiative: <https://bja.ojp.gov/program/smart-policing-initiative-spi/overview>.
- ◆ TerraServer—comprehensive satellite imagery: <http://www.terraserver.com/>.
- ◆ The Association of Law Enforcement Intelligence Units (LEIU): <http://leiu.org/>.
- ◆ The Marshall Project on Police Technology: <https://www.themarshallproject.org/records/247-police-technology#.xcuWTe5TQ>.
- ◆ U.S. Computer Emergency Readiness Team (CERT): <https://www.us-cert.gov/>.
- ◆ Victims of Cyber Crime Information and Resources: <https://resources.lawinfo.com/criminal-defense/computer-crime/>.

As is the case with any information, a resource often reflects the agenda of its sponsor. Keeping this in mind, an intelligence manager can gain valuable information to remain current on the issues for which a manager is responsible.

## HUMAN RESOURCE ISSUES

Who should perform information collection and intelligence analysis in an SLTLE agency, and what qualifications should those persons have? This question is impossible to answer conclusively because it depends on a myriad of variables tied to the attributes of a given law enforcement agency. The agency's size, jurisdiction, and geographic location; the priority intelligence is given; resource flexibility; competing crime and calls for service issues; and collective bargaining agreements must be calculated into the formula. Rather than provide for the ideal situation,

this discussion will present issues and guidelines that will enable law enforcement executives to make informed decisions about options available for staffing the intelligence function.

## STAFFING

Clerical and support staffing decisions can be made for the intelligence function just as for any other assignment in the agency, taking into consideration professional staff workloads, service demands, nonprofessional work activities (e.g., data entry, clerical work), and budget, among others. The key positions are with the professional staff.<sup>1017</sup>

**The intelligence analyst.** The intelligence analyst is a professional who collects various facts, documents, circumstances, evidence, interviews, and other material related to a crime or threat and places them in a logical, related framework to develop a threat analysis, explain a criminal phenomenon, describe crime and crime trends, and sometimes develop a criminal case. The analyst should have at least a baccalaureate degree and receive training in the intelligence process, research methods, criminal law and procedure, statistical analysis, and factual and evidentiary analysis. The analyst should be an objective, analytic thinker with good writing and presentation skills. This is a professional position that should be compensated accordingly. Remember: Executives and managers make important operational and resource decisions based on the analysis of information and data. Hence, having the best-qualified and best-trained analysts is essential.

As noted previously, an ongoing issue is whether the intelligence analyst will be sworn or nonsworn. Different agencies use different models, each with its advantages and disadvantages. Those who advocate that the intelligence analyst position would be best served by a nonsworn employee argue that a nonsworn analyst's characteristics and background may provide a more creative and less restrictive view of data when compared with the backgrounds of sworn personnel. Further, a sworn employee is likely to be either transferred or promoted out of the intelligence unit, thereby reducing the unit's overall efficiency. Advocates of having a nonsworn employee argue that the position does not require law enforcement authority; therefore, placing a sworn person in an analyst's position may be viewed as an ineffective use of personnel. Finally, the role of an analyst is highly experiential: Over the years, an experienced analyst accumulates a mental repository of names, locations, businesses, and so forth that can be highly useful in an analysis. If this person is a sworn employee who is transferred out of the unit, that accumulated knowledge is lost.

---

1017 For more detail, see Wells, I. (2000). "Staffing the Intelligence Unit." (2000). *Intelligence 2000: Revising the Basic Elements*. A joint publication of the Association of Law Enforcement Intelligence Units and the International Association of Law Enforcement Intelligence Analysts, pp. 53–66.

## WHAT CHARACTERISTICS ARE DESIRED IN A GOOD ANALYST?

- ◆ General factors [modified from Frost (1984)]
  - Impeccable standards of honesty and integrity
  - A thorough understanding of the concepts of
    - Intelligence
    - Civil liberties
    - Criminal law enforcement
  - The capacity to think in a logical and rational manner
  - The capacity to approach situations from broad and divergent perspectives
  - The ability to comprehend complex masses of data and communicate its contents to others
- ◆ Background factors
  - Broad range of interests
  - Developed research ability (library, qualitative, quantitative)
  - Helpful previous experience (law enforcement, military, security, etc.)
- ◆ Mental traits
  - Intellectual curiosity
  - Rapid assimilation of information
  - Keen recall of information
  - Tenacity
  - Willingness and capacity to make judgments
- ◆ Communication skills
  - Developed writing ability
  - Skill in oral briefing
  - Interviewing and interrogation skills
  - Skill in eliciting information from officers
- ◆ "Liberal arts" skills
  - Good writing ability
  - Fluency in a second language (desirable)
  - Good knowledge of geography
- ◆ Working style
  - Initiative and self-direction
  - Effective personal interaction
  - Disciplined intellectual courage

Conversely, opponents argue that nonsworn employees do not have the substantive knowledge and experience for conducting investigations, nor do they understand, with the same degree of insight, the life of the street where many intelligence targets live and operate. The analyst builds his or her expertise and knowledge cumulatively throughout the work life. Much of this expertise is substantive knowledge and information (persons, crime patterns, locations, and so forth) learned while working on a variety of criminal cases. The analyst needs to view crime problems from the big picture—a picture that is most precisely focused with years of law enforcement street experience.

Other factors not related to the conceptual responsibilities enter the equation, such as the compensation package, collective bargaining agreement provisions, civil service regulations, organizational culture, the candidate pool, and so forth. This is a critical position requiring an effective analytic capability, and care should be taken to hire the right person to fit the agency's needs. It should not be, as has too often been the case, an appointment of convenience or a "reward appointment" to a good clerical person who has worked hard for the department. Professional output from the intelligence unit will occur only if the position is filled by a professional analyst.

To this end, the CICC developed the *Analyst Professional Development Road Map*, the purpose of which is:

. . .to create a sustainable, professional career path for analysts operating within federal, state, local, tribal, and territorial organizations. This path focuses on the development and enhancement of analytic knowledge, skills, and abilities over four successive analyst levels (basic, intermediate, advanced, and supervisory) and the training recommended for achieving each level. Historically, crime analysts and intelligence analysts have been viewed as having different career paths, but this is no longer the case. Analysts now operate in a hybrid environment dealing with national intelligence as well as criminal intelligence, often working with a combination of fusion centers, task forces, investigators, etc.<sup>1018</sup>

Two important aspects to be noted are the need for a professional career path for analysts and the need for continued training to continually refine skills, apply new technologies to intelligence analysis, and effectively address the changing criminal environment. Law enforcement agencies can perform more efficiently and effectively using the products of analysts. However, the analyst must be given the skills, knowledge, and professional career motivation to be most effective.

## TRAINING

A needs assessment of intelligence training conducted by the BJA-funded Criminal Intelligence Training Coordination Strategy Working Group found, among other things, that:

- ◆ Training is lacking in all of the training classifications. However, respondents rated intelligence analyst and intelligence manager as the classes most lacking in adequate training. While 62 percent of respondents stated they are receiving adequate training, more than a third (36 percent) indicated that they were not receiving adequate training.
- ◆ The majority of respondents cited lack of funding as the primary impediment of training, but respondents also rated high on difficulty in finding good trainers, travel and lodging costs, and unsure of available training. Only a handful of respondents selected unsure of appropriate training for personnel as an impediment. One respondent indicated that to support the tenets of the NCISP, additional training guidelines and opportunities are needed. Other respondents indicated that training can be sporadic, which dovetails with the need for core minimum standards that can be used consistently nationwide. Other respondents indicated that their

---

1018 *Analyst Professional Development Road Map, Version 2.0.* (2019). Washington, DC: Criminal Intelligence Coordinating Council, Global Justice Information Sharing Initiative. <https://it.ojp.gov/GIST/1210/Analyst-Professional-Development-Road-Map--Version-2-0>

agencies have not needed intelligence training because they do not have the staff or resources to engage in an intelligence function.<sup>1019</sup> (Emphasis in original.)

As a result of these findings, the *Minimum Criminal Intelligence Training Standards*<sup>1020</sup> were created and later revised. The standards were designed to “. . . provide perspective and guidance for the development and delivery of law enforcement intelligence training.”<sup>1021</sup> The report goes on to note that:

. . .It is recognized that any type of “standard” can be debated based on an individual’s personal philosophy, professional priorities, and life experiences. In order to minimize bias or atypical context, the development process for these standards used a consensual approach reflecting the cumulative judgment of law enforcement intelligence practitioners, managers, executives, trainers, and scholars from all levels of government. The standards reflect the collective judgment of these subject-matter experts (SMEs) with respect to the minimum training needed in each noted classification to provide the basic knowledge, skills, and abilities for personnel in each classification in order for them to perform their intelligence duties.<sup>1022</sup>

Clearly, intelligence training currently represents the proverbial mixed bag of content, availability, and structure. The content or subject matter of law enforcement intelligence can be divided in two broad categories. The first is *protocols and methodology of the intelligence process*. This includes subjects such as information collection methodologies; laws and regulations associated with intelligence records systems; analytic methods and tools; intelligence reporting structures and processes; and intelligence dissemination. These elements constitute the discipline of law enforcement intelligence.

The second category is somewhat more amorphous. Broadly speaking, this is *subject-matter expertise*. It includes understanding the motives, methods, targets, and/or commodities of criminal intelligence targets. Intelligence researchers and analysts must have subject-matter knowledge of the types of enterprises that are being investigated and the context within which these enterprises occur. Whether the target crime is criminal extremism, drug trafficking, money laundering, or the trafficking of stolen arts and antiquities, the intelligence analyst must have subject-matter knowledge on the genre of criminality being investigated, both in general as well as with the unique facts associated with a specific investigation.

---

1019 Bureau of Justice Assistance, Criminal Intelligence Training Coordination Strategy Working Group. (2004). *Survey of Law Enforcement on Intelligence Training*. Unpublished staff report.

1020 [https://it.ojp.gov/documents/minimum\\_criminal\\_intel\\_training\\_standards.pdf](https://it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf)

1021 Intelligence Training Coordination Working Group. (2007). *Minimum Criminal Intelligence Training Standards*. Washington, DC: Global Intelligence Working Group, p. 1.

1022 Ibid.

TABLE 14-4: INTELLIGENCE TRAINING CATEGORIES AND DESCRIPTIONS

TRAINING CATEGORY	DESCRIPTION
AWARENESS	The broadest, most diverse, types of intelligence training could best be described as “awareness” training. These programs, which vary in length, tend to include information about the intelligence discipline (e.g., definitions, methods, processes) as integrated with a specific subject matter (e.g., drugs, terrorism, gangs). The BJA State and Local Anti-Terrorism Training (SLATT) Program, the Federal Law Enforcement Training Centers (FLETC), and other groups offer this training throughout the United States.
INTELLIGENCE ANALYST	Intelligence analyst training programs have a reasonable degree of consistency in the subject-matter topics; however, the hours of training on each topic have more variability. In some cases, the curricula include substantive modules on subject matter; for example, the DHS/Federal Emergency Management Agency (FEMA) Basic Intelligence and Threat Analysis course. The most widely used analytic training program is the Foundations of Intelligence Analysis Training <sup>1023</sup> (FIAT), developed by IALEIA and LEIU and also offered by the NW3C. <sup>1024</sup>
INVESTIGATORS AND INTELLIGENCE UNIT RESEARCHERS	Some intelligence training programs exist which lack the depth of training found in the analyst curricula but are more detailed than simply awareness training. It appears that the intended audience for these programs is investigators, investigative analysts, or intelligence researchers. In each of the cases, the curricula are similar. Notable among these courses are the FLETC intelligence courses.
EXECUTIVE AND MANAGEMENT ISSUES FOR INTELLIGENCE	Two programs funded by BJA are in this category: Criminal Intelligence for the Chief Executive and the Intelligence Commanders Course. In addition, the FLETC offers chief executive training, and an intelligence course at the FBI National Academy is designed for SLTLE managers.
SPECIALIZED TRAINING	This training focuses on a narrow aspect of the entire intelligence process. Courses that fall into this category are generally software courses, such as classes on how to use a particular type of intelligence software (typically, either analytic software or databases).

For example, an intelligence analyst working on cases of terrorism by Islamic extremists needs to substantively understand the distinctions between Shiite and Sunni Muslims, the role of sectarian extremism (notably as related to Palestine), the different Islamic terrorist groups (e.g., al-Qaida, ISIS, HAMAS, Hezbollah) and their methods, the culture of Muslim nations, different leaders, methods of funding, and so forth. This type of substantive knowledge is essential for an analyst to be effective.

Training programs currently available contain some aspect of the protocols and methodology of the intelligence process, although most programs for nonanalysts provide an overview of these issues rather than detailed instruction. Fewer programs contained integrated subject-matter information for intelligence as part of the training. For those that did provide this information, it was typically because the agency sponsoring the training had a specific

1023 [https://www.ialeia.org/foundations\\_of\\_intelligence\\_an.php](https://www.ialeia.org/foundations_of_intelligence_an.php)

1024 The NW3C also offers intelligence training at <https://www.nw3c.org/find-class>.

jurisdictional responsibility (e.g., the Regional Counterdrug Training Academy's<sup>1025</sup> "Operational Intelligence" course integrates "intelligence concepts" with more-specific "drug intelligence indicators").

Training programs continue to emerge on intelligence-related topics, most notably funded by BJA and DHS/FEMA.<sup>1026</sup> Perhaps the best single source to monitor training programs of all types is the National Criminal Intelligence Resource Center.<sup>1027</sup>

## FEDERAL LAW ENFORCEMENT TRAINING CENTERS (FLETC)

Serving 72 federal law enforcement agencies, as well as SLTLE agencies, FLETC has a massive training responsibility. It offers an "Investigative Analysis for Law Enforcement"<sup>1028</sup> course and a wide range of related subject-matter courses, such as on Internet investigations, digital evidence, money laundering, electronic surveillance, and economic crime, among others. FLETC courses change quite frequently, so monitoring the center's website and online course catalog is recommended.<sup>1029</sup>

## DHS-APPROVED INTELLIGENCE TRAINING

DHS has offered or reviewed other agency intelligence courses for compliance with the *Common Competencies for State, Local, and Tribal Intelligence Analysts*<sup>1030</sup> and approved by FEMA for inclusion in the FEMA National Preparedness Directorate (NPD), the National Training and Education Division (NTED) Course Catalog,<sup>1031</sup> and the FEMA NPD, NTED State and Federal Sponsored Course Catalog.<sup>1032</sup> The intelligence courses include the following:

- ◆ DHS Basic Intelligence and Threat Analysis Course (BITAC)
- ◆ DHS Critical Thinking and Analytic Methods (CTAM)
- ◆ DHS Introduction to Risk Analysis Course
- ◆ DHS Intermediate Risk Analysis Course
- ◆ DHS Principles of Intelligence Writing and Briefing (PIWB)
- ◆ Foundations in Intelligence Analysis Training (FIAT)
- ◆ Fundamentals of Suspicious Activity Reporting Analysis
- ◆ Intelligence Analyst Professional Development Program (IAPDP)
- ◆ Intermediate Fusion Center Analyst Training: Analysis and Terrorism Prevention
- ◆ Intermediate Fusion Center Analyst Training: Strategic Analysis and Oral Briefings
- ◆ Law Enforcement Analyst Program
- ◆ Office of the Director of National Intelligence (ODNI) Analysis 101
- ◆ Suspicious Activity Reporting: The Analytic Role
- ◆ Terrorism Intelligence Analysis

---

1025 <https://www.rcta.org/rctasite/>

1026 As an example, see <https://www.dhs.gov/fema-approved-intelligence-analyst-training-courses>.

1027 <https://www.ncirc.gov/Training.aspx>

1028 <https://www.fletc.gov/investigative-analysis-law-enforcement/investigative-analysis-law-enforcement>

1029 <https://www.fletc.gov/>

1030 [https://www.ncirc.gov/documents/public/common\\_competencies\\_state\\_local\\_and\\_Tribal\\_intelligence\\_analysts.pdf](https://www.ncirc.gov/documents/public/common_competencies_state_local_and_Tribal_intelligence_analysts.pdf)

1031 <https://www.firstrespondertraining.gov/frts/npcatalog>

1032 [https://www.firstrespondertraining.gov/frtserver/catalogs/SF\\_course\\_catalog.pdf?\\_=1581704745854](https://www.firstrespondertraining.gov/frtserver/catalogs/SF_course_catalog.pdf?_=1581704745854)

In addition, DHS is developing a new initiative called the Intelligence Training Optimization Division (ITOD). While the program is in its infancy at this writing, DHS provided a briefing to the CICC stating that the initiative would emphasize career planning, training, curriculum development, and programs of study to aid not only in development of intelligence expertise but also for career development. While it appears that ITOD will be initially directed to DHS I&A personnel, there are also plans to extend the resources of the program to SLTLE.

## INTELLIGENCE COURSES IN HIGHER EDUCATION

In recent years, there has been increasing recognition in the academic community of the need for coursework in intelligence that incorporates broad multidisciplinary issues, research, and a philosophical approach to intelligence issues. An increasing number of colleges and universities are offering courses and degrees in intelligence studies. Indeed, growth has been so significant that a new organization was formed to represent them: the International Association for Intelligence Education.<sup>1033</sup> Most programs focus on the national security Intelligence Community.

Acknowledging the author's prerogative, there is one higher-education program that focuses exclusively on law enforcement intelligence. The nation's oldest criminal justice degree program at Michigan State University (MSU) has offered a cross-listed undergraduate/graduate course titled "Law Enforcement Intelligence Operations" for approximately 20 years. As a result of a partnership created with the Drug Enforcement Administration, MSU developed a master's degree program in law enforcement intelligence and analysis.<sup>1034</sup> The program, offered completely online, is taught by regular MSU criminal justice faculty members and is designed as a terminal degree, much like a master's degree in business administration. In addition, Michigan State offers a certificate program in different aspects of intelligence, many of which are available for academic credit. Clearly, the demand for academic preparation for an intelligence career is a growing market.

## CONCLUSIONS

This chapter provided an overview of selected issues in the management of the law enforcement intelligence function. As a rule, the application of management principles may be applied generally regardless of the unit or assignment within a law enforcement agency. The intelligence unit checklist and the ConOps discussion were particularly directed to assist SLTLE agencies to develop (or reengineer) their intelligence capacity to meet current national standards.

Criminal investigation commanders need to understand caseload differentials for crimes; patrol commanders must know minimum staffing requirements to handle calls for service; and traffic commanders must understand traffic analysis and its application to selective enforcement. It is no different with the intelligence commander. This chapter identified critical substantive elements of the intelligence function that will aid law enforcement managers to manage this activity more effectively.

---

1033 <https://www.iafie.org/>

1034 <https://online.cj.msu.edu/masters-law-enforcement-intelligence-analysis>

# CHAPTER ANNEX 14-1: TEN SIMPLE STEPS TO ADOPT THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN

(CRIMINAL INTELLIGENCE COORDINATING COUNCIL)

## TEN SIMPLE STEPS TO ADOPT THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN<sup>1035</sup>

### 1. Recognize your responsibilities and lead by example.

Recognize the value of sharing intelligence information within your own agency, and encourage the practice of sharing information with other law enforcement and public safety agencies. Use the guidelines and action steps outlined in the *National Criminal Intelligence Sharing Plan* (“Plan”) to implement or enhance your organization’s intelligence function.

### 2. Establish a mission statement and a policy to address developing and sharing information and intelligence data within your agency.

The Plan provides model policies and guidelines for implementing or reviewing an agency’s intelligence function. Examples include Criminal Intelligence Systems Operating Policies federal regulation 28 CFR Part 23, the IACP’s *Model Policy on Criminal Intelligence*, and the LEIU’s *Criminal Intelligence File Guidelines*.

### 3. Connect to your state criminal justice network and regional intelligence databases, and participate in information sharing initiatives.

Many states provide access to other government databases, including motor vehicles, corrections, and others. Regional intelligence databases and sharing initiatives promote communication and collaboration by providing access to other agencies’ and organizations’ investigative and intelligence data.

### 4. Ensure privacy issues are protected in policy and practice.

The protection of individuals’ privacy and constitutional rights is an obligation of government officials and is crucial to the long-term success of criminal intelligence sharing. The Plan provides guidelines that support policies that will protect privacy and constitutional rights while not hindering the intelligence process. Implementing and supporting privacy policies and practices within your agency will also reduce your organization’s liability concerns.

### 5. Access law enforcement websites, subscribe to law enforcement listservs, and use the Internet as an information resource.

Many websites on the Internet and others on closed networks provide valuable intelligence assessments and news. Listservs provide instant and widespread communication for investigators. Listservs allow both the receipt and distribution of intelligence information. The Internet provides a wealth of open source information, including government information and access to private agencies that share with law enforcement.

### 6. Provide your agency members with appropriate training on the criminal intelligence process

Some training models or modules are already found online, such as the IALEIA, the NW3C, and LEIU “Turn Key Intelligence.” A listing of available intelligence training sources and specifically scheduled classes is found on the IALEIA website: [www.ialeia.org](http://www.ialeia.org). This listing allows individuals to directly contact training source agencies and organizations for more information on classes and schedules.

1035 Bureau of Justice Assistance. (June 2005). *Ten Simple Steps to Adopt the National Criminal Intelligence Sharing Plan*. Washington, DC: BJA brochure.

**7. Become a member of your in-region Regional Information Sharing Systems (RISS) Center.**

RISS operates a secure Web-based nationwide network for communication and exchange of criminal intelligence information by local, state, federal, and tribal participating law enforcement member agencies. RISS partners with other law enforcement systems to electronically connect them to RISSNET, including High Intensity Drug Trafficking Areas (HIDTA) Investigative Support centers and other federal and state agency systems.

**8. Become a member of the FBI's Law Enforcement Online (LEO) system.**

The FBI's LEO system is a sensitive but unclassified, real-time information sharing communications system for all levels of the law enforcement community and available at no cost to its approximately 40,000 users. LEO provides secure email capability, a national alert mechanism, and access to over 125 special-interest groups for sharing information by providing access to other networks, systems, databases, and other services.

**9. Partner with public and private infrastructure sectors.**

Regular communication with the entities that control America's critical infrastructures such as energy, agriculture, transportation, and shipping is critically important to ensuring the safety and security of the citizens in your community.

**10. Participate in local, state, and national intelligence organizations.**

In most areas of the country, there are locally based intelligence organizations that welcome participation from all agencies and are often affiliated with state and national organizations.

# CHAPTER ANNEX 14-2: WHY LAW ENFORCEMENT AGENCIES NEED AN ANALYTIC FUNCTION

## (BUREAU OF JUSTICE ASSISTANCE)

### WHY LAW ENFORCEMENT AGENCIES NEED AN ANALYTICAL FUNCTION<sup>1036</sup>

#### 1. Helps solve criminal investigations.

The analytical function develops a variety of intelligence products to assist investigators in detecting, preventing, and responding to criminal and terrorism activities. Analytical personnel initiate inquiries, conduct information searches, and act as a central point for information gathered.

#### 2. Increases the ability to prosecute criminals.

Personnel assigned to the analytical function develop summary tables, charts, maps, and other graphics for use in a grand jury or trial. Analysts provide factual and expert testimony and organize evidence for presentation in court.

#### 3. Supports the chief executive and the agency's mission.

By maximizing the analytical function, the chief executive can obtain important information and intelligence to possibly prevent future criminal activities. Personnel can prepare materials to assist in allocating resources; developing budget and resource requests; and preparing departmental reports, investigative briefings, and press releases.

#### 4. Proactively informs law enforcement officers of crime trends and develops threat, vulnerability, and risk assessments.

The analytical function provides support to tactical and strategic operations. Personnel analyze crime reports, identify crime hot spots, develop crime bulletins and summaries, study serial crime data, and forecast future crime. The analytical function develops proactive intelligence products that assess the potential threats of crime groups or criminal activities and recommends methods to intervene in these threats.

#### 5. Trains law enforcement and other intelligence personnel.

Staff members develop course modules on intelligence and analytic methods and provide awareness and methodology training to agency members, executives, and managers.

#### 6. Assists in the development of computerized databases to organize information and intelligence.

Personnel within the analytical function help in the development and maintenance of systems that collect, collate, retrieve, and disseminate information. Analytical staff members participate in departmental testing and acquisition of investigative, intelligence, and analytical software.

#### 7. Fosters meaningful relationships with other law enforcement personnel.

Analytical staff members interact with other law enforcement agencies and build relationships with peers, allowing them to quickly obtain information and efficiently assist in multijurisdictional or complex cases. Through contact with national programs and professional associations, personnel are able to ascertain national issues that may affect local agencies.

---

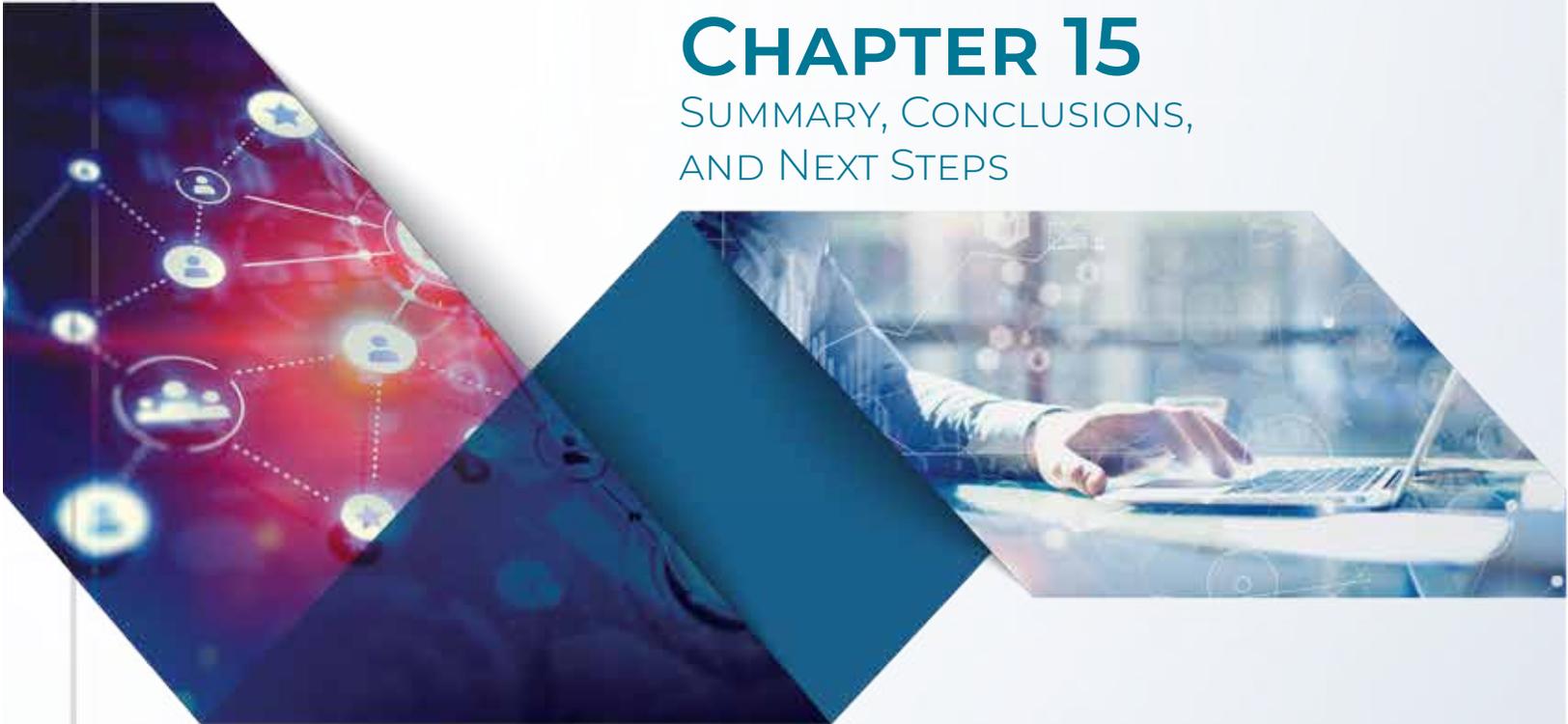
1036 Bureau of Justice Assistance. (October 2005). *Why Law Enforcement Agencies Need an Analytical Function*. Washington, DC: BJA brochure.

**8. Ensures compliance with local, state, tribal, and federal laws and regulations.**

Analytical personnel provide expertise and knowledge in the development of protocols to ensure compliance with local, state, tribal, and federal laws and rules that govern intelligence sharing, privacy, and civil liberties.

**9. Provides support to fusion centers.**

Personnel provide support to local, state, or regional fusion centers by performing intelligence services such as crime-pattern, association, telephone-toll, and financial analysis. They create intelligence reports, briefs, threat assessments, and other intelligence products to aid in the prevention and deterrence of crime, including terrorism.



# CHAPTER 15

## SUMMARY, CONCLUSIONS, AND NEXT STEPS

Effective law enforcement intelligence operations are sometimes confusing to understand, frequently controversial, and often challenging to implement. Yet the intelligence process has demonstrated that it is an effective tool for community safety.

**Intelligence is confusing** because many people do not make the distinction between law enforcement intelligence and national security intelligence. Moreover, the term is used generically to describe a wide body of activities. Added to this is the development of the Information Sharing Environment, which is not only changing our information sharing relationships but making the demarcation between law enforcement and national security somewhat more difficult to discern on matters of terrorism. One purpose of this guide is to provide consistent and clear definitions and processes accepted by law enforcement intelligence professionals that reflect national standards and initiatives in intelligence to help reduce the confusion.

**Law enforcement intelligence operations are controversial**, both because of the checkered history of intelligence activities and the concern of many today that in the zeal to prevent criminal extremism and targeted violence, citizens' civil rights will be abridged. There is no doubt that law enforcement suffered setbacks as a result of lawsuits against criminal intelligence practices of the 1960s and 1970s. However, with those setbacks, important lessons were learned that not only set the stage for 28 CFR Part 23 but helped lay the foundation for the law enforcement intelligence profession. Further controversies face law enforcement, as concerned citizens and civil rights groups, who often do not fully understand the intelligence function, fear that law enforcement agencies will gather and keep information about citizens who have not committed crimes but are exercising their constitutional rights on

controversial issues. New and emerging surveillance technologies only serve to heighten these concerns. The lessons law enforcement has learned from public education and community policing initiatives can help eliminate these fears—not only through the practice of ethical policing but also by reaching out to diverse communities to explain police practices, respond to questions, and establish open, trusted lines of communication.

**Intelligence operations are difficult as well.** Changes in processes and in interagency relationships are required to establish links with different law enforcement organizations and groups to maximize effective information sharing. A reallocation of resources is also required to make the intelligence function perform effectively and to meet operational and training standards set out in the *National Criminal Intelligence Sharing Plan* and the *Minimum Criminal Intelligence Training Standards*. A change in culture is required for intelligence-led policing to become a reality, and a realignment of priorities may be needed to accomplish new goals. There is always resistance to change, and legitimate competing interests always must be weighed.

**Finally, law enforcement intelligence processes can be effective.** Intelligence can help identify threats to a community whether from terrorists, organized crime, or even noncriminal hazards. It takes diverse and often disparate information, integrated into a cohesive package, to provide insight that might otherwise be lost. Increasingly, law enforcement intelligence is more thorough, of higher quality, and disseminated more effectively as a result of cooperative initiatives by the Criminal Intelligence Coordinating Council and its work with the partner engagement initiatives of the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI). Similarly, there is a greater emphasis on law enforcement intelligence, punctuated by the evolution of fusion centers, and creative work by the National Fusion Center Association,<sup>1037</sup> the Association of Law Enforcement Intelligence Units,<sup>1038</sup> and the International Association of Law Enforcement Intelligence Analysts.<sup>1039</sup> All three of these organizations are instrumental in the ongoing professional development of law enforcement intelligence. Through their annual meetings and training sessions, they explore new applications of intelligence as related to emerging crime trends and the applications of new technologies. The end result of all of these initiatives is to make our communities safer; hence this investment pays important dividends for protecting America’s people.

## CHALLENGES FOR THE FUTURE

The most effective method of examining challenges for the future is a strategic approach that takes a macro view of critical trends and determines their impact on the law enforcement environment. An interesting—and relevant—study comes from the Intelligence Community, as a project from ODNI, which seeks to identify trends that threaten U.S. sovereign principles. Although written over a decade ago, the observations resonate as accurately today. The report observed that:

[m]any drivers and trends are shaping the future global environment in which the Intelligence Community must operate—demographic and social change, increased economic integration and competition, rapid technological innovation and diffusion, environmental pressures and growing energy demand, broad geopolitical changes and new forms of governance. Each driver and trend independently produces unique changes and challenges; those points where factors intersect often reinforce and amplify the effects of change and create a series of complex and often unpredictable threats and risks that *transcend geographic borders and organizational boundaries*.<sup>1040</sup> (Emphasis in original.)

---

1037 <https://nfcausa.org/>

1038 <http://www.leiu.org/>

1039 <https://ialeia.org/>

1040 McConnell, J. M. (2008). *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*. Washington, DC: Office of the Director of National Intelligence, p. 4.

These same trends that have potential effects on national security can also have effects in our local communities. At the least, these trends have an impact on public order and most likely influence crime trends that are diverse and transjurisdictional in nature. For example, the number of terrorist attacks by far-right perpetrators quadrupled in the United States between 2016 and 2017 and rose by 43 percent in Europe over the same period.<sup>1041</sup> Whereas right-wing extremism used to be viewed as a domestic problem, it is now a global threat, with European movements having an effect on domestic right-wing extremism.

The ODNI report goes on to observe that:

To these persistent threats we add a growing array of emerging missions that expands the list of national security (and hence, intelligence) concerns to include infectious diseases, science and technology surprises, financial contagions, economic competition, environmental issues, energy interdependence and security, cyberattacks, threats to global commerce, and transnational crime. Foremost among these challenges is the *blurring* of lines that once separated *foreign and domestic intelligence* and the increased importance of homeland security. By necessity, we must be involved with numerous new partners in interactive relationships, but we must also *respect and maintain the privacy and civil liberties of all Americans*.<sup>1042</sup> (Emphasis in original.)

The novel coronavirus pandemic of 2020 illustrates these points. A public health risk resulted in gubernatorial executive orders across the United States for required social distancing, stay-at-home orders, and prohibitions of gatherings of more than ten people. Law enforcement was then challenged with how to enforce these orders—with varying degrees of success. Thus, like the Intelligence Community, law enforcement intelligence will have increasing responsibility to manage criminal and all-hazards types of threats while working in a broadened environment of information sharing. The challenges are not only to learn to deal with these new threats—and new disciplines—but to do so while ensuring the constitutional guarantees of all people.

These are sobering challenges that the country must confront. The safety of American society cannot wait to react; rather, law enforcement must be proactive. This, of course, is difficult to do. The challenges of handling current problems on a much broader scale than ever while experiencing proportionately smaller budgets require creativity and new ways of solving problems.

## CHALLENGES TO ADDRESS

There are always going to be challenges that arise quickly—law enforcement must ensure that it has the analytic capability to understand these challenges and the executive capability to respond in an effective manner. Some lessons learned from the past provide insight for law enforcement to look ahead.

- ◆ Develop creative real-time analysis, not only to identify threats that may emerge but also to determine early indicators of crime trends. For example, not only should law enforcement have forecast the opioid crisis; it also should have anticipated the reaction of drug traffickers to increase purity levels and lower costs of other drugs—such as methamphetamine, cocaine, and heroin—to take back their market share lost by opioids. Instead, law enforcement was slow to embrace the magnitude of the opioid threat. Once anti-opioid programming started, law enforcement and public health focused on opioids, almost to the exclusion of other drugs, because of the crisis. Abuse of methamphetamine, heroin, and cocaine then increased and once again, government programming had to catch up.
- ◆ Law enforcement organizations, and, by extension, intelligence units and fusion centers, need to become nimble—not only being able to identify threats and trends but aiding in the development of creative and effective operational responses. Being able to have quick organizational responses will enhance effectiveness.

1041 Jones, S. G. (2018). The Rise of Far-Right Extremism in the United States. *CSIS Research Brief*, November, 1–9.

1042 McConnell, op cit.

- ◆ Intelligence leaders must remember that threats rarely disappear. They may diminish for a certain period, but they often resurface. For example, despite the amount of time that has passed since the September 11, 2001 (9/11), attacks, al-Qaeda (as well as ISIS) continues to view the United States as an enemy and seeks to harm this country and U.S. interests. They have patience and must be viewed as a continuing threat, not a past threat. We must constantly multitask, recognizing that a responsibility of the intelligence process is to continue monitoring these threats, ever aware that they not only exist but can also morph. Similarly, in the 1980s and 1990s, there were several attacks and a pervasive presence of white supremacists. That presence diminished, reappearing with violence in 2017 and ensuing years. The threat did not disappear.
- ◆ While progress has been made, law enforcement intelligence needs to more fully embrace critical thinking and be more scientific in how problems are analyzed and solutions are developed when assessing future threats. Similarly, if law enforcement leaders more proactively embrace intelligence analysis, particularly strategic intelligence, they will increase the probability of being prepared as the threat environment changes.
- ◆ Law enforcement needs to continue to embrace emerging technologies and their applications, both as a tool for law enforcement and as an instrumentality of complex criminality. Technology evolves so quickly that it is easy for law enforcement to fall behind the curve, while it seems that criminal offenders learn how to quickly use and exploit technology in their enterprises.

While law enforcement and the Intelligence Community have made significant, and necessary, investments in technology, success in the production and application of intelligence relies on people. Law enforcement needs to recognize that the creativity to solve the complex problems of the future will require the best and brightest to work in government service. Effective and creative analysis of problems can help lead to interventions and solutions. Not only must law enforcement leaders explore the problems of the future, but it must also examine the law enforcement culture of today. Analysts must be compensated and treated as equal professionals in law enforcement organizations. Law enforcement leaders must understand that their use of intelligence and analysis is as important to their success as are their efforts in enforcement. The changes that are required to prepare our organizations must begin now, because the process can be long and challenging. One approach is to use a model the author refers to as R-cubed.

## IMPLEMENTING CHANGE: THE R-CUBED APPROACH<sup>1043</sup>

Implementing new intelligence initiatives can be difficult. As a road map to accomplish this, the author recommends a process referred to as “R-cubed”: reassessing, refocusing, and reallocating (R<sup>3</sup>).

The intent of the R<sup>3</sup> exercise is to provide a framework for organizational change as related to intelligence responsibilities. It requires a critical self-assessment of responsibilities and resources; objectivity absent special interests; realistic perspectives; both tactical and strategic considerations of traditional and new policing responsibilities; and methods (including financing) for accomplishing all police responsibilities. This is a labor-intensive, difficult process that cannot be rushed and should be inclusive. That is, consideration of the inputs of others—employees, community members, elected officials, and other agencies—should be included in the process. Final decisions, however, remain with law enforcement executives to make changes as best determined by their collective judgment of responsibilities, priorities, and available resources. A number of factors may be included in each component of the R<sup>3</sup> exercise.

### REASSESSING

Examine both current and new priorities for intelligence and community safety to determine which activities need to be continued to maintain security in the community and fulfill the law enforcement mission related to crime control,

---

1043 Carter, D. L. (2004). *The Police and the Community*. 8th ed. Upper Saddle River, NJ: Prentice-Hall.

order maintenance, and counterextremism. This assessment should include consideration of a number of variables, such as the following:

- ◆ The number of calls for service received by a law enforcement agency and the ability to handle those calls for service.
- ◆ Specialization that currently exists in the law enforcement agency (e.g., gangs, narcotics, school programs, initiatives directed toward senior citizens, traffic) and the true demand or need for that specialization.
  - Objectivity is critical because special interests can skew priorities.
- ◆ Specialization that needs to be developed (e.g., intelligence capacity; first-responder capabilities [including weapons of mass destruction]; computer crime/cyberterrorism prevention and investigative expertise; investigative capacity for terrorism; obligation to assign personnel to a Joint Terrorism Task Force; and expertise in all-hazards threats that can affect public safety and public order).
- ◆ Resources that can be used to help with police responsibilities of all forms (e.g., police reserves, volunteers, expertise in other agencies, community organizations).
- ◆ Objective assessment of threats and potential targets within the community and within the region (the latter includes how multijurisdictional crime and terrorist threats would affect an agency directly and indirectly, including mutual aid obligations).
- ◆ Current intelligence expertise and practices, including information sharing, and the need to modify these practices, including adding a private sector component for critical infrastructure.
- ◆ Political mandates from elected officials and/or the community that should not be ignored because expectations and concerns of these groups must be taken into account in any assessment process.

Reassessing the intelligence process is particularly important as communities call for police reform in furtherance of social justice issues. This is particularly true for technological information collection, surveillance, and analytic forecasting of criminal behavior.

## REFOCUSING

Guided by the results of the reassessment, an agency must develop a plan for change that incorporates its new priorities, as appropriate. Virtually all of the department's current tasks will continue in some form, but the amount of emphasis and the proportion of resources devoted to those tasks will differ, notably in light of added homeland security responsibilities.

Refocusing first requires the department to establish its new priorities by reassessing and evaluating its responsibilities. From there, it can refocus on its priorities, if needed. While *reassessment* involves information gathering and analysis, *refocusing* is the development and implementation of policy steps to make the changes operational.

Second, each area of responsibility must be weighted (i.e., weight constitutes the amount of emphasis given to each broad area of tasks and determines which area receives the greatest amount of attention). The author does not suggest that intelligence should be the top priority; indeed, in most police agencies, managing calls for service will remain the top priority. Instead, this is a realistic expectation that priorities will change with emphasis on some new programming and that all responsibilities will be affected to some degree. Therefore, to determine this realignment, responsibilities and weights must be stipulated.

Third, these changes are implemented through the issuance of updated (and new, when applicable) policies, procedures, and orders. Implementation also requires communication and, in some cases, in-service training to explain and clarify the changes.

## REALLOCATING

Once refocusing decisions have been made, the department must reallocate its resources to meet adjusted priorities. This includes personnel, operating expenses, equipment (from cars to radios to computers), and office space, as needed. There is always the possibility that the department will receive an increased appropriation in its budget, but it should not be counted on. If so, most likely it will be only a proportion of actual resource needs. The difficult process of reallocation is a necessity that will produce some alienation and, in all likelihood, political rifts within the organization. Reallocation, therefore, also requires effective leadership to guide the organization and motivate personnel to understand the necessity of the changes and the concomitant benefits to the community.

There is no explicit recipe for change in an organization. This is particularly true with intelligence, where a renewed emphasis is given to a process that is largely not understood by most personnel. There is little guidance, and, despite the best plans, time will be needed for experimentation. Agencies should take the time to carefully consider all new responsibilities, balance them with legitimate competing demands within the agency, and then make a clear step toward adjusting the organization.

## CONCLUSIONS

As demonstrated throughout this guide, America's law enforcement agencies continue to face challenges. Throughout the history of policing, challenges have been faced; they have been met with resolute determination; and America has been safer as a result. New challenges, whatever they may be, are no different. The intent of this guide has been to help America's state, local, and tribal law enforcement agencies make this journey, keeping these core "intelligence lessons learned" in mind:

1. Intelligence analysis, smart policing, and crime analysis are important interdependent tools for efficient, effective counterterrorism and crime suppression.
2. Intelligence is the product of the analysis of raw information for the purpose of identifying criminal threats or changes in the criminal threat picture.
3. Intelligence requires a different thought process from the one that officers typically learn in their law enforcement careers.
4. The current intelligence model has diverse priorities, all of which have some overlap.
5. Law enforcement intelligence has an important role in the suppression of violent crime.
6. National professional standards for the intelligence process and for protecting personally identifiable information need to be adopted and followed.
7. In the intelligence process, the application of First Amendment protections for expressive activity and Fourth Amendment privacy protections must be mastered.
8. Information collection for the intelligence process must have a directed focus to learn about threats, not a general exploration or a dragnet.
9. Intelligence-led policing will be most successful if it is built on a community policing foundation and proven data analysis (e.g., CompStat).
10. Implementation of intelligence-led policing and the intelligence process requires patience, diligence, policy change, training, the control of dogmatism, and the willingness to look forward to new issues, resources, and challenges.
11. For a law enforcement agency to implement a successful criminal intelligence program, the program must have support, understanding, and direction from the leadership of the agency.

## BIBLIOGRAPHY

- Adams, Jean, et al. (2016). "Searching and Synthesizing 'Grey Literature' and 'Grey Information' in Public Health." *Systematic Reviews*. Volume 5, Article 164.
- Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (2002). *Implementing the National Strategy*. Washington, DC: The Rand Corporation.
- Allen, C. E. (April 2, 2008). Testimony of the Under Secretary for Homeland Security before the Senate Committee on Homeland Security and Governmental Affairs.
- Allen, C. E. (July 23, 2008). *Information Sharing at the Federal, State and Local Levels*. Statement for the Record before the United States Senate Committee on Homeland Security and Governmental Affairs.
- Allen, C. E. (May 6, 2008). DHS Under Secretary for Intelligence and Analysis. Address to the Washington Institute for Near East Policy. Washington, DC.
- American Friends Service Committee. (1979). *The Police Threat to Political Liberty*. Philadelphia, PA: American Friends Service Committee.
- Analyst Professional Development Road Map, Version 2.0*. (2019). Washington, DC: Criminal Intelligence Coordinating Council, Global Justice Information Sharing Initiative. Attorney General's Report to Congress on the Growth of Violent Street Gangs in Suburban Areas. (2008). Washington, DC: U.S. Department of Justice, p. 14.
- Background on the Controlled Unclassified Information Framework*. (May 9, 2008). (Unpublished background paper.) Washington, DC: Executive Office of the President, pp. 4–7.
- Best, R., and Cumming, A. (2007). *Open Source Intelligence (OSINT): Issues for Congress*. Washington, DC: Congressional Research Service.
- Best, R., and Boerstling, H. A. (1996). *The Intelligence Community in the 21st Century*. House of Representatives 104 Congress, Permanent Select Committee on Intelligence.
- Beutel, A., and Weinberger, P. (2016). "Public-Private Partnerships to Counter Violent Extremism: Field Principles for Action." *Final Report to the U.S. Department of State*. College Park, MD.
- Bhanu, C., and Stone, C. (2004). *Public-Private Partnerships for Police Reform*. New York, NY: Vera Institute of Justice.
- Blackstock, N. (1975). *COINTELPRO: The FBI's Secret War on Political Freedom*. New York, NY: Vintage.
- Boba, R. (2003). *Problem Analysis in Policing*. Washington, DC: Police Foundation.
- Boba, R. (2005). *Crime Analysis and Crime Mapping*. Thousand Oaks, CA: Sage. Publications.
- Brannon, V. C. (2019). *Free Speech and the Regulation of Social Media Content*. Congressional Research Service, R45650.
- Brantingham, P. J., M. Valasik, and Mohler, G. O. (2018). "Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Control Trial." *Journal of Statistics and Public Policy*. Vol. 5, No. 1, pp. 1–6.
- Bullock, K. (2013). Community, intelligence-led policing and crime control. *Policing and Society*, 23:125–144.
- Bureau of Justice Assistance, Criminal Intelligence Training Coordination Strategy Working Group. (2004). *Survey of Law Enforcement on Intelligence Training*. Unpublished staff report.
- Bureau of Justice Assistance. (2005). *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: Office of Justice Programs, U.S. Department of Justice.
- California Peace Officers' Association. (1998). *Criminal Intelligence Program for the Smaller Agency*. Sacramento, CA: California Peace Officers' Association.
- Calling Time on Crime*. (2004). London, UK: Her Majesty's Inspectorate of Constabulary.
- Carr, T. (2017) "Event Deconfliction Avoids Operational Conflicts, Saves Lives, and Solves Cases." *The Police Chief*. (February).
- Carter, D. L. (2000). *The Police and the Community*. 7th ed. Englewood Cliffs, NJ: Prentice-Hall, Inc.
- Carter, D. L. (2002). *Law Enforcement Intelligence Operations*. 8th ed. Tallahassee, FL: SMC Sciences, Inc.
- Carter, D. L. (2004). *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*. Washington, DC: Office of Community

- Oriented Policing Services, U.S. Department of Justice.
- Carter, D. L. (2004). *The Police and the Community*. 8th ed. Upper Saddle River, NJ: Prentice-Hall.
- Carter, D. L. (2013). *Homicide Process Mapping: Best Practices for Increasing Homicide Clearances*. Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance.
- Carter, D. L., and Carter, J. G. (2015) "Effective Police Homicide Investigations: Evidence from Seven Cities with High Clearance Rates." *Homicide Studies*. 20(2).
- Carter, D. L., and Martinelli, T. (2007). "Civil Rights and Law Enforcement Intelligence." *The Police Chief*. (June).
- Carter, D. L., et al. (2011). *Understanding the Intelligence Practices of State, Local and Tribal Law Enforcement Agencies*. A grant report to the National Institute of Justice.
- Carter, J. (2015). "Inter-organizational Relationships and Law Enforcement Information Sharing Post September 11, 2001." *Journal of Crime and Justice*, 38, 522–542.
- Carter, J. G. (2013). *Intelligence-Led Policing: A Policing Innovation*. El Paso, TX: LFB Scholarly.
- Carter, J. G. (2015). "Intelligence Analysis within U.S. Law Enforcement Agencies: Empirical Insights from a National Sample." *Journal of Intelligence Analysis*, 22:1–24.
- Carter, J. G. (2018). *Bibliography of Intelligence-Led Policing*, Oxford, UK: Oxford Bibliographies.
- Chermak, S., Carter, J., Carter, D., McGarrell, E., and Drew, J. (2013). "Law Enforcement's Information Sharing Infrastructure: A National Assessment." *Police Quarterly*, 16(2), 211–244.
- Chevigny, P. G. (1984). "National Security and Civil Liberties: Politics and Law in the Control of Local Surveillance." *Cornell Law Review*. 69(April), p. 735.
- Christopher, S. (2004). "A Practitioner's Perspective of UK Strategic Intelligence." In J. H. Ratcliffe (ed.). *Strategic Thinking in Criminal Intelligence*. Sydney: Federation Press.
- Clarke, R. V., and Eck, J. (2005). *Crime Analysis for Problem Solvers in 60 Small Steps*. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.
- Coffey, A. F. (2015). *Measuring Effectiveness in the Domestic Intelligence Community: Taking a Configurational Approach to Explain Organizational Outcomes in the National Network of Fusion Centers*. A dissertation submitted to the Virginia Polytechnic Institute and State University.
- Collier, P. M., Edwards, J. S., and Shaw, D. (2004). "Communicating Knowledge about Police Performance." *International Journal of Productivity and Performance Management*. 53(5), 458–467.
- Commission on Accreditation of Law Enforcement Agencies. (2002). *Standards for Law Enforcement Accreditation*. "Standard 51.1.1 – Criminal Intelligence." Washington, DC: CALEA.
- Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. Washington, DC: U.S. Government Printing Office.
- Cope, N. (2004). "Intelligence-Led Policing or Policing-Led Intelligence? Integrating Volume Crime Analysis Into Policing." *British Journal of Criminology*, 44:188–203.
- Counterterrorism Division. (2006). *Terrorism: 2002–2005*. Washington, DC: Federal Bureau of Investigation.
- Covert, J. M. (2012). *Evolving the Local Fire Service Intelligence Enterprise in New York State: Implementing a Threat Liaison Officer Program*. Monterey, CA: Naval Postgraduate School.
- Cowan, P., Egleson, N., and Hentoff, N. (1974). *State Secrets: Police Surveillance in America*.
- Creswell, J. W., and J. D. Creswell (2019). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 4th ed. Thousand Oaks, CA: Sage Publications.
- Criminal Intelligence Coordinating Council. (2019). *Fusion Center Privacy, Civil Rights, and Civil Liberties Development Guide, Version 3.0*. Washington, DC: Global Justice Information Sharing Initiative.
- Dark Web Monitoring Challenges*. (2020). Cobweb Technologies white paper.
- Decker, S. H., and Pyrooz, D., (2013). "Gangs: A New Form of Organized Crime?" *Oxford Handbooks Online*. DOI:10.1093/oxfordhb/9780199730445.013.008.
- Department of Homeland Security. (May 11, 2004). Management Directive System, MD Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.

- DHS Lexicon Terms and Definitions. (2017). Washington, DC: Management Directorate, Department of Homeland Security.
- Dillon, D. R. (2002). "Breaking Down Intelligence Barriers for Homeland Security." *Backgrounder #1536*. Washington, DC: Heritage Foundation.
- Dintino, J., and Martens, F. (1983). *Police Intelligence in Crime Control*. Springfield, IL: Charles C. Thomas.
- Dobrin, A. (2017). Volunteer Police: History, Benefits, Costs and Current Descriptions." *Security Journal*. Vol 30, No. 3, pp. 717–733.
- Donner, F. (1992). *Protectors of Privilege*. Berkeley, CA: University of California Press.
- Dutton, G., et al. (2015). *The Impact of Forensic Science Research and Development*. Washington, DC: National Institute of Justice.
- Elliff, J. T. (1971). *Crime, Dissent, and the Attorney General*. Beverly Hills, CA: Sage Publications.
- European Commission. (2003). *Report of the Seminar on Public Private Partnerships*. The Hague, Netherlands.
- Face Recognition Policy Development Template for Use in Criminal Intelligence and Investigative Activities. (2017). Washington, DC: Criminal Intelligence Coordinating Council.
- Federal Bureau of Investigation. (undated). "The FBI's Counterterrorism Program Since September 2001." *A Report to the National Commission on Terrorists Attacks Upon the United States*. Washington, DC: FBI.
- Fein, R., and Vossekuil, B. (1999). "Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approaches." *Journal of Forensic Sciences* 44(2), 321–333.
- Fisher, L. E. (2004). "Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups." *Arizona Law Review*. 46(Winter), p. 621.
- Friedman, R. S., and Peek, F. (2002). "Problem-Based Learning and Problem-Solving Tools: Synthesis and Direction for Distributed Education Environments." *Journal of Interactive Learning Research*. Vol. 13, No. 3, pp. 239–257.
- Frost, C., and Morris, J. (1983). *Police Intelligence Reports*. Orangevale, CA: Palmer Press.
- General Accountability Office. (2007). *TECHNOLOGY: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*. Washington, DC: GAO.
- General Accountability Office. (October 2007). *Homeland Security: Federal Efforts are Helping Alleviate Some Challenges Encountered by State and Local fusion centers*. Washington, DC: General Accountability Office, GAO-08-35 Homeland Security.
- German, M., and Stanley, J. (2007). *What's Wrong with Fusion Centers?* New York, NY: American Civil Liberties Union.
- Global Intelligence Working Group. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: U.S. Department of Justice.
- Global Intelligence Working Group. (2007). *Privacy Committee Report: Tips and Leads Issues Paper*. Washington, DC: Global Justice Information Sharing Initiative, U.S. Department of Justice.
- Global Justice Information Sharing Initiative. (2006). *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Bureau of Justice Assistance.
- Global Justice Information Sharing Initiative. (2006). *Privacy Policy Development Guide*. Washington, DC: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.
- Godfrey, E.D., and Harris, D. R. (1971). *Basic Elements of Intelligence*. Washington, DC: Law Enforcement Assistance Administration.
- Goldstein, H. (1990). *Problem-Oriented Policing*. New York: McGraw-Hill.
- Gruenewald, J., et al. (2019). "Suspicious Preoperational Activities and Law Enforcement Interdiction of Terrorist Plots." *Policing: An International Journal*. Volume 42, Issue 1.
- Heaton, R. (2010). The prospects for intelligence-led policing: Some historical and quantitative considerations. *Policing and Society*, 9:337–355.
- Herzog, T. J. (2007). *Integrating Correctional Authorities in the Fusion Center Rubric*. Palm Coast, FL: Correctional Technology Association.
- Homeland Security Advisory Council. (2005). *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Washington, DC: Department of Homeland Security.

- Information Exchange Package Document (IEPD) for the Suspicious Activity Report of State and Local Entities IEPD. Version 1.01.* A joint document of the Program Manager-Information Sharing Environment and the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.
- Information Sharing Environment Annual Report to Congress.* (2019). Washington, DC: Office of the Director of National Intelligence.
- Information Sharing Environment Functional Standard for Suspicious Activity Reporting, Version 1.5.5.* (2019). Washington, DC: Department of Homeland Security.
- Information Sharing Environment Implementation Plan.* (2006). Washington, DC: Program Manager-Information Sharing Environment.
- Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives.* (April 2007). A report to the Chairman, Committee on Homeland Security, U.S. House of Representatives. Washington, DC: General Accountability Office.
- Institute for Intergovernmental Research. (2015). *After-Action Assessment of the Police Response to the August 2014 Demonstrations in Ferguson, Missouri.* Washington, DC: COPS Office.
- Intelligence Training Coordination Working Group. (2007). *Minimum Criminal Intelligence Training Standards.* Washington, DC: Global Intelligence Working Group.
- International Association of Chiefs of Police. (2002). *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels.* Alexandria, VA: International Association of Chiefs of Police.
- International Association of Law Enforcement Intelligence Analysts. (undated). *Successful Law Enforcement Using Analytic Methods.* Internet-published document.
- Introduction to the National Information Exchange Model.* (February 12, 2007). Washington, DC: NIEM Program Management Office.
- James, A. (2014). *Examining Intelligence-Led Policing: Developments in Research, Policy and Practice.* Basingstoke: Palgrave MacMillan.
- James, N. (2018). *Recent Violent Crime Trends in the United States.* Washington, DC: Congressional Research Service.
- Johnson, B., and Dorn, S. (2008). "Fusion Centers: New York State Intelligence Strategy Unifies Law Enforcement." *The Police Chief.* (February), p. 38.
- Johnson, L. (1985). *A Season of Inquiry: The Senate Intelligence Investigation.* Lexington, KY: The University Press of Kentucky.
- Jones, S. G. (2018). The Rise of Far-Right Extremism in the United States. *CSIS Research Brief,* November, 1–9.
- Joyal, R. (2012). "How Far Have We Come? Information Sharing, Inter-Agency Collaboration, and Trust Within the Law Enforcement Community." *Criminal Justice Studies,* 25(4), 357–370.
- Justice Department's Project to Interview Aliens After September 11, 2001.* (2003). Washington, DC: General Accounting Office. Report Number GAO-03-459.
- Kerry, C. F. (2018). *Why Protecting Privacy is a Losing Game—and How to Change the Game.* Washington, DC: Brookings Institution.
- Kindsvater, L. C. (2003). "The Need to Reorganize the Intelligence Community." *Studies in Intelligence.* Vol. 47, No. 1.
- Knezo, G. J. (2006). *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information.* Washington, DC: Congressional Research Service.
- Knoke, D., and Yang, S. (2020). *Social Network Analysis.* 3rd. ed. Thousand Oaks, CA: Sage Publications.
- Koehnlein, B. (2003). *The History of the Handschu Decree.* New York, NY: New York Civil Liberties Union.
- Ladich, S. (2018.) *Asserting Collective State Sovereignty to Strengthen the National Network of Fusion Centers.* A thesis submitted to the Naval Postgraduate School.
- Laipson, E. (2008). *New Information and Intelligence Needs in the 21st Century Threat Environment.* Washington, DC: The Stimson Center,
- Law Enforcement Analytic Standards.* (2004). Washington, DC: Global Justice Information Sharing Initiative and the International Association of Law Enforcement Intelligence Analysts.

- Law Enforcement Analytic Standards*. 2d ed. (2012). Washington, DC: Global Justice Information Sharing Initiative and the International Association of Law Enforcement Intelligence Analysts.
- Law Enforcement Forecasting Group. (2012). *Increasing Analytic Capacity of State and Local Law Enforcement Agencies: Moving Beyond Data Analysis to Create a Vision for Change*. Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance.
- Law Enforcement Intelligence Unit. (Revised 2002). *Criminal Intelligence File Guidelines*. Sacramento, CA: LEIU.
- Lee, C. "The NYPD Wants to Watch You." *The Village Voice*. Series of articles December 18–24, 2002.
- Leson, J. (2005). *Assessing and Managing the Terrorism Threat*. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice.
- Lewandowski, C., and Carter, J. G. (2017). "End-User Perceptions of Intelligence Dissemination From a State Fusion Center." *Security Journal*, 30(2), 467–486.
- Lilly, J. R. (2003). "National Security at What Price? A Look Into Civil Liberty Concerns in the Information Age Under the USA Patriot Act of 2001 and a Proposed Constitutional Test for Future Legislation." *Cornell Journal of Law and Public Policy*. 12(Spring), p. 447.
- Los Angeles Police Department. (March 5, 2008). *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*. Special Order Number 11.
- Lowe, T., and Innes, M. (2012). "Can We Speak in Confidence? Community Intelligence and Neighborhood Policing v2.0." *Policing and Society*, 22:295–316.
- Loyka, S. A., Faggiani, D. A., and Karchmer, C. (2005). *The Production and Sharing of Intelligence: Vol. 4. Protecting your Community from Terrorism*. Washington, DC: Office of Community Oriented Policing Services and the Police Executive Research Forum.
- MacLellan, T. (2006). *Protecting Privacy in Integrated Justice Systems*. Washington, DC: National Governors' Association Center for Best Practices.
- Maguire, M. (2010). "Policing by Risks and Targets: Some Dimensions and Implications of Intelligence-Led Crime Control." *Policing and Society*, 9:315–336.
- Martens, F. (1987). "The Intelligence Function." In Herbert Edelhertz (ed.). 1987 (September). *Major Issues in Organized Crime Control: Symposium Proceedings*. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.
- Masse, T. (2005). *The National Counterterrorism Center: Implementation Challenges and Issues for Congress*. Washington, DC: Congressional Research Service.
- Masse, T., and Rollins, J. (September 19, 2007). "A Summary of Fusion Centers: Core Issues and Options for Congress." *CRS Report for Congress*. Washington, DC: Congressional Research Service, United States Congress.
- Matthies, C., and Chiu, T. (2014) *Putting a Value on Crime Analysts*. New York: Vera Institute.
- McConnell, J. M. (2008). *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*. Washington, DC: Office of the Director of National Intelligence.
- McCreesh, P., and Neuman, C. (2007). *Managing for Counter-Terrorism Success in the Los Angeles Police Department*. New York, NY: The Manhattan Institute and Cambridge, MA: John F. Kennedy School of Government, Harvard University.
- McDowell, D. (2000). *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*. Cooma, NSW, Australia: Istana Enterprises, Pty., Ltd.
- McEwen, T. (2011). *The Role and Impact of Forensic Evidence in the Criminal Justice System*. Alexandria, VA: The Institute for Law and Justice.
- McKnight, G. D. (1987). (Winter). "A Harvest of Hate: The FBI's War Against Black Youth – Domestic Intelligence in Memphis, Tennessee." *South Atlantic Quarterly* 86: 1–21.
- McNamara, T. (2008). *Annual Report to the Congress on the Information Sharing Environment*. Washington, DC: Program Manager-Information Sharing Environment.
- McNamara, T. (April 26, 2007). Statement for the Record before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Committee on Homeland Security.

- McNamara, T. (April 26, 2007). Statement of the Program Manager-Information Sharing Environment before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Homeland Security Committee, U.S. House of Representatives.
- Michigan State University and University of Illinois at Chicago. (2013), "Promising Strategies for Violence Reduction: Lessons from Two Decades of Innovation," *Project Safe Neighborhoods Case Study Report #13*, Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance,
- Modafferi, P., and Bouche, K. (2005). "Intelligence Sharing: Efforts to Develop fusion center Intelligence Standards." *The Police Chief*. (February). Vol 72, No. 2.
- Modzeleski, W., and Randazzo, M. R. (2018). "School Threat Assessment in the USA: Lessons Learned from 15 Years of Teaching and Using the Federal Model to Prevent School Shootings." *Contemporary School Psychology* 22, 109–115.
- Morabito, A., and Greenberg, S. (2005). *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington, DC: Bureau of Justice Assistance.
- Mund, B. (2018). "Social Media Searches and the Reasonable Expectation of Privacy." *Yale Journal of Law and Technology*, 19(1), 238–273.
- Murphy, W. (November 27, 2007). Statement by the former FBI Assistant Director, Directorate of Intelligence at the 2007 IACP Intelligence Summit, Washington, DC.
- Muslim Public Affairs Council. (2003). *A Review of U.S. Counterterrorism Policy: American Muslim Critique and Recommendations*. Washington, DC: Muslim Public Affairs Council, p. 8.
- National Advisory Commission on Civil Disorders. (1968). *Summary Report*. Washington, DC: U.S. Government Printing Office.
- National Advisory Commission on Criminal Justice Standards and Goals. (1973). *Police*. Washington, DC: U.S. Government Printing Office.
- National Advisory Commission on Criminal Justice Standards and Goals. (1976). *Report of the Task Force on Disorder and Terrorism*. Washington DC: U.S. Government Printing Office.
- National Advisory Commission for Criminal Justice Standards and Goals. (1976). *Task Force Report on Organized Crime*. Washington, DC: U.S. Government Printing Office.
- National Centre for Policing Excellence. (2005). *Guidance on the National Intelligence Model*. London, UK: Association of Chief Police Officers.
- National Commission on the Causes and Prevention of Violence. (1968). *Law and Order Reconsidered*. Washington, DC: U.S. Government Printing Office.
- National Criminal Intelligence Sharing Plan, Version 2.0*. (2013). Washington, DC: Criminal Intelligence Coordinating Council.
- National Criminal Justice Association. (NCJA). (2002). *Justice Information Privacy Guide*. Washington, DC: NCJA.
- National Preparedness Directorate. (2007). *Targeted Capabilities List*. Washington, DC: U.S. Department of Homeland Security.
- National Strategy for Homeland Security*. (2002). Washington, DC: Executive Office of the President.
- Next Generation CJIS?*. (March 2006). "Time System Newsletter of the Wisconsin Department of Justice." Volume 2005-2, p. 1.
- Novak, M. (2020). "Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and issues for Consideration." *Journal of Digital Forensics, Security and Law*. Vol. 14, No. 4, Article 3.
- Office of Intelligence and Analysis. (2008). *National Strategy for the Fire Service Intelligence Enterprise*. Washington, DC: U.S. Department of Homeland Security.
- Office of the Chief Intelligence Officer. (2006). *DHS Intelligence Enterprise Strategic Plan*. Washington, DC: U.S. Department of Homeland Security.
- Office of the Director of National Intelligence (ODNI). (October 17, 2007). ICD 206. *Sourcing Requirements for Disseminated Analytic Requirements*.
- Office of the Director of National Intelligence. (2007). *National Open Source Enterprise*. Washington, DC: ODNI.

- Office of the Inspector General. (May 2008). *The Drug Enforcement Administration use of Intelligence Analysts*. Washington, DC: U.S. Department of Justice.
- Office of the Under Secretary for Intelligence and Analysis. (2012). *DHS Intelligence Enterprise Product Line Brochure*. Washington, DC: Department of Homeland Security.
- Orrick, W. D. (undated). *Best Practices Guide: Developing a Police Department Policy-Procedure Manual*. Alexandria, VA: International Association of Chiefs of Police.
- Peterson, M. (2005). *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC: Bureau of Justice Assistance.
- Peterson, M. (1994). *Applications in Criminal Analysis: A Sourcebook*. Westport, CT: Greenwood Press.
- Peterson, M., et al. (1996). *Successful Law Enforcement Using Analytic Methods*. Richmond, VA: International Association of Law Enforcement Intelligence Analysts.
- Peterson, M., Morehouse, B., and Wright, R. (eds.). (2000). *Intelligence 2000: Revising the Basic Elements*. Sacramento, CA: Law Enforcement Intelligence Unit, and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc.
- Pherson, R. H., and Richards, J. H. (2020). *Structured Analytic Techniques for Intelligence Analysis*. 3rd. ed. Thousand Oaks, CA: Sage Publications.
- Pistole, J. S. (August 23, 2004). Former FBI Executive Assistant Director of Counterterrorism and Counterintelligence. Statement before the House Judiciary Committee Subcommittee on Crime, Terrorism and Homeland Security.
- Planty, M., Banks, D., Lindquist, C., Cartwright, J., and Witwer, A. (2020). *Tip Lines for School Safety: A National Portrait of Tip Line Use*. Research Triangle Park, NC: RTI International/National Institute of Justice.
- Police Executive Research Forum. (2013). *CompStat: Its Origins, Evolution, and Future in Law Enforcement Agencies*, Washington, DC, U.S. Department of Justice, Bureau of Justice Assistance.
- Predictive Analytics Handbook for National Defense*. (2020). McClean, VA: Booz Allen Hamilton.
- President's Commission on Law Enforcement and Administration of Justice. (1967). *Task Force Report: Organized Crime*. Washington, DC: U.S. Government Printing Office.
- President's Commission on Organized Crime. (1984). *Organized Crime and Money Laundering*. Washington, DC: U.S. Government Printing Office, 1984.
- President's Commission on Organized Crime. (1987). *Final Report*. Washington, DC: U.S. Government Printing Office.
- Privacy Impact Statement for the Homeland Security Information Network Database*. (April 5, 2006). Washington, DC: Unpublished report of the DHS Office of Operations Coordination.
- Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*. (2010). Washington, DC: Global Justice Information Sharing Initiative.
- Promising Practices in Forensic Lab Intelligence*. (2019). Washington, DC: Global Advisory Committee.
- Protecting Your Community from Terrorism*. (undated). Washington, DC: COPS/PERF.
- Ramsey, T. (May 9, 2007). *Global Maritime Intelligence Integration (GMII) Enterprise*. PowerPoint Presentation. Washington, DC: Office of the Director of National Intelligence.
- Randol, M. A. (2009). *Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches*. Washington, DC: Congressional Research Service.
- Ratcliffe, J., and Guidetti, R. (2007) "State Police Investigative Structure and the Adoption of Intelligence-Led Policing." *Policing: An International Journal of Police Strategies and Management*.
- Ratcliffe, J. H. (2004). "The Structure of Strategic Thinking." In J. H. Ratcliffe (ed.), *Strategic Thinking in Criminal Intelligence*. Sydney, NSW, Australia: Federation Press. pp. 1–10.
- Ratcliffe, J. H. (2008). *Intelligence-Led Policing*. Cullompton, Devon, UK: Willan Publishing.

- Ratcliffe, J. H. (2007). *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.
- Reducing Crime Through Intelligence Led Policing*. (2012). Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance.
- Reese, S. (2005). *State and Local Homeland Security: Unresolved Issues for the 109th Congress*. Washington, DC: Congressional Research Service, Library of Congress.
- Reiber, J. (2019). *A Public, Private War: How the U.S. Government and U.S. Technology Sector Can Build Trust and Better Prepare for Conflict in the Digital Age*. Berkeley, CA: Center for Long-Term Cyber Security.
- Riley, K. K., Treverton, G., Wilson, J., and Davis, L. (2005). *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation.
- Rossmo, D. K. (2000). *Geographic Profiling*. Boca Raton, FL: CRC Press.
- Sanders, C., Weston, C., and Schott, N. (2015). Police Innovations, “Secret Squirrels” and Accountability: Empirically Studying Intelligence-Led Policing in Canada. *British Journal of Criminology*, 55(4), 711–729.
- Saupp, K. (February 2010). “Fusion Liaison Officer Programs: Effective Sharing of Information to Prevent Crime and Terrorism.” *Police Chief Magazine*.
- Saupp, K., Engelhardt, D., Collins, M., and Hale, B. (August 2017). “Integrating State and Local Expertise into the Intelligence Community.” *Police Chief Magazine*.
- Schaible, L. M., and Sheffield, J. (2012). Intelligence-led policing and change in state law enforcement agencies. *Policing: An International Journal of Police Strategies and Management*, 35: 761-784.
- Scheider, M., Chapman, R., and Seelman, M. (2004). “Connecting the Dots for a Proactive Approach.” Border and Transportation Security. Washington, DC: Office of Community Oriented Policing Services.
- Scott, M. S. (2000). *Problem-Oriented Policing: Reflections on the First 20 Years*. Washington, DC: Office of Community Oriented Policing Services.
- Security Clearances*. (2004). GAO-04-596. Washington, DC: U.S. General Accountability Office.
- Shane, J. (2004). “CompStat Process.” *FBI Law Enforcement Bulletin*. Vol. 73, No. 2. (April). pp. 12–23.
- Simeone, M. J. (2007). *The Integration of Virtual Public-Private Partnerships in Law Enforcement to Achieve Enhanced Intelligence-Led Policing*. Monterey, CA: A thesis prepared for the Naval Postgraduate School.
- Staff Statement No. 12: *Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States*. (2004). National Commission on Terrorist Attacks Upon the United States.
- Steigman, J. L. (2003). “Reversing Reform: The Handschu Settlement in Post-September 11 New York City.” *Brooklyn Journal of Law and Policy*. Vol. 11, p. 759.
- Stone, K. (2006). *Deploying and Operating an Effective Regional Fusion System: Lessons Learned from the North Central Texas Fusion System*. Unpublished policy paper prepared by the North Central Texas Fusion System, McKinney, TX.
- Sullivan, J. P. (2005). *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence*. A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada.
- Suspicious Activity Report Support and Implementation Project. (2008). *Final Report*. Washington, DC: Major City Chiefs Association; U.S. Department of Justice and U.S. Department of Homeland Security.
- Target Capabilities List*. (2007). Washington, DC: National Preparedness Directorate. U.S. Department of Homeland Security.
- Taylor, R., and Russell, A. (2012). The failure of police fusion centers and the concept of national intelligence sharing plan. *Police Practice and Research*, 13(2), 184–200.
- Telep, C. W., Read, J., and Bottema, A. J. (2017). “Working Towards Intelligence-Led Policing: The Phoenix Police Department Intelligence Officer Program. *Policing: A Journal of Policy and Practice*, doi:10.1093/police/pax094.
- The “Crime Gun Intelligence Center” Model: Case Studies of the Denver, Milwaukee, and Chicago Approaches to Investigating Gun Crime*. (2017). Washington, DC: Police Executive Research Forum.

- The Center for Community Safety. (2013). *Winston-Salem Intelligence-Led Policing: A Blueprint for Implementing*. Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance.
- “The Rise of Cybercrime as a Service.” (2017). *CSO Online—Cybersecurity Insights*.
- The Warren Commission Report. (2003). *Report of the President’s Commission on the Assassination of President John F. Kennedy*. New York: Barnes and Noble, Inc. [Originally published in 1964].
- This is Not a Game: How the Gaming Website ‘Steam’ Harbors Extremists*. (2020). New York NY: Anti-Defamation League.
- Townsley, M., Johnson, S., and Pease, K. (2003). “Problem Orientation, Problem Solving and Organizational Change.” *Crime Prevention Series*. Vol. 15 (pp. 183–212). Monsey, NY: Criminal Justice Press.
- Tsesis, A. (2017). “Social Media Accountability for Terrorist Propaganda.” *Fordham Law Review*, V86, 12, 605–631.
- United States Senate Select Committee to Study Government Operations. (1976). *Intelligence Activities: Final Report*. Washington, DC: U.S. Government Printing Office.
- United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (April 26, 1976). *Intelligence activities and the rights of Americans: Final report*. Book II.
- Vossekuil, B., Fein, R., Reddy, M., Borum, R., and Modzeleski, W. (2002). *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*. Washington, D.C.: U.S. Secret Service and Department of Education.
- Waters, G. (2012). Social Media and Law Enforcement. *FBI Law Enforcement Bulletin*, Vol. 81, No. 11, p. 2.
- Weimer, D. R. (2005). *The Copyright Doctrine of Fair Use and the Internet: Case Law*. Washington, DC: Congressional Research Service.
- Wells, I. (2000). “Staffing the Intelligence Unit.” (2000). *Intelligence 2000: Revising the Basic Elements*. A joint publication of the Law Enforcement Intelligence Unit and the International Association of Law Enforcement Intelligence Analysts.
- Williams, H., and Blum, I. (2018). *Defining Second Generation Open Source Intelligence for the Defense Enterprise*. Santa Monica, CA: RAND Corporation.
- Wongthongtham, P., et al. (2018). “State-of-the-Art Ontology Annotation for Personalized Teaching and Learning and Prospects for Smart Learning Recommender Based on Multiple Intelligence and Fuzzy Ontology.” *International Journal of Fuzzy Systems*. Vol. 20, No. 4, pp. 1357–1372.
- Wortzel, L. (2002). “Creating an Intelligent Department of Homeland Security.” *Executive Memorandum 828*. Washington, DC: Heritage Foundation.





# APPENDIX A

## ACRONYMS FOR LAW ENFORCEMENT INTELLIGENCE

The number of acronyms used by all levels of government is massive. Rather than attempt to develop a list of acronyms that is completely comprehensive, those listed in this appendix are the ones most likely to be encountered in law enforcement intelligence as well as those used in this guide. For a significantly expanded listing of words, phrases, acronyms, and their authority, as applicable, see the DHS Lexicon at <https://www.dhs.gov/publication/dhs-lexicon>.

For an exhaustive list of acronyms that go far beyond the intelligence discipline, see <https://www.dhs.gov/terms>.

AAR	After-Action Report
ACS	Automated Case System (FBI)
ADNET	Anti-Drug Network
AFIS	Automated Fingerprint Identification System
AFIWC	Air Force Information Warfare Center
AGILE	Advanced Generation of Interoperability for Law Enforcement
AI	Artificial Intelligence
ALPR	Automated License Plate Reader

AOR	Area of Responsibility	CALEA	Commission on Accreditation of Law Enforcement Agencies	CI	Confidential Informant as used by investigators
ARJIS	Automated Regional Justice Information System	CALEA	Communications Assistance for Law Enforcement Act	CI/KR	Critical Infrastructure/Key Resources
ASAC	Assistant Special Agent in Charge	CAT	Communities Against Terrorism	CIA	Central Intelligence Agency
ASCLD	American Society of Crime Lab Directors	CBA	Collective Bargaining Agreement	CICC	Criminal Intelligence Coordinating Council
ATAC	Anti-Terrorism Advisory Council	CBP	U.S. Customs and Border Protection	CICE	Criminal Intelligence for the Chief Executive Training Program
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives	CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive	CIIMS	Critical Infrastructure Inspection Management System
ATPA	Auto Theft Prevention Authority	CDC	Centers for Disease Control and Prevention	CIO	Chief Information Officer
BATIC	Border Auto Theft Information Center	CDICG	Counterdrug Intelligence Coordination Group	CIP	Critical Infrastructure Protection
BATS	Bombing and Arson Tracking System (ATF)	CDX	Counterdrug Intelligence Executive Secretariat	CIPA	Classified information Procedures Act
BJA	Bureau of Justice Assistance, U.S. Department of Justice	CERT	Computer Emergency Response Team	CIPWG	Critical Infrastructure Protection Working Group
BLS	As used by OJP and DHS, Blended Learning Strategy	CFI	Certified Firearms Instructor	CIRT	Computer Incident Response Team
BLS	As used by the Department of Commerce, Bureau of Labor Statistics	CFR	Code of Federal Regulations	CISAnet	Criminal Information Sharing Alliance Network
BRTC	Border Research Technology Center	CGIC	Crime Gun Intelligence Center	CITAC	Computer Investigation and Infrastructure Threat Assessment Center
BSA	Bank Secrecy Act (FinCEN-related)	CHRI	Criminal History Record Information	CJIS	Criminal Justice Information Services of the FBI
BWC	Body-Worn Camera	CI	Counterintelligence as used by the Intelligence Community	CLE	Criminal Law Enforcement
C3	Command, Control, and Communications	CI	Critical Infrastructure as used by DHS	CLEAR	Chicago Citizen and Law Enforcement Analysis and Reporting
C3I	Command, Control, Communications, and Information				
CAD	Computer-Aided Dispatch				

CODIS	Combined DNA Indexing System	CUI	Controlled Unclassified Information	DOJ	U.S. Department of Justice
COMINT	Communications Intelligence	CVE	Countering Violent Extremism	DOS	U.S. Department of State
COMPSTAT	Computerized Statistics (also CompStat)	CVNIP	Commercial Vehicle Narcotics Interdiction Program	DOT	Department of Transportation
COMSEC	Communications Security	CWIN	Critical Infrastructure Warning Information Network	DTO	Drug Trafficking Organization
CONOPS	Concept of Operations			EMS	Emergency Medical Services
CONUS	Continental United States	DCI	Director of Central Intelligence	EOC	Emergency Operations Center
COPS	Office of Community Oriented Policing Services	DDNIR	Domestic DNI Representative	EOP	Executive Office of the President
CP	Community Policing	DDoS	Distributed Denial of Service Attack	EPIC	El Paso Intelligence Center
CP	Crime Prevention	DEA	U.S. Drug Enforcement Administration	ERT	Evidence Response Team (FBI)
CPTED	Crime Prevention Through Environmental Design	DHS I&A	Department of Homeland Security, Office of Intelligence and Analysis	EUROPOL	European Agency for Law Enforcement Cooperation
CRS	Congressional Research Service			FAS	Federation of American Scientists
CSDN	Customs Secure Data Network	DHS IE	Intelligence Enterprise	FBI OPE	Office of Partner Engagement
CST	Civil Support Team (Regional National Guard WMD Teams)	DHS	U.S. Department of Homeland Security	FBI	Federal Bureau of Investigation
CT	Counterterrorism	DIA	Defense Intelligence Agency	FBINET	FBI (Secret Level) Network
CTAC	Counter-Drug Technology Assessment Center	DISA	Defense Information Systems Agency	FEMA	Federal Emergency Management Agency
CTC	Counter-Terrorism Center	DISN	Defense Information System Network	FFL	Federal Firearm License
CTISS	Common Terrorism Information Sharing Standards	DL	Driver's License	FIDM	Federated Identity Management
CTO	Chief Technology Officer	DNA	Deoxyribonucleic Acid (for biometric identification)	FI	Field Interview/Field Interview Card
CTTWG	Counterterrorism Training Working Group	DNI	Director of National Intelligence	FIG	Field Intelligence Group of the FBI Field Offices
		DNS	Domain Name Servers		
		DoD	U.S. Department of Defense		

FinCEN	Financial Crimes Enforcement Network	HIDTA	High Intensity Drug Trafficking Area	IAFIS	Integrated Automated Fingerprint Identification System
FLETC	Federal Law Enforcement Training Centers	HIFCA	High Intensity Financial Crime Area	IAIP	DHS Information Analysis and Infrastructure Protection Directorate
FOIA	Freedom of Information Act	HIPAA	Health Insurance Portability and Accountability Act		
FOUO	For Official Use Only	HIR	Homeland Intelligence Reports	IALEIA	International Association of Law Enforcement Intelligence Analysts
FPS	Federal Protective Service	HIVA	Hazard Identification and Vulnerability Assessment	IC	Intelligence Community
FR	Facial Recognition				
FSIE	Fire Service Intelligence Enterprise	HQ	Headquarters	ICE	U.S. Immigration and Customs Enforcement
FTTTF	Foreign Terrorist Tracking Task Force	HS	Homeland Security		
FY	Fiscal Year	HSAS	Homeland Security Advisory System	ICEPIC	ICE Pattern Analysis and Information Collection System
GAC	Global Justice Information Sharing Initiative Advisory Committee	HSDN	Homeland Security Data Network (secret level network)	ICHAT	Internet Criminal History Access Tool
GAO	General Accountability Office	HSIN	Homeland Security Information Network	ICS	Incident Command System
GISC	Gang Intelligence Strategy Committee (of Global)	HSPD	Homeland Security Presidential Directive	IED	Improvised Explosive Device
GIWG	Global Intelligence Working Group	HUMINT	Human Intelligence	IEPD	Information Exchange Package Description
GJXDM	Global Justice Extensible Markup Language Data Model	HVE	Homegrown Violent Extremist	III	Interstate Identification Index
Global	Global Justice Information Sharing Initiative	I&A	Office of Intelligence and Analysis	ILO	Intelligence Liaison Officer or Industry Liaison Officer
GPS	Global Positioning System	IA	Information Assurance	ILP	Intelligence-Led Policing
GSA	General Services Administration	IACP	International Association of Chiefs of Police	IMINT	Imagery Intelligence
HazMat	Hazardous Materials Team	IAD	Internal Affairs Division	INFOSEC	Information Systems Security
HEAT	Help End Auto Theft Program	IADLEST	International Association of Directors of Law Enforcement Standards and Training	INTERPOL	International Criminal Police Organization
				IoT	Internet of Things
				IP	Internet Protocol

IRS	Intelligence Resource Specialist	JTTF	Joint Terrorism Task Force	MIPT	Memorial Institute for the Prevention of Terrorism
IRS	Internal Revenue Service	KR	Key Resources	ML	Machine Learning
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004	LE	Law Enforcement	MOA	Memorandum of Agreement
		LEA	Law Enforcement Agency	MOCIC	Mid-States Organized Crime Information Center (a RISS Center)
ISAC	Information Sharing and Analysis Centers	LECC	Law Enforcement Coordinating Committee (DOJ)	MOU	Memorandum of Understanding
ISC	Information Sharing Council	LEEP	Law Enforcement Enterprise Portal (of the FBI)	NamUS	National Missing and Unidentified Persons System
ISE	Information Sharing Environment	LEI	Law Enforcement Intelligence	NARA	National Archives and Records Administration
ISI	Gateway Information Sharing Initiative	LEIN	Law Enforcement Information Network	NCB	National Central Bureau (U.S. contact for INTERPOL)
ISOO	Information Security Oversight Office	LEISP	Law Enforcement Information Sharing Program	NCBI	National Center for Biotechnology Information
ISR	Intelligence, Surveillance, and Reconnaissance	LEIU	Law Enforcement Intelligence Unit	NCIC	National Crime Information Center
IT	Information Technology	LES	Law Enforcement Sensitive	NCIRC	National Criminal Intelligence Resource Center
ITACG	Interagency Threat Assessment Coordination Group (Part of NCTC)	LIInX	Law Enforcement Information Exchange	NCIS	Naval Criminal Investigative Service
		MAGLOCLEN	Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (a RISS Center)	NCISP	National Criminal Intelligence Sharing Plan
ITWG	Intelligence Training Working Group	MASINT	Measurement and Signatures Intelligence	NCJRS	National Criminal Justice Reference Service
IW	Information Warfare	MATRIX	Multistate Anti-Terrorism Information Exchange	NCTC	National Counterterrorism Center
JABS	Joint Automated Booking System	MCCA	Major Cities Chiefs Association	NDCAC	National Domestic Communications Assistance Center
JCAT	Joint Counterterrorism Assessment Team	MCSA	Major County Sheriffs of America		
JCON	Justice Consolidated Office Network				
JITF–CT	Joint Intelligence Task Force–Combating Terrorism				
JRIES	Joint Regional Information Exchange System				

N-DEX	Law Enforcement National Data Exchange	NIPC	National Infrastructure Coordination Center	NSL	National Security Letter
NDPIX	National Drug Pointer Index	NIPP	National Infrastructure Protection Plan	NSS	National Seizure System (DEA)
NESPIN	New England State Police Information Network (a RISS Center)	NIPRNET	Non-classified Internet Protocol Router Network	NTAC	United States Secret Service National Threat Assessment Center
NFCA	National Fusion Center Association	NISP	National Industrial Security Program	NTC	National Tracing Center (ATF firearms tracing)
NFCCG	National Fusion Center Coordination Group	NIST	National Institute of Standards and Technology	NTER	National Threat Evaluation and Reporting Program
N-FOCIS	National Field Office Case Information System (of ATF)	NJTTF	National Joint Terrorism Task Force	NVPS	National Virtual Pointer System
NGA	National Governors Association	NLECTC	National Law Enforcement and Corrections Technology Centers	NVTC	National Virtual Translation Center
NGI	Next Generation Identification System	NLETS	National Law Enforcement Telecommunications System	NW3C	National White Collar Crime Center
NGIC	National Gang Intelligence Center	NMEC	National Media Exploitation Center	OCA	Original Classification Authority
NIBIN	National Integrated Ballistic Information Network	NNFC	National Network of Fusion Centers	OCDEF	Organized Crime Drug Enforcement Task Force
NIBRS	National Incident Based Reporting System	NOC	National Operations Center	OCONUS	Outside the Continental United States
NICS	National Instant Criminal Background Check System	NSA	National Security Agency	ODMAP	Overdose Detection Mapping Application Program
NIEM	National Information Exchange Model	NSA	National Sheriffs' Association	ODNI	Office of the Director of National Intelligence
NIJ	National Institute of Justice	NSD	National Security Directive	OIG	Office of Inspector General
NIM	British National Intelligence Model	NSI	National Security Information or Intelligence	OJP	Office of Justice Programs
NIMA	National Imagery and Mapping Agency	NSI	Nationwide Suspicious Activity Reporting Initiative	OMB	Office of Management and Budget
NIMS	National Incident Management System	NSIS	National Strategy for Information Sharing		

OPM	Office of Personnel Management	RFI	Request for Information	SIGINT	Signal Intelligence
OPSEC	Operations Security	RFS	Request for Service	SIPRNET	Secret Internet Protocol Router Network
OS	Open Source	RICO	Racketeering Influenced Corrupt Organization	SITG	Security Intelligence Threat Group (typically in corrections agencies)
OSIF	Open Source Information				
OSINT	Open Source Intelligence	RISC	Repository for Individuals of Special Concern (FBI)	SLATT	State and Local Anti-Terrorism Training Program of BJA
OSIS	Open Source Information System	RISS	Regional Information Sharing Systems		
P/CRCL	Privacy, Civil Rights and Civil Liberties	RISSNET	RISS Secure Cloud	SLIC	State and Local Intelligence Community of Interest
P3I	Public-Private Partnership for Intelligence	RMIN	Rocky Mountain Information Network (a RISS Center)	SLT	State, Local, and Tribal
PC	Personal Computer	RMS	Records Management System	SLTLE	State, Local, and Tribal Law Enforcement
PCII	Protecting Critical Infrastructure Information	ROCIC	Regional Organized Crime Information Center (a RISS Center)	SLTT	State, Local, Tribal, and Territorial
PDF	Portable Document Format	SAC	Special Agent in Charge (FBI, DEA, ATF)	SOP	Standard Operating Procedure (directives at the division/unit level)
PE-ISE	Partner Engagement-Information Sharing Environment	SAP	Special Access Programs	SPIN	Security/Police Information Network, Nassau County, New York
PGC	Privacy Guidelines Committee	SAR	Suspicious Activity Report		
PII	Personally Identifiable Information	SATINT	Satellite Intelligence	SPPADS	State and Provincial Police Academy Directors Section
PM-ISE	Program Manager – Information Sharing Environment	SBU	Sensitive But Unclassified		
PPE	Personal Protective Equipment	SCC	Sector Coordinating Councils	START	National Consortium for the Study of Terrorism and Responses to Terrorism
PPP	Public-Private Partnerships	SCI	Sensitive Compartmented Information	SVTC	Secure Video Teleconference
PSP	National Public Safety Partnership	SCIF	Sensitive Compartmented Information Facility	SWBSADIS	Southwest Border States Anti-Drug Information System
R&D	Research and Development	SHSI	Sensitive Homeland Security Information		
RAC	Resident Agent in Charge	SIG	Special Interest Groups	TAG	Transnational Anti-Gang Task Force (FBI)

TCL	Target Capabilities List	VPN	Virtual Private Network
TDY	Temporary Duty		
TEW	Terrorism Early Warning Group	WMD	Weapons of Mass Destruction
TFO	Task Force Officer	WSIN	Western States Information Network (a RISS Center)
TIP	DOS Terrorist Interdiction Program		
TLO	Terrorism Liaison Officer	XML	Extensible Markup Language
TLP	Traffic Light Protocol		
TRP	Threat Review and Prioritization Process		
TS	Top Secret		
TSA	Transportation Security Act and Transportation Security Administration		
TSC	Terrorist Screening Center		
TSDB	Terrorist Screening Database (of the TSC)		
TTIC	Terrorist Threat Integration Center		
UCR	Uniform Crime Reports		
URL	Uniform Resource Locator		
USAO	United States Attorney's Office		
USC	United States Code		
VBIED	Vehicle-Based Improvised Explosive Device		
VGTOF	Violent Gang and Terrorist Organization File of NCIC		
VICAP	Violent Criminal Apprehension Program		
VIN	Vehicle Identification Number		

The graphic features three overlapping hexagonal shapes. The leftmost hexagon is dark blue and contains various digital icons like a star, a person, and a bar chart, connected by dotted lines. The middle hexagon is a solid dark blue. The rightmost hexagon is light blue and shows a person's hands typing on a laptop keyboard. The background is a light blue gradient.

# APPENDIX B

## GLOSSARY OF TERMS FOR LAW ENFORCEMENT INTELLIGENCE

Law enforcement agencies at all levels of government are working together more than ever to support information sharing. It is important to note that there is a tremendous effort under way to streamline intelligence processes to facilitate information sharing. As a result, criminal intelligence terminology is changing and sometimes merging. The definitions contained herein are provided from the perspective of law enforcement intelligence primarily, but not exclusively as used at the state, local, and tribal levels. Further, it is recognized that some words and phrases will have alternate or additional meanings when used in the context of national security intelligence, the military, or the private sector. The definitions are intended to be merely descriptive of an entity, issue, or process that may be encountered by those working within the criminal intelligence function. Definitions may differ according to state statutes or local rules.

## GLOSSARY OF LAW ENFORCEMENT INTELLIGENCE TERMS

**Actionable:** Intelligence and information with sufficient specificity and detail that explicit responses to prevent a crime or terrorist attack can be implemented.

**Administrative Analysis:** The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions.

**All-Hazards Intelligence:** The collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat. (Same as Homeland Security Intelligence).

**Allocation:** Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

**Analysis of Competing Hypotheses (ACH):** An eight-step procedure to help analysts make judgments on important issues requiring careful weighing of alternative explanations or conclusions. The process leaves an audit trail to show what analysts considered and how they arrived at their judgment.

**Analysis:** That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

**Analytic Writing:** Written communication focusing on distilling and summarizing factual information to provide concise and clear reports for managers and other customers.

**Archiving (Records):** The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

**Assessments:** Strategic and tactical assessments to assess the impact of a crime group or a criminal activity on a jurisdiction, now or in the future. These may include assessments of threat, vulnerability, or risk.

**Association Analysis/Link Analysis:** Collection and analysis of information that indicates relationships among varied individuals suspected of involvement in criminal activity and provision of insight into the criminal operation and which investigative strategies might be the most effective.

**Association Analysis:** The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix.

**Bias/Hate Crime:** Any criminal act directed toward any person or group as a result of that person's or group's race, ethnicity, religious affiliation, or sexual preference.

**C3:** An intelligence application concept initially used by military intelligence that stands for command, control, and communication as the hallmark for effective intelligence operations.

**Clandestine Activity:** An activity that is usually extensive and goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. "Storefront" operations, "stings," and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine collections.

**Classified Information/Intelligence:** A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is maintained in confidence to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities.

**Collation (of information):** A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement

of useful information into a form or system that permits easy and rapid access and retrieval.

**Collection (of information):** The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the intelligence cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

**Collection Plan:** The preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information, and a timeline for collecting the information.

**Command and Control:** Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.

**Commodity (Illegal):** Any item or substance that is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted, or marketed in an unlawful manner.

**Commodity Flow Analysis:** Graphic depictions and descriptions of transactions, shipment, and distribution of contraband goods and money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities.

**Communications Intelligence (COMINT):** The capture of information, either encrypted or in “plaintext,” exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and/or analysis of the substantive meaning of the communication.

**Conclusion:** A definitive statement about a suspect, action, or state of nature based on the analysis of information.

**Confidential Classification:** Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

**Confidential:** See Classified Information/Intelligence, Confidential Classification.

**Continuing Criminal Enterprise:** Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity, that are involved in a continuing or perpetuating criminal activity.

**Controlled Unclassified Information (CUI):** A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended.

**Coordination:** The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

**Counterintelligence:** Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, or subversion that is related to national security concerns. A national security intelligence activity that involves blocking or developing a strategic response to other groups, governments, or individuals through the identification, neutralization, and manipulation of their intelligence services.

**Covert Intelligence:** A covert activity is planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity.

**Crime Analysis:** The process of analyzing information collected on crimes and police service delivery variables to give direction for police officer deployment, resource allocation, and policing strategies as a means to maximize crime prevention activities and the cost-effective operation of the police department.

**Crime-Pattern Analysis:** An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables.

**Criminal History Record Information (CHRI):**

Information collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any disposition arising therefrom, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

**Criminal Informant:** See Informant.

**Criminal Intelligence:** The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends or support informed decision making by management. (Same as Law Enforcement Intelligence).

**Criminal Investigative Analysis:** An analytic process that studies serial offenders, victims, and crime scenes to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s).

**Criminal Predicate:** Information about an individual or his/her behavior that may only be collected and stored in a law enforcement intelligence records system when there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

**Critical Infrastructure/Key Resources:** The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

**Critical Infrastructure:** Certain national infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

**Critical Thinking:** The objective, open, and critical cognitive process applied to information to achieve a greater understanding of data, often through developing and answering questions about the data.

**Cryptanalysis:** The process of deciphering encrypted communications of an intelligence target.

**Cryptography:** The creation of a communications code/ encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

**Cryptology:** The study of communications encryption methods that deal with the development of codes and the scrambling of communications to prevent the interception of the communications by an unauthorized or unintended party.

**Customers:** Consumers of intelligence products who may be within the analyst's agency or in other agencies or organizations.

**Cybersecurity:** Improving resiliency and reducing threats related to computers or computer networks.

**Data Element:** A field within a database that describes or defines a specific characteristic or attribute.

**Data Owner:** The agency that originally enters information or data into a law enforcement records system.

**Data Quality:** Controls implemented to ensure that all information in a law enforcement agency's records system is complete, accurate, and secure.

**Data Sources:** Various sources of information that analysts may utilize as they develop analytical products, resources, reports, and briefings.

**Data:** Raw facts or measurable variables used as a basis for reasoning, discussion, or calculation.

**Deconfliction:** The process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime and which provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is an information and intelligence

sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

**Deductive Logic:** The reasoning process of taking information and arriving at conclusions from within that information.

**Delphi Method:** A method developed by the RAND Corporation that entails a group of experts who anonymously reply to questionnaires and subsequently receive feedback in the form of a statistical representation of the group response, after which the process repeats itself. The goal is to reduce the range of responses and arrive at something closer to expert consensus.

**Demographic/Social Trend Analysis:** An examination of the nature of demographic changes and their impact on criminality, the community, and law enforcement.

**Deployment:** The short-term assignment of personnel to address specific crime problems or police service demands.

**Designated State and/or Major Urban Area Fusion Center:** The fusion center in each state designated as the primary or lead fusion center for the information sharing environment.

**Dissemination (of Intelligence):** The process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

**Due Process:** Fundamental fairness during the course of the criminal justice process, including adherence to legal standards and the civil rights of the police constituency; the adherence to principles that are fundamental to justice.

**El Paso Intelligence Center (EPIC):** A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. The primary concern is drug trafficking; however, intelligence on other crimes is also managed by EPIC.

**Emergency Management:** The coordination and integration of all activities necessary to build, sustain, and improve the capabilities to prepare for, respond to, recover from, or mitigate against threatened or actual disasters or emergencies, regardless of cause.

**Enterprise:** Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity.

**Estimate:** See Intelligence Estimate.

**Evaluation (of Information):** All information collected for the intelligence cycle is reviewed for its quality with an assessment of the validity and reliability of the information.

**Event Flow Analysis:** Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event, intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events.

**Exemptions (to the Freedom of Information Act):** Circumstances wherein a law enforcement agency is not required to disclose information from a Freedom of Information Act (FOIA) request.

**Feedback/Reevaluation:** A review of the operation of the intelligence process and the value of the output to the consumer.

**Field Intelligence Group (FIG):** The centralized intelligence component in a Federal Bureau of Investigation (FBI) field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

**Field Intelligence Report (FIR):** An officer-initiated interview of a person believed by the officer to be acting in a suspicious manner that may be indicative of planning or preparing to conduct criminal activity.

**Financial Analysis:** A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and applications of funds, financial statement analysis, and/or Bank Secrecy Act record

analysis. It can also show destinations of proceeds of crime and support prosecutions.

**Flow Analysis:** The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. It can include timelines, event flow analysis, commodity flow analysis, and activity flow analysis. May show missing actions or events that need further investigation.

**For Official Use Only (FOUO):** A designation applied to unclassified sensitive information that may be exempt from mandatory release to the public under the FOIA.

**Forecast (as related to Criminal Intelligence):** The product of an analytic process that provides a probability of future crimes and crime patterns based on a comprehensive, integrated analysis of past, current, and developing trends.

**Freedom of Information Act (FOIA):** The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

**Fusion Center Guidelines:** A series of nationally recognized standards developed by law enforcement intelligence subject-matter experts designed for the good practice of developing and managing an intelligence fusion center.

**Fusion Center:** The physical location of the law enforcement intelligence fusion process.

**Fusion Process:** The overarching process of managing the flow of information and intelligence across levels and sectors of government.

**Geographic Analysis:** An evaluation of the locations of criminal activity or criminals to determine whether future criminal activity can be deterred or interdicted through forecasting activity based on historical raw data.

**Granularity:** Considers the specific details and pieces of information, including nuances and situational inferences that constitute the elements on which intelligence is developed through analysis.

**Guidelines:** See Intelligence Records Guidelines.

**Homeland Security Advisory System:** An information and communications structure designed by the U.S. government for disseminating information to all levels of government and the American people regarding the risk of terrorist attacks and for providing a framework to assess the risk at five levels: Low, Guarded, Elevated, High, and Severe.

**Homeland Security Intelligence:** The collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat. (Same as All Hazards Intelligence).

**Human Intelligence (HUMINT):** Intelligence-gathering methods that require human interaction or observation of the target or targeted environment. The intelligence is collected through the use of one's direct senses or the optical and/or audio enhancement of the senses.

**Human Trafficking:** The recruitment, transportation, transfer, harboring, or receipt of persons by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.

**Hypothesis (from criminal intelligence analysis):** An interim assumption regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proven or disproved by further investigation and analysis.

**Imagery:** The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the sensing media and sensing platform.

**Indicator Analysis:** A review of past criminal activity to determine whether certain actions or postures taken can reflect future criminal activity. It can result in the development of behavioral profiles or early warning systems in computerized environments.

**Indicator:** Generally defined and observable actions that, based on an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act.

**Inductive Logic:** The reasoning process of taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

**Inference Development:** The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based upon the use of inductive or deductive logic in the analysis of raw information related to the target.

**Informant:** An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself/herself from prosecution and/or provide the information in exchange for payment.

**Information Classification:** See Classified Information/Intelligence.

**Information Evaluation:** See Evaluation (of Information).

**Information Sharing Environment:** A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against territories, people, and interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications.

**Information Sharing System:** An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes, and/or events to enhance prevention and apprehension activities by law enforcement.

**Information System:** An organized means, whether manual or electronic, of collecting, processing, storing, and retrieving information on individual entities for purposes of record and reference.

**Information:** Pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

**Intelligence Analyst:** A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group.

**Intelligence Assessment:** A comprehensive report on an intelligence issue related to criminal or national security threats available to local, state, tribal, and federal law enforcement agencies.

**Intelligence Bulletins:** A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically sensitive but unclassified (SBU) and available for distribution to local, state, tribal, and federal law enforcement.

**Intelligence Community:** Those agencies of the U.S. government, including the military, that have the responsibility of preventing breaches to U.S. national security and responding to national security threats.

**Intelligence Cycle:** An organized process by which information is gathered, assessed, and distributed to fulfill the goals of the intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form.

**Intelligence Estimate:** The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to criminal offenders and terrorists and the order of probability of their adoption. Includes strategic projections on the economic, human,

and/or quantitative criminal impact of the crime or issue that is subject to analysis.

**Intelligence Function:** That activity within a law enforcement agency responsible for some aspect of law enforcement intelligence, whether collection, analysis, and/or dissemination.

**Intelligence Gap:** An unanswered question about a cyber, criminal, or national security issue or threat.

**Intelligence Information Reports (IIR):** Raw, unevaluated intelligence concerning “perishable” or time-limited information about criminal or national security issues. While the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to SBU information in the report under the tear line.

**Intelligence Mission:** The role that the intelligence function of a law enforcement agency fulfills in support of the overall mission of the agency; it specifies in general language what the function is intended to accomplish.

**Intelligence Mutual Aid Pact (IMAP):** A formal agreement between law enforcement agencies designed to expedite the process of sharing information in intelligence records.

**Intelligence Officer:** A law enforcement officer assigned to an agency’s intelligence function for purposes of investigation, liaison, or other intelligence-related activity that requires or benefits from having a sworn officer perform the activity.

**Intelligence Products:** Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution.

**Intelligence Records (Files):** Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts or are suspected of being or having been

involved in criminal activities with known or suspected crime figures.

**Intelligence Records Guidelines:** Derived from the federal regulation 28 CFR Part 23, these are guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

**Intelligence:** Information plus evaluation; the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities. Intelligence is information analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

**Intelligence-Led Policing:** The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses.

**International Criminal Police Organization (INTERPOL):** INTERPOL is a worldwide law enforcement organization established for mutual assistance in the prevention, detection, and deterrence of international crimes. It houses international police databases, provides secure international communications between member countries for the exchange of routine criminal investigative information, and is an information clearinghouse on international criminals/fugitives and stolen properties.

**Investigatory Value (of Information):** Intelligence or information is disseminated in the law enforcement community for surveillance, apprehension, or furtherance of an investigation.

**Key Resources:** Publicly or privately controlled resources essential to the minimal operations of the economy and government.

**Key Word in Context (KWIC):** An automated system that indexes selected key words which represent the evidence or information being stored.

**Law Enforcement Intelligence:** The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises

with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity, with the intent to pursue criminal prosecution, project crime trends, or support informed decision making by management. (Same as Criminal Intelligence).

**Law Enforcement Sensitive (LES):** SBU information specifically compiled for law enforcement purposes which, if not protected from unauthorized access, could reasonably be expected to (1) interfere with law enforcement proceedings, (2) deprive a person of a right to a fair trial or impartial adjudication, (3) constitute an unwarranted invasion of the personal privacy of others, (4) disclose the identity of a confidential source, (5) disclose investigative techniques and procedures, and/or (6) endanger the life or physical safety of an individual.

**Methods:** These are the methodologies (e.g., electronic surveillance or undercover operations) by which critical information is obtained and recorded.

**Microintelligence:** Intelligence activities focusing on current problems and crimes, either for case development or resource allocation.

**Money Laundering:** The practice of using multiple unlawful transactions of money and/or negotiable instruments gained through illegal activities with the intent of hiding the origin of the income, those who have been “paid” from the income, and/or the location of the unlawful income.

**National Central Bureau (NCB or USNCB):** The United States headquarters of INTERPOL is located in Washington, DC.

**National Criminal Intelligence Resource Center (NCIRC):** An Internet website that contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized resource information bank to access a multitude of criminal intelligence resources to help law enforcement agencies develop, implement, and retain a lawful and effective intelligence capacity.

**National Criminal Intelligence Sharing Plan (NCISP):** A formal intelligence sharing initiative, supported by the U.S. Department of Justice, Office of Justice Programs,

that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence information. The plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

**National Security Intelligence:** The collection and analysis of information concerned with the relationship and equilibrium of the United States with foreign powers, organizations, and persons with regard to political and economic factors, as well as the maintenance of the United States’ sovereign principles.

**Need to Know:** As a result of jurisdictional, organizational, or operational necessities, intelligence or sensitive information is disseminated to further an investigation.

**Network:** A structure of interconnecting components designed to communicate with each other and perform a function or functions as a unit in a specified manner.

**Open Communications (OPCOM):** The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

**Open Source Information (or Intelligence):** Individual data, records, reports, and assessments that may shed light on an investigatory target or event which do not require any legal process or any type of clandestine collection techniques for a law enforcement agency to obtain. Rather, it is obtained through means that meet copyright and commercial requirements of vendors, as well as being free of legal restrictions to access by anyone who seeks that information.

**Operational Analysis:** An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist.

**Operational Intelligence:** Information is evaluated and systematically organized on an active or potential target, such as groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature, wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information to develop a case for arrest or indictment.

**Outcome Evaluation:** The process of determining the value or amount of success in achieving a predetermined objective through defining the objective in some qualitative or quantitative measurable terms, identifying the proper criteria (or variables) to be used in measuring the success toward attaining the objective, determination and explanation of the degree of success, and recommendations for further program actions to attain the desired objectives/outcomes.

**Personally Identifiable Information:** Any information or data from which a reasonable person may identify a specific individual. When Personal Identifying Information is collected, civil rights protections and privacy standards must be afforded to the document or report that contains the information.

**Planning:** The preparation for future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations.

**Pointer System or Index:** A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

**Policy:** The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities which are directed toward the attainment of goals.

**Prediction:** The projection of future criminal actions or changes in the nature of crime trends or a criminal enterprise based on an analysis of information depicting historical trends from which a forecast is based.

**Privacy (Information):** The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process permits use of the personally identifiable information.

**Privacy (Personal):** The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his/her communications, associations, and transactions—will be adhered to by criminal justice agencies, with use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation.

**Privacy Act:** Legislation that allows an individual to review almost all federal files (and state files under the auspices of the respective state privacy acts) pertaining to him/her, places restrictions on the disclosure of personally identifiable information, specifies that there be no secret records systems on individuals, and compels the government to reveal its information sources.

**Proactive:** Taking action that is anticipatory to a problem or situation with the intent to eliminate or mitigate the effect of the incident.

**Procedural Due Process:** Mandates and guarantees of law that ensure that the procedures employed to deprive a person of life, liberty, or property, during the course of the criminal justice process, meet constitutional standards.

**Procedures:** A method of performing an operation or a manner of proceeding on a course of action. It differs from policy in that it directs action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal-oriented. However, policy establishes limits to action, while procedure directs responses within those limits.

**Profile/Criminal Profile:** An investigative technique used to identify and define the major personality and behavioral characteristics of the criminal offender based on an analysis of the crime(s) he or she has committed.

**Protocol (of Intelligence Collection):** Information collection procedures employed to obtain verbal and written information, actions of people, and physical evidence required for strategic and tactical intelligence analysis.

**Public Value (of Information):** Intelligence or information can be released to the public when there is a need to know and a right to know the information because of the value that may be derived from public dissemination, to (1) aid in locating targets/suspects and (2) for public safety purposes (i.e., hardening targets, taking precautions).

**Purging (Records):** The removal and/or destruction of records because they are deemed to be of no further value or further access to the records would serve no legitimate government interest.

**Qualitative (Methods):** Research methods that collect and analyze information that is described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information.

**Quantitative (Methods):** Research methods that collect and analyze information that can be counted or placed on a scale of measurement that can be statistically analyzed.

**Racketeer Influenced Corrupt Organization (RICO) or similar state statutes:** Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961–1968) provides civil and criminal penalties for persons who engage in a pattern of racketeering activity or collection of an unlawful debt that has a specified relationship to an enterprise that affects interstate commerce.

**Racketeering Activity:** State felonies involving murder, robbery, extortion, and several other serious offenses and more than 30 serious federal offenses, including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

**Reasonable Suspicion:** When information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

**Recommendations:** Suggestions for actions to be taken based on the findings of an analysis.

**Records (Intelligence):** See Intelligence Records (Files).

**Records System:** A group of records from which information is retrieved by reference to a name or other personal identifier, such as a social security number.

**Red Team:** A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities and to anticipate possible modes of attack.

**Regional Information Sharing Systems (RISS):** RISS is composed of six regional intelligence centers that provide secure communications, information sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to more than 9,500 local, state, tribal, and federal member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Canada, and England.

**Reliability:** Asks the question, “Is the source of the information consistent and dependable?”

**Reporting:** Depending on the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption.

**Requirements (Intelligence):** The types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations to enable law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

**Responsibility:** Responsibility reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

**Right to Know:** Based on having legal authority, one’s official position, legal mandates, or official agreements, allowing an individual to receive intelligence reports.

**Risk Management-Based Intelligence:** An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policymaking, especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability, or modality; can be quantitative if a proper database exists to measure likelihood and impact and calculate risk; can be qualitative and subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations.

**Rules:** A specific requirement or prohibition that is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

**SCI (Sensitive Compartmented Information):** Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems.

**SCIF (Sensitive Compartmented Information Facility):** An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

**Sealing (Records):** Records are stored by an agency but cannot be accessed, referenced, or used without a court order or statutory authority based on a showing of evidence that there is a legitimate government interest to review the sealed information.

**Secret Classification:** Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

**Security:** A series of procedures and measures that, when combined, provide protection of people from harm, information from improper disclosure or alteration, and assets from theft or damage. (Criminal Justice Commission, 1995.)

**Sensitive But Unclassified (SBU) Information:** Information that has not been classified by a federal law enforcement agency, which pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria only to those persons necessary to further the investigation or to prevent a crime or terrorist act.

**Signal Intelligence (SIGINT):** The interception of various radio frequency signals, microwave signals, satellite audio communications, nonimagery infrared and coherent light signals, and transmissions from surreptitiously placed audio microtransmitters in support of the communications intelligence activity.

**Source Reliability:** A scale reflecting the reliability of information sources, often shown as A–D or A–E. It ranges from factual source to reliability unknown.

**Sources:** From an intelligence perspective, these are persons (human intelligence, or HUMINT) who collect or possess critical information needed for intelligence analysis.

**Spatial Analysis:** The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity.

**Statistical System:** An organized means of collecting, processing, storing, and retrieving aggregate information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

**Strategic Intelligence:** An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

**Substantive Due Process:** Guarantees persons against arbitrary, unreasonable, or capricious laws and acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

**Surveillance:** The observation of activities, behaviors, and associations of a LAWINT target (individual or group), with the intent to gather incriminating information, or

“lead” information, which is used for the furtherance of a criminal investigation.

**Suspicious Activity Report:** A report and process wherein criminal indicators and behaviors that appear to have a criminal nexus are documented and processed through a law enforcement organization to determine whether a crime is being planned, is in the process of being committed, or has been committed.

**Tactical Intelligence:** Information regarding a specific criminal event of immediate use by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.

**Target Profile:** A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or a networked group of individuals.

**Target:** Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

**Targeting:** The identification of crimes, crime trends, and crime patterns that have discernable characteristics which make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

**Tear-Line Report:** A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the tear line can be released as SBU.

**Telemetry:** The collection and processing of information derived from noncommunications electromagnetic radiations emitting from sources such as radio navigation systems (e.g., transponders), radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

**Telephone Record (Toll)/Communications Analysis:** An assessment of telephone call activity associated with investigatory targets to include telephone numbers

called and/or received, the frequency of calls between numbers, the dates of calls, length of calls, and patterns of use.

**Third-Agency Rule:** An agreement whereby a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency.

**Threat Assessment:** An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal’s or terrorist’s opportunity, capability, and willingness to fulfill the threat and recommends ways to mitigate the threat.

**Threat Financing:** A term used to encompass various types of financing that support activities harmful to U.S. national security.

**Threat Inventory:** An information and intelligence-based survey within the region of a law enforcement agency to identify potential individuals or groups that pose a criminal or terrorist threat without a judgment of the kind of threat they pose. The inventory is simply used to determine their presence.

**Top Secret Classification:** Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

**Undercover Investigation:** Active infiltration of or an attempt to infiltrate a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or lead information that is used for the furtherance of a criminal investigation.

**Validity:** Asks the question, “Does the information actually represent what we believe it represents?”

**Variable:** Any characteristic on which individuals, groups, items, or incidents differ.

**Vet:** To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts

to ascertain the product's accuracy, consistency with philosophy, and/or feasibility before proceeding.

**Violent Criminal Apprehension Program (VICAP):** A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

**Vulnerability Assessment:** An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

**Warning:** Notification in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack.

# GLOSSARY OF TERMS EXPRESSLY RELATED TO TERRORISM AND CRIMINAL EXTREMISM

**Al-Qa’ida (AQ):** Al-Qa’ida is an Islamist extremist organization founded in 1988 by Usama bin Ladin and other Arab foreign fighters who fought against the Soviet Union in Afghanistan in the 1980s. It provides religious authority and strategic guidance to its followers and affiliated groups.

**Al-Qa’ida in the Arabian Peninsula (AQAP):** AQAP is an Islamist extremist organization based in Yemen. It is al-Qa’ida’s most active global affiliate.

**Al-Qa’ida in the Indian Subcontinent (AQIS):** AQIS is an Islamist extremist group that aims to fight the governments of Pakistan, India, Burma, and Bangladesh to establish an Islamic state.

**Al-Qa’ida in the Islamic Maghreb (AQIM):** AQIM was formed in 2007 and is al-Qa’ida’s North African affiliate, which aims to overthrow regional governments to institute an Islamic state. In March 2017, AQIM merged with several other regional groups to form Jama’at Nasr al-Islam Wal Muslim.

**Al-Qa’ida Network:** The al-Qa’ida Network is a decentralized organization that relies on social ties and local relationships to share resources among the affiliates.

**Al-Shabaab:** Al-Shabaab is an Islamist extremist organization founded in 2006 that seeks to establish an austere version of Islam in Somalia and also operates in Kenya, Ethiopia, Tanzania, and Uganda.

**Anarchist Extremists:** Anarchist extremists advocate violence in furtherance of movements such as anti-racism, anti-capitalism, anti-globalism, anti-fascism, and environmental extremism.

**Animal Rights Extremists:** Animal rights extremists believe all animals—human and nonhuman—have equal rights of life and liberty and are willing to inflict economic damage on individuals or groups to advance this ideology.

**Anti-Abortion Extremists:** Anti-abortion extremists are individuals or groups who believe that abortion is

unethical and that violence is justified against people and establishments providing abortion services.

**Anti-Government Extremists:** Anti-government extremists believe that the U.S. political system is illegitimate and that force is justified to bring about change. In addition, this includes individuals who do not necessarily question the legitimacy of government but express their opposition to specific policies, entities, officials, and political parties through threats or acts of violence. This category can include militia extremists and sovereign citizen extremists.

**Black Separatist Extremists:** Black separatist extremists are individuals or groups that seek to establish an independent nation for people of African descent through violence and other criminal activity.

**Boko Haram:** Boko Haram is an Islamist extremist organization based in northeastern Nigeria, which also conducts operations in Chad, Cameroon, and Niger.

**Domestic Terrorism:** Domestic terrorism is violence committed by individuals or groups associated primarily with U.S.-based movements, including anti-government, race-based, religious, and single-issue extremist ideologies.

**Environmental Extremists:** Environmental extremists view manmade threats to the environment as so severe that violence and property damage are justified to prevent further destruction.

**HAMAS:** HAMAS, an acronym for Harakat al-Muqawama al-Islamiyya, or the “Islamic Resistance Movement,” founded in 1987, is an offshoot of the Palestinian Muslim Brotherhood that aims to end the Israeli occupation of Palestinian territory and establish a Palestinian state.

**Hizballah:** Hizballah is an Islamist militant group based in Lebanon and allied with Iran.

**Homegrown Violent Extremists (HVEs):** HVEs are individuals inspired—as opposed to directed—by foreign terrorist organizations and radicalized in the countries in which they are born, raised, or reside.

**Hurras al-Din:** Hurras al-Din is an Islamist extremist organization based in Syria. It is officially recognized as the Syrian affiliate of al-Qa’ida.

**Incels:** Short for “involuntary celibates,” members of an online subculture who define themselves as unable to find a romantic or sexual partner despite desiring one. They have become increasingly violent and threatening to warrant classification as domestic extremists.

**ISIS:** ISIS, also referred to as the Islamic State of Iraq and Syria, the Islamic State of Iraq and the Levant, the Islamic State, or Daesh, is a Salafi-jihadist militant group that split from al-Qa’ida in 2014 and established its self-proclaimed “caliphate,” claiming authority over all Muslims.

**Lashkar-e-Tayyiba (LeT):** LeT is an Islamist extremist organization focused on attacking and expelling Indians from Kashmir, a northern state in India that borders Pakistan and is home to a Muslim-majority population.

**Militia Extremists:** Militia extremists view the federal government as a threat to the rights and freedoms of Americans. They judge armed resistance to be necessary to preserve these rights.

**Racially or Ethnically Motivated Extremism:** Threats involving the potentially unlawful use of force or violence, in furtherance of political and/or social agendas that are deemed to derive from bias—often related to race or ethnicity—held by the actor against others, including a given population group.

**Single-Issue Extremists:** Single-issue extremists participate in violence stemming from domestic, political, or economic issues. This category includes animal rights, environmental, and anti-abortion extremists.

**Sovereign Citizen Extremists:** Sovereign citizen extremists throughout the United States view federal, state, and local governments as illegitimate, justifying their violence and other criminal activity.

**Terrorism:** Terrorism is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

**White Supremacist Extremists:** White supremacist extremists believe in the inherent superiority of the white race. They seek to establish dominance over nonwhites through violence and other criminal activity.



# APPENDIX C

## INTELLIGENCE UNIT MANAGEMENT AUDIT

### AUDIT CRITERIA FOR THE LAW ENFORCEMENT INTELLIGENCE FUNCTION

VERSION 3.0<sup>1044</sup>

The intent of the checklist is for the intelligence function in a law enforcement agency to “take inventory” of its policies and practices from a management perspective. It provides guidance on relevant issues and trends in the management and performance of the law enforcement agency’s intelligence processes. A review of the questions and responses will indicate issues that may need to be examined more closely to determine whether the function and accountability of the intelligence function are meeting accepted levels of good practice. Not every question will apply to every agency, and there is no “right” or “wrong” outcome or score. The checklist is essentially a management pointer system for reviewing core issues in intelligence operations.

---

1044 Prepared by David L. Carter, Michigan State University, as part of an intelligence unit audit for compliance with a federal civil rights settlement. (Updated 2020.)

## SECTION A: MEETING NATIONAL STANDARDS

1. Does the police department subscribe to the tenets and standards of the *Global Justice Information Sharing Initiative*?  
 Yes  No
2. Does the police department subscribe to the standards of the *National Criminal Intelligence Sharing Plan, Version 2.0*?  
 Yes  No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the CICC *Unified Message Regarding Information Sharing*?  
 Yes  No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 40.2.3 *Criminal Intelligence Procedures*?  
 Yes  No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) *Model Policy on Criminal Intelligence*?  
 Yes  No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) *Criminal Intelligence File Guidelines*?  
 Yes  No
7. Does the police department subscribe to the IACP *Code of Ethics* or have an articulated code of ethics?  
 Yes  No
8. Does the police department subscribe to the IACP *Code of Conduct* or have an articulated code of conduct?  
 Yes  No
9. Does the police department have an articulated statement of values?  
 Yes  No
10. Does the police department adhere to the regulations of 28 CFR Part 23 for its criminal intelligence records system?  
 Yes  No
11. Does the police department operate a federally funded multijurisdictional criminal intelligence records system?  
 Yes  No
12. Does the police department subscribe to the tenets of the *Justice Information Privacy Guidelines*?  
 Yes  No
13. Does the police department subscribe to the tenets for information system security defined in the report titled *Applying Security Practices to Justice Information Sharing*?  
 Yes  No
14. Does the law enforcement agency subscribe to the philosophy of intelligence-led policing?  
 Yes  No
15. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious, or doctrinal purpose?  
 Yes  No

## SECTION B: MANAGEMENT ISSUES

1. Has a mission statement been written for the intelligence unit?  
 Yes  No
2. Is the purpose and role of the unit clearly articulated and related to the police department's mission statement?  
 Yes  No
3. Have priorities been established for the types of crimes the unit will address?  
 Yes  No
4. Is any written rationale provided for these priorities?  
 Yes  No
5. Are expected activities of the unit articulated?  
 Yes  No
6. Does the mission statement express ethical standards?  
 Yes  No
7. Does the mission statement express the importance of protecting community members' rights?  
 Yes  No

## B-1. POLICIES AND PROCEDURES

1. Are there written and officially articulated policies and procedures for management of the intelligence function?
  - Yes  No
2. Have intelligence policies been formed to minimize the discretion of information collectors?
  - Yes  No
  - If Yes, Describe:
3. Is there a policy and procedures on information collection?
  - Yes  No
  - If Yes, Describe:
4. Do policies and procedures clearly articulate the chain of command for the intelligence functions?
  - Yes  No
5. Do policies and procedures or personnel guidelines articulate clear job descriptions, authority, and responsibilities for all intelligence personnel?
  - Yes  No
6. Do policies and procedures or personnel guidelines articulate all factors on which all intelligence personnel are annually evaluated?
  - Yes  No
2. What is the source of the definitions?
  - NCISP  Federal agency
  - Mixed  N/A
3. Has the department articulated standards for protecting sensitive information in the intelligence unit?<sup>1046</sup>
  - Yes  No
4. How are those standards monitored and enforced?
  - Yes  No
5. Does the department have a system for assessing the *reliability of sources* that provide information that will be retained in the intelligence records system?
  - Yes  No
6. Are there standardized definitions of the reliability scale?
  - Yes  No
7. Does the department have a system for assessing the validity of the information that will be retained in the intelligence records system?
  - Yes  No
8. Are there standardized definitions of the validity scale?
  - Yes  No
9. Does the intelligence unit have operational definitions that can be applied to a person under investigation for a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a permanent file or a temporary file?
  - Yes  No

## B-2. MANAGEMENT OF INFORMATION:<sup>1045</sup> DEFINITIONAL STANDARDS

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?
  - Yes  No

1045 The questions in this audit outline the parameters of 28 CFR Part 23. This guideline specifies standards that are required for state and local law enforcement agencies operating a federally funded multijurisdictional criminal intelligence system. While the guideline does not apply to the criminal intelligence records systems of all state and local agencies, the law enforcement intelligence community considers it good practice for law enforcement agencies to adhere to the standards regardless of whether or not they are formally required to do so.

1034

Priority	Classification	Description	Release Authority
Highest Level	Restricted	Current corruption case; complex criminality; confidential informants, high-threat cases	Department executive or intelligence commander
Medium Level	Sensitive	Sensitive threat information may include the need for P/CRCL protections	Intelligence unit commander or supervisor
Lowest Level	Confidential	LE use but no need for high security of information	Intelligence unit personnel
Not Sensitive	Public Access	Information that may be released to public and media	Intelligence unit personnel

If Yes. . .

- a. Are the types of identifying information that should be placed in the file articulated?  
 Yes     No
- b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?  
 Yes     No
- c. Is there a procedure articulating the conditions wherein a temporary file may be created?  
 Yes     No
- d. Does the procedure specify a time limit that the temporary file can be kept?  
 Yes     No
- e. Are there an operational definition of “noncriminal identifying information” and procedures for recording and retaining this information?  
 Yes     No
- f. Are there clear procedures that *describe* the types of information that should *not* be entered into the intelligence records system?  
 Yes     No

### B-3. MANAGEMENT OF INFORMATION: SOURCE DOCUMENTS

1. Does the department have a written directive explaining the different types of source documents that will be entered into the intelligence records system?  
 Yes     No
2. What types of source documents are entered into the intelligence records system?<sup>1047</sup>  
Describe:
3. Does the police department have a written directive that the rationale for each source document entered into the intelligence records system must be articulated in a report or notation?  
 Yes     No

---

1047 For example, intelligence products generated by the police department; intelligence products generated by other agencies; offense reports; arrest reports; criminal history checks; output from consolidated databases; field interview reports, newspaper and open source materials, informant statements, etc.

### B-4. MANAGEMENT OF INFORMATION: DATA ENTRY

1. Who is responsible for entering information into the intelligence records system?  
Position/Classification:
2. Who supervises the information entry process?  
Position/Classification:
3. Who reviews the information entry process?  
Position/Classification:

### B-5. MANAGEMENT OF INFORMATION: ACCOUNTABILITY

1. Who is the custodian of the intelligence records system, ensuring that all regulations, law, policies, and procedures are being followed?  
Position/Classification:
2. Is there a person external to the intelligence unit who is designated to monitor the intelligence records system and related processes?  
 Yes     No  
If Yes, Position/Classification:
3. Does the department have written procedures for the retention of records in the intelligence records system?  
 Yes     No

### B-6. MANAGEMENT OF INFORMATION: RETENTION AND PURGING OF RECORDS

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?  
 Yes     No
2. Do the retention policy and procedure include written criteria for purging information?  
 Yes     No
3. How often does a review and purge process occur?  
Frequency:
4. What is the purge process?  
Describe:
5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy, and relevancy?  
 Yes     No
6. Does the purge process require destruction of the source document and removal of all references to

the document to be purged if the information is no longer appropriate for retention?

- Yes  No

7. What is the destruction process for purged hard-copy records?  
Describe:
8. After information has been purged from a computerized intelligence records system, are free space on the hard drive and/or specific purged files electronically “wiped”?  
 Yes  No
- a. Are backups wiped?  
 Yes  No
- b. What is the accountability system for purging backups?  
Describe:
9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?  
 Yes  No
10. What is the process for purging partial information from hard-copy source documents?  
Describe:
11. Who is responsible for ensuring compliance of the purge process?  
Position/Classification:

#### B-7. MANAGEMENT OF INFORMATION: PERSONAL/INDIVIDUALLY HELD RECORDS AND FILES

1. Is there an intelligence unit policy and procedure concerning the retention of individual notes and records that identify persons wherein criminality is suspected but that are not in either a temporary or a permanent file and are not entered into any formal records system or database?  
 Yes  No
- a. How is the possession of personal records monitored?  
Describe:
- b. How is the policy enforced?  
Describe:

#### B-8. MANAGEMENT OF INFORMATION: ACCESSING INTELLIGENCE RECORDS

1. Is access to the intelligence records limited?  
 Yes  No
2. If yes, who may access the intelligence records system?  
Describe:
3. What security controls exist for accessing computerized records?  
Describe:
4. Can the computerized records system be accessed through *remote* access?  
 Yes  No
- a. If so, what security controls exist for *remote access*?  
Describe:
5. How are physical records stored?  
Describe:
6. Who grants access privileges to intelligence records?  
Position/Classification:
7. Who has access to records?  
Position/Classification:
8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?  
 Yes  No
9. What *audit process* is in place for access to computerized records?  
Describe:
10. What audit process is in place for access to physical records?  
Describe:
11. How are physical records secured?  
Describe:
12. What process is in place to handle unauthorized access to intelligence physical records?  
Describe:
13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?  
Describe:

## B-9. PHYSICAL LOCATION OF THE INTELLIGENCE UNIT AND RECORDS

1. *Sufficiency:* Is the intelligence unit in a physical location that has sufficient space to perform all of its responsibilities?  
 Yes  No
2. *Security:* Is the intelligence unit in a physical location wherein the entire workspace may be completely secured?  
 Yes  No
  - a. Are there adequate secured storage cabinets (or a vault) for (1) documents deemed sensitive by the intelligence unit and (2) sensitive records storage *within* the intelligence unit's physical location?  
 Yes  No
3. *Convenience:* Is the intelligence unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?  
 Yes  No

## B-10. TANGENTIAL POLICY ISSUES: CONFIDENTIAL INFORMANTS AND UNDERCOVER OPERATIONS<sup>1048</sup>

1. Is there a formally articulated policy and procedure for managing confidential informants?  
 Yes  No
  - a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?  
 Yes  No
  - b. Are informant files secured separately from intelligence files?  
 Yes  No

---

1048 The use of confidential informants and undercover operations varies among law enforcement agencies. In some cases, these resources may be a functional part of the intelligence unit, but in many agencies, they are relied on by the unit for information collection. Understanding the management and control of these activities can be important for the intelligence commander, for they can reflect the validity, reliability, and constitutional admissibility of the information collected.

2. Is there a formally articulated policy and procedures concerning undercover operations that apply to information collectors assigned to the intelligence unit?  
 Yes  No
3. Does the police department have a policy on alcohol consumption for officers working undercover?  
 Yes  No
  - a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?  
 Yes  No
4. Does the police department have a "narcotics simulation" policy and training for undercover officers?  
 Yes  No
5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?  
 Yes  No
6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?  
 Yes  No
7. With respect to undercover operating funds:
  - a. Is there a one-tier or two-tier process to approve use of the funds?  
 Yes  No
  - b. Is a written report required to document expenditure of the funds?  
 Yes  No
  - c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?  
 Days  No set time
  - d. Is there a regular external audit of undercover funds?  
 Yes (how often?)  No

## SECTION C: PERSONNEL

1. Is a position classification plan in place that provides a clear job description for each position in the unit?  
 Yes  No
2. Is a position classification plan in place that articulates knowledge, skills, and abilities (KSAs) for each position?  
 Yes  No
3. Are there sufficient *hierarchical* staff members (managers/supervisors) assigned to the unit to effectively perform supervisory responsibilities?  
 Yes  No
4. Are there sufficient *functional* staff members (analysts and/or investigators) to effectively fulfill defined unit responsibilities?  
 Yes  No
5. Are there sufficient support staff members (secretaries, clerks) to effectively support the unit's activities?  
 Yes  No
6. Does the screening process for nonsworn employees of the intelligence unit require:
  - a. Fingerprint check  
 Yes  No
  - b. Background investigation  
 Yes  No
7. If the intelligence unit has non-PD employees assigned to it—e.g., National Guard analysts, personnel from the state or local law enforcement agencies—would there be a screening process for those persons?  
 Yes  No  
If Yes, Describe:
8. Are all personnel assigned to the intelligence function required to sign a nondisclosure agreement?  
 Yes  No

### C-1. TRAINING

1. What types of training do pre-service and newly assigned personnel receive?  
 None  Some—describe:

- a. Are sworn employees newly assigned to the intelligence unit required to attend 28 CFR Part 23 training?  
 Yes  No
  - b. Are newly hired or assigned nonsworn employees required to attend 28 CFR Part 23 training?  
 Yes  No
2. What types of training do in-service personnel receive?<sup>1049</sup>  
 None  Some—describe:
  3. Have members of the intelligence unit attended any of the following federal government intelligence training programs, which are open to state and local law enforcement officers?
    - a. DEA Intelligence Training  
 Yes  No
    - b. FBI Intelligence Training  
 Yes  No
    - c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course  
 Yes  No
    - d. FEMA Intelligence Training  
 Yes  No
    - e. National White Collar Crime Center Intelligence Training  
 Yes  No
    - f. Regional Counterdrug Training Academy Intelligence Operations Course  
 Yes  No
    - g. Other intelligence training  
 Yes  No  
Specify:
  4. Are intelligence analysts required to attend the LEIU/IALEIA Foundations of Intelligence Analysis Training (FIAT)?  
 Yes  No
  5. Are intelligence analysts required to meet the Global/CICC Law Enforcement Analyst Certification Standards?  
 Yes  No

1049 Nota bene: Training should go beyond the basics and include updates of law, current crime issues and trends; new technologies, new resources, etc.

6. Is there a career path for nonsworn intelligence analysts, such as use of the *CICC Analyst Professional Development Roadmap, Version 2.0*?  
 Yes     No

### C-2. SUPERVISION

1. Does supervision effectively monitor adherence to written procedures?  
 Yes     No
2. Does supervision effectively monitor adherence to guidelines adopted by the department?  
 Yes     No
3. Are performance evaluations tied directly to the job descriptions?<sup>1050</sup>  
 Yes     No
4. Does supervision effectively monitor the performance of required duties (Including the *quality* of performance)?  
 Yes     No
5. Is supervision effectively monitoring personnel to ensure that civil rights allegations cannot be made with respect to negligence in. . . .
  - a. Failure to train  
 Yes     No
  - b. Hiring  
 Yes     No
  - c. Failure to supervise  
 Yes     No
  - d. Assignment  
 Yes     No
  - e. Failure to direct  
 Yes     No
  - f. Failure to discipline  
 Yes     No
  - g. Entrustment  
 Yes     No
6. Is there effective supervision of the intelligence unit throughout the chain of command external to the intelligence unit?  
 Yes     No

<sup>1050</sup> Intelligence unit staff responsibilities are sufficiently different from other police positions that standard performance evaluations typically do not apply.

## SECTION D: FISCAL MANAGEMENT

1. Is the budget sufficient to fulfill the stated mission?  
 Yes     No
2. Does the intelligence commander have input into the budget planning process?  
 Yes     No
3. Is there overreliance on “soft money” to operate the unit?<sup>1051</sup>  
 Yes     No
4. Are equipment and personnel line items assigned directly to the intelligence unit?<sup>1052</sup>  
 Yes     No
5. Is there an established process for reliably monitoring credit cards assigned to personnel?  
 Yes     No     NA
6. Is there an established process for reliably monitoring smartphones assigned to personnel?  
 Yes     No     NA
7. Is there an established process for reliably monitoring tablets or laptop computers assigned to personnel?  
 Yes     No     NA

## SECTION E: UNIT EVALUATION

1. As a whole, is the unit effective with respect to:
  - a. Providing information to prevent crime?  
 Yes     No
  - b. Providing information to apprehend criminals?  
 Yes     No
  - c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?  
 Yes     No
  - d. Identifying threats?  
 Yes     No
  - e. Preventing or mitigating threats?  
 Yes     No

<sup>1051</sup> For example, grants, cooperative agreements, contracts with other agencies, etc.

<sup>1052</sup> Nota bene: If such items are not specifically assigned, then they can be withdrawn more easily.

2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence unit's productivity as an organizational entity?
  - a. Number and type of analytic products developed
    - Yes  No  NA
  - b. Number and type of analytic products that led to arrest
    - Yes  No  NA
  - c. Assets seized from illegal activities wherein intelligence contributed to an arrest and/or seizure
    - Yes  No  NA
  - d. Number and types of strategic intelligence products delivered to the command staff
    - Yes  No  NA
  - e. Number of intelligence sharing meetings attended by unit staff
    - Yes  No  NA
  - f. Number of briefings provided by the intelligence staff
    - Yes  No  NA
  - g. Total number of queries into the intelligence database
    - Yes  No  NA
  - h. Number of permanent files opened
    - Yes  No  NA
  - i. Number of temporary files investigated
    - Yes  No  NA
  - j. Number of requests for information to the unit from outside agencies
    - Yes  No  NA
3. Are the products produced by the intelligence unit
  - a. In a consistent format?
    - Yes  No
  - b. Easily consumed and used (i.e., understandable and actionable)?
    - Yes  No
  - c. Filled with timely information and disseminated in a timely manner?
    - Yes  No
  - d. Provided with substantive contact to aid in preventing or controlling crime?
    - Yes  No

4. Given the confidential nature of the information contained in the intelligence unit, is there a policy and procedures for a city, county, state, or federal fiscal or program auditor who seeks to audit the intelligence unit?
  - Yes  No

If Yes, Describe:

## SECTION F: COLLECTION

1. Is there an articulated collection plan for the intelligence unit?
  - Yes  No

If Yes, Describe:

  - a. How often and when is the plan updated?
    - Describe:
2. Have the following activities been performed by the intelligence unit?
  - a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists.
    - Yes  No
  - b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region.
    - Yes  No
  - c. A target or criminal commodity analysis of the region.
    - Yes  No
  - d. A target or criminal commodity vulnerability assessment in the region.
    - Yes  No
3. For each identified threat, have intelligence requirements been articulated?
  - Yes  No
  - a. Yes, describe the methods of collection that will be used to fulfill those intelligence requirements.

## SECTION G: TECHNOLOGY AND NETWORKING

1. Are any members of the intelligence unit subscribed members of the FBI's Law Enforcement Enterprise Portal (LEEP)?
  - Yes-All  Yes-Some  No

2. Are any members of the intelligence unit subscribed members of the secure Regional Information Sharing Systems (RISS) RISSNET network?
  - Yes-All     Yes-Some     No
 If yes, are the RISS databases (e.g., RISSGang) regularly used?
  - Yes     No
3. Is the police department a member of RISS?
  - Yes     No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted by the primary state fusion center are received by intelligence personnel?
  - Yes     No
5. Are you connected to any state-operated intelligence or information networks?
  - Yes     No
 If Yes, Describe:
6. Are you connected to any regional intelligence or information networks (including fusion centers and HIDTA)?
  - Yes     No
 If Yes, Describe:
7. Does the intelligence unit have access to and use the recognized deconfliction systems?
  - Yes     No
8. Is there a formal approval process for entering into a memorandum of understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?
  - Yes     No
 If Yes, Describe the Process:
 

Who must approve the MOU?
9. Is there sufficient security in place for externally networked computers?
  - Yes     No
 How often are network and computer security precautions reviewed? Specify:

10. Is there sufficient security in place for department-issued smartphones?
  - Yes     No
 How often are smartphone security precautions reviewed? Specify:

## SECTION H: LEGAL ISSUES

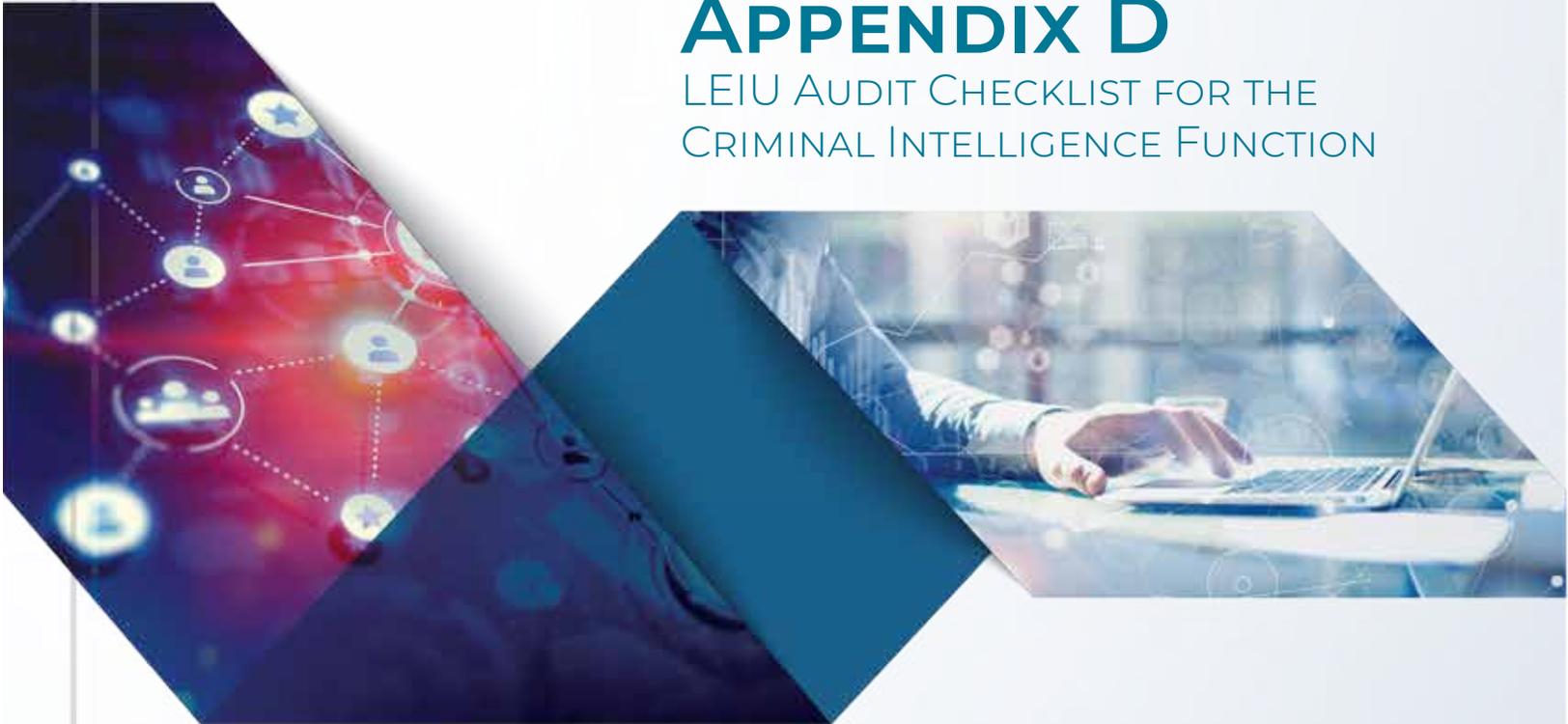
1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?
  - Yes     No
2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the intelligence unit?
  - Yes     No
3. Is there a designated person the police department contacts in response to a subpoena for a file in the intelligence records system?
  - Yes     No
4. Does the intelligence unit commander have a legal resource for advice to help protect intelligence records from objectionable access?
  - Yes     No
5. Does the intelligence unit commander have a legal resource for advice on matters related to criminal procedure and civil rights?
  - Yes     No
6. Does the intelligence unit commander have a legal resource for advice on matters related to questions of civil liability as related to all aspects of the intelligence function?
  - Yes     No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
  - Yes     No
8. Is there a designated person in the police department who provides updated advice to the intelligence unit on issues related to protecting the privacy, civil rights, and civil liberties of community members?
  - Yes     No

Once the audit is completed, review the results.

- ◆ Are there responses of “No” that need to be addressed?
- ◆ Are you able to clearly articulate a response to the questions that ask the respondent to “specify” or “describe” as part of the response?
- ◆ Share the results with members of the intelligence unit and the chain of command and seek their candid feedback.

Remember, the audit is not meant to be a critical exercise, but a self-awareness exercise to provide direction on how the intelligence function can be strengthened.



The graphic consists of several overlapping hexagonal shapes. The leftmost hexagon is dark blue and contains a network of glowing nodes and lines, with some nodes having icons like a star and a person. The middle hexagon is a solid dark blue. The rightmost hexagon is a lighter blue and shows a person's hands typing on a laptop keyboard. The background is a light blue gradient.

# APPENDIX D

## LEIU AUDIT CHECKLIST FOR THE CRIMINAL INTELLIGENCE FUNCTION

The Law Enforcement Intelligence Unit (LEIU) is the oldest professional organization for law enforcement intelligence. The organization has established a solid reputation for professionalism, objectivity, and promoting intelligence activities that protect the constitutional rights and privacy of all Americans. This checklist was prepared to aid in the professional management of a state, local, and tribal law enforcement intelligence function. Additional materials, including a description of how the checklist was prepared, are available in the original *LEIU Audit Checklist* document at [https://it.ojp.gov/documents/LEIU\\_audit\\_checklist.pdf](https://it.ojp.gov/documents/LEIU_audit_checklist.pdf).

## INTRODUCTION

The purpose of this checklist is to provide law enforcement executives and senior- to mid-level law enforcement managers with a tool for conducting an audit or evaluation of their agencies' criminal intelligence functions. Specifically, this audit tool can help an agency ensure that it is carrying out the criminal intelligence function in accordance with applicable laws, regulations, and guidelines. The principles found in the checklist apply most directly to municipal, county, and state law enforcement agencies. Several introductory comments are appropriate.

**This checklist should be applied only to criminal intelligence files—not to other types of law enforcement records.** Some law enforcement officials fail to make the distinction between criminal intelligence files and other types of law enforcement records (e.g., investigative files). In the law enforcement context, however, these differences are important and must be recognized.

“Investigation” generally refers to the systematic examination of facts to determine whether a crime has occurred and, if so, to develop a case for prosecution. Generally, the term “investigative files” refers to information collected in the course of an investigation where there are reasonable grounds to suspect that a person has committed specific criminal acts.

On the other hand, the criminal intelligence process is an ongoing activity and is not necessarily triggered by the investigation of any specific offense. While investigation tends to be reactive in nature, criminal intelligence is proactive and used to identify and understand criminals operating in a particular area. Once individuals or groups are identified and their habits known, law enforcement authorities may begin to assess current trends in crime and to forecast, and possibly prevent, future criminal activities. Intelligence provides the knowledge on which to base decisions and select appropriate targets (subjects, criminal groups, or businesses), for investigations. Although criminal intelligence may be used to assist in investigations, surveillance operations, and prosecution of cases, it also provides law enforcement agencies with the ability to effectively manage resources, budget, and meet their responsibility to forecast community threats to prevent crime.

Criminal intelligence consists of pieces of raw information, which, when collected, evaluated, collated, and analyzed, form meaningful and useful judgments that are both accurate and timely. Taking this raw information and turning it into intelligence can be described as a sequential process with multiple distinct phases. Following appropriate planning, the first phase is collection, which is obtaining raw information from various sources. Evaluation then occurs, which is determining the reliability of the source and the validity of the information. The third phase is collation and involves indexing, cross-referencing, and filing of information. The fourth phase is analysis, which identifies trends, future developments, and case building. The fifth phase is dissemination, which involves the actual dispensing of the intelligence information. A unit that does not complete each of these phases is not a criminal intelligence unit.

This checklist is designed to be utilized by senior law enforcement managers who are not directly involved in the day-to-day operations of the agency's criminal intelligence function. This helps ensure that the audit is objective and accurately identifies the function's strengths and weaknesses. However, the checklist can also be used as a self-assessment tool by personnel who are directly involved with the agency's criminal intelligence function. This type of effort will help determine whether the unit is acting in accordance with the standard practices and procedures established by LEIU.

Historically, criminal intelligence units have experienced problems in the area of unit operating procedures, collection, collation, and dissemination; therefore, this checklist focuses on these four areas.

ITEM	QUESTION	
1.	Does the criminal intelligence unit have a mission statement? If no, go to question 10.	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.	Does the mission statement contain a concise, well-defined mandate describing the criminal intelligence unit?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.	Does the mission statement describe the use of the intelligence process in support of the criminal intelligence unit?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	Is the statement focused toward criminal predicate?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	Does the statement indicate that the criminal intelligence unit will provide the chief executive with criminal information and resulting analysis to counter and control criminal activities?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.	Does the statement identify the criminal intelligence unit's expected results?	<input type="checkbox"/> Yes <input type="checkbox"/> No
7.	Is the criminal intelligence unit staying within its mission?	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.	Is the criminal intelligence unit assuming work beyond the authorized crime areas?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.	Is the statement reviewed on a periodic basis to ensure that it is meeting the needs of the agency/organization?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.	Does the criminal intelligence unit have policy and procedure guidelines? If no, go to question 18.	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.	Do the guidelines describe the criminal intelligence unit's operations?	<input type="checkbox"/> Yes <input type="checkbox"/> No
12.	Do the guidelines provide the criminal intelligence unit's mission statement?	<input type="checkbox"/> Yes <input type="checkbox"/> No
13.	Do the guidelines detail the criminal intelligence unit's methods of operation?	<input type="checkbox"/> Yes <input type="checkbox"/> No
14.	Do the guidelines outline the criminal intelligence unit's file guidelines?	<input type="checkbox"/> Yes <input type="checkbox"/> No
15.	Do the guidelines establish the criminal intelligence unit's security procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No
16.	Do the guidelines describe personnel responsibilities and assigned duties?	<input type="checkbox"/> Yes <input type="checkbox"/> No
17.	Have the guidelines been provided to personnel?	<input type="checkbox"/> Yes <input type="checkbox"/> No
18.	Are periodic security updates conducted for intelligence personnel on a regular basis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.	Is the criminal intelligence unit located in a physically secure location?	<input type="checkbox"/> Yes <input type="checkbox"/> No
20.	Are unauthorized persons prevented from accessing the criminal intelligence unit's location?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21.	Is access terminated when personnel are on leave or cease to work in an intelligence capacity?	<input type="checkbox"/> Yes <input type="checkbox"/> No
22.	Are there guidelines for transferring material to or from digital media?	<input type="checkbox"/> Yes <input type="checkbox"/> No
23.	Does the criminal intelligence unit have access to the chief executive?	<input type="checkbox"/> Yes <input type="checkbox"/> No
24.	Does the unit provide the chief executive with recommendations?	<input type="checkbox"/> Yes <input type="checkbox"/> No
25.	Does the unit provide the agency with valuable strategic and tactical products?	<input type="checkbox"/> Yes <input type="checkbox"/> No
26.	Do personnel receive appropriate training?	<input type="checkbox"/> Yes <input type="checkbox"/> No
27.	Are there clear lines of responsibility and accountability for the functions of the intelligence unit?	<input type="checkbox"/> Yes <input type="checkbox"/> No
28.	Is a regular security risk review of the intelligence unit and its systems conducted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
29.	Are procedures in place governing the criminal intelligence unit's use of special funds?	<input type="checkbox"/> Yes <input type="checkbox"/> No
30.	Is the criminal intelligence unit's mission achievable with the number of assigned staff members?	<input type="checkbox"/> Yes <input type="checkbox"/> No

ITEM	COLLECTION	
31.	Does a collection effort begin with the development of a written plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No
32.	Does the collection plan include a set of information requirements that specifies what data is needed by the agency or investigator(s)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
33.	Does the collection plan comply with applicable local, state, and federal statutes and case law?	<input type="checkbox"/> Yes <input type="checkbox"/> No
34.	Is the collection plan focused on identifying the nature and extent of criminal activity?	<input type="checkbox"/> Yes <input type="checkbox"/> No
35.	Does the collection plan utilize all known available sources?	<input type="checkbox"/> Yes <input type="checkbox"/> No
36.	Are the plan's objectives and requirements communicated to criminal intelligence unit staff?	<input type="checkbox"/> Yes <input type="checkbox"/> No
37.	Has the criminal intelligence function encouraged the development of a close working relationship between analysts and investigators?	<input type="checkbox"/> Yes <input type="checkbox"/> No
38.	Have those assigned to the criminal intelligence function received training in the right to privacy?	<input type="checkbox"/> Yes <input type="checkbox"/> No
39.	Does your state have laws that address the collection of criminal intelligence data?	<input type="checkbox"/> Yes <input type="checkbox"/> No
40.	Do the methods used by information collectors fall within legal guidelines?	<input type="checkbox"/> Yes <input type="checkbox"/> No
41.	Does your agency have informant guidelines in place? If not, go to question 44.	<input type="checkbox"/> Yes <input type="checkbox"/> No
42.	Do these guidelines address informant control and management?	<input type="checkbox"/> Yes <input type="checkbox"/> No
43.	Do these guidelines address the maintenance of informant files?	<input type="checkbox"/> Yes <input type="checkbox"/> No
ITEM	COLLATION	
44.	Does the unit have criminal intelligence file guidelines?	<input type="checkbox"/> Yes <input type="checkbox"/> No
45.	Is the criminal intelligence unit operating within the guidelines?	<input type="checkbox"/> Yes <input type="checkbox"/> No
46.	Are files kept ONLY on individuals who are suspected of being involved in actual or attempted criminal acts or suspected of being involved in criminal activities with known or suspected crime figures?	<input type="checkbox"/> Yes <input type="checkbox"/> No
47.	Are files kept ONLY on organizations, businesses, and groups that are suspected of being involved in actual or attempted criminal acts or suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures?	<input type="checkbox"/> Yes <input type="checkbox"/> No
48.	Do files include ONLY information that relates to a criminal predicate?	<input type="checkbox"/> Yes <input type="checkbox"/> No
49.	Do the guidelines clearly delineate criteria for determining whether information should be entered and retained in the files?	<input type="checkbox"/> Yes <input type="checkbox"/> No
50.	Is the information stored in criminal intelligence files evaluated according to source reliability and content validity before it is included in a criminal intelligence file?	<input type="checkbox"/> Yes <input type="checkbox"/> No
51.	Is there a clearly articulated system for assessing source reliability and content validity?	<input type="checkbox"/> Yes <input type="checkbox"/> No
52.	Is a distinction made among permanent, temporary, and working files, along with appropriate retention periods?	<input type="checkbox"/> Yes <input type="checkbox"/> No
53.	Is the information stored in criminal intelligence files classified to protect sources, investigators, and the individual's right to privacy?	<input type="checkbox"/> Yes <input type="checkbox"/> No
54.	Are files clearly marked with appropriate classification?	<input type="checkbox"/> Yes <input type="checkbox"/> No
55.	Is information maintained in the criminal intelligence file reviewed for reclassification or purge on a periodic basis to ensure that it is current and accurate, safeguards an individual's right to privacy, and is classified at an appropriate security level?	<input type="checkbox"/> Yes <input type="checkbox"/> No
56.	Is information maintained in the criminal intelligence file reviewed on a periodic basis for utility, timeliness, appropriateness, accuracy, and completeness?	<input type="checkbox"/> Yes <input type="checkbox"/> No

ITEM	QUESTION	
57.	Do the criminal intelligence unit's purge policies comply with local, and/or state law regarding records retention?	<input type="checkbox"/> Yes <input type="checkbox"/> No
58.	Are there specific staff members who are responsible for purging files?	<input type="checkbox"/> Yes <input type="checkbox"/> No
59.	Are procedures in place to govern the storage, handling, and security of hard-copy source material?	<input type="checkbox"/> Yes <input type="checkbox"/> No
60.	Does the criminal intelligence unit retain hard copies of source documents? If no, go to question 63.	<input type="checkbox"/> Yes <input type="checkbox"/> No
61.	Are these documents stored in a safe and secure location?	<input type="checkbox"/> Yes <input type="checkbox"/> No
62.	Is access to these documents restricted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
63.	Are procedures in place to govern the storage, handling, and security of source material in an electronic database?	<input type="checkbox"/> Yes <input type="checkbox"/> No
64.	Is access to the file database restricted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
65.	Are specific employees responsible for controlling automated access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
66.	Are automated access audits conducted periodically?	<input type="checkbox"/> Yes <input type="checkbox"/> No
67.	Is a record of audits maintained?	<input type="checkbox"/> Yes <input type="checkbox"/> No
68.	Is automated access immediately deleted when personnel leave or transfer?	<input type="checkbox"/> Yes <input type="checkbox"/> No
69.	Are files adequately safeguarded through backup and recovery routines and off-site storage of critical files, programs, and systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No
70.	Is the system isolated from other networks or protected by a firewall to restrict unauthorized access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
71.	Are files (either hard or electronic copy) indexed in an organized fashion?	<input type="checkbox"/> Yes <input type="checkbox"/> No
72.	Is a file locator system in place?	<input type="checkbox"/> Yes <input type="checkbox"/> No
73.	Are particular employees responsible for overseeing the criminal intelligence file system so that it is operating within the guidelines of all applicable laws?	<input type="checkbox"/> Yes <input type="checkbox"/> No
74.	Are purged documents destroyed in a secure and appropriate manner according to all applicable laws?	<input type="checkbox"/> Yes <input type="checkbox"/> No
75.	Is information regarding political, religious, or social views of an individual or group prohibited from inclusion in a criminal intelligence file unless it directly relates to criminal conduct or activity?	<input type="checkbox"/> Yes <input type="checkbox"/> No
ITEM	DISSEMINATION	
76.	Are procedures in place for responding to requests for information?	<input type="checkbox"/> Yes <input type="checkbox"/> No
77.	Are records kept of requests for information and responses? If not, go to question 79.	<input type="checkbox"/> Yes <input type="checkbox"/> No
78.	Are these records audited periodically?	<input type="checkbox"/> Yes <input type="checkbox"/> No
79.	Are there procedures in place governing the methods of enveloping, dispatching, and recording the dissemination of law enforcement sensitive material?	<input type="checkbox"/> Yes <input type="checkbox"/> No
80.	Is criminal intelligence information released only to those who have demonstrated a right to know and a need to know?	<input type="checkbox"/> Yes <input type="checkbox"/> No
81.	Is there an audit trail to determine who has accessed criminal intelligence files?	<input type="checkbox"/> Yes <input type="checkbox"/> No
82.	Has the criminal intelligence unit established a policy prohibiting third-party dissemination?	<input type="checkbox"/> Yes <input type="checkbox"/> No
83.	Has the agency identified legal resources that are familiar with criminal intelligence issues and procedures and can adequately represent the agency in legal matters?	<input type="checkbox"/> Yes <input type="checkbox"/> No

## REFERENCES

*Audit Factors for the Law Enforcement Intelligence Function.* Prepared by David L. Carter (2004).

*Criminal Intelligence File Guidelines.* Prepared by LEIU (Revised in March 2002).

*Criminal Intelligence Standards and Guidelines.* Prepared by the California Peace Officers' Association (July 2003).

*Evaluation Checklists for Intelligence Units.* Written by Paul R. Roger.

*Turn-Key Intelligence: Unlocking Your Agency's Intelligence Capabilities.* Produced by IALEIA, LEIU, and NW3C.

*Gang File Audit Checklist.* Prepared by the California Bureau of Investigation, Division of Law Enforcement, California Department of Justice (May 2001).

*Guidelines for the Criminal Intelligence Function.* Prepared by Dick Wright, Simi Valley Police Department (Revised in September 1998).

*Intelligence 2000: Revising the Basic Elements; A Guide for Intelligence Professionals.* Prepared by LEIU and IALEIA (2000). Managing Editor Marilyn B. Peterson, Editors Bob Morehouse and Dick Wright.

*National Criminal Intelligence Sharing Plan 2003* (October). Sponsored by the Office of Justice Programs, U.S. Department of Justice, Award No. 2000-LD-BX-0003.



# APPENDIX E

## BIOGRAPHY OF DR. DAVID L. CARTER



### DAVID L. CARTER, PH.D.

PROFESSOR, SCHOOL OF CRIMINAL JUSTICE, MICHIGAN STATE UNIVERSITY  
DIRECTOR OF RESEARCH, INSTITUTE FOR INTERGOVERNMENTAL RESEARCH

David L. Carter (Ph.D., Sam Houston State University; LL.D. [Hon], University of Central Missouri) is a professor in the School of Criminal Justice and the Director of the Intelligence Program at Michigan State University. His expertise is in the areas of policing issues, violent crime control, law enforcement intelligence, and homicide investigation. A former Kansas City, Missouri, police officer, Dr. Carter was chair of the Department of Criminal Justice at the University of Texas Rio Grande Valley nine years prior to his appointment at Michigan State in 1985. He has served as a trainer, a consultant, and an advisor to many law enforcement agencies throughout the United States, Europe, Asia, and Australia on various law enforcement issues. In addition, he has presented training sessions at the Federal Bureau of Investigation (FBI) National Academy, the FBI Law Enforcement Executive Development Seminar (LEEDS), and the International Law Enforcement Academy in Budapest, Hungary, as well as the United Nations Asia and Far East Institute (UNAFEI) in Tokyo. He has presented special programs for the Royal Thai Police, the Hong Kong Police, the British Police Staff College at Bramshill, several British police constabularies, and police “command colleges” of several

states. He also served at the FBI Academy's Behavioral Sciences Unit during the first academic faculty exchange with the FBI. Dr. Carter has been an instructor in the Bureau of Justice Assistance's State and Local Anti-Terrorism Training (SLATT) Program; wrote the Office of Community Oriented Policing Services- and U.S. Department of Homeland Security (DHS)-funded publication, *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement*; served as project director for three multimillion-dollar DHS-funded national intelligence training programs; and served as co-project director of a National Institute of Justice grant to do a nationwide study on the best practices and efficacy of law enforcement intelligence initiatives. Dr. Carter served as team leader for the U.S. Department of Justice's (DOJ) assessment of the police response in Ferguson, Missouri. He also served as team leader of two DOJ assessments of the homicide units at the New Orleans, Louisiana, Police Department and the Puerto Rico Police Department. He is an academic fellow of the Foundation for Defending Democracies, wherein he studied terrorism in Israel. He is the author or co-author of five books and numerous articles and monographs on policing issues and is a member of the editorial boards of various professional publications. He has received many professional awards, including the University Distinguished Alumni Award from Sam Houston State University and an honorary doctorate of laws from the University of Central Missouri, as well as professional awards from the Academy of Criminal Justice Sciences.

\*\*\*

