Fusion Center Guidelines

Developing and Sharing Information and Intelligence in a New Era

Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels

Law Enforcement Intelligence, Public Safety, and the Private Sector

Global Justice
Information
Sharing
Initiative

Fusion Center Guidelines

Developing and Sharing
Information and Intelligence
in a New Era

Guidelines for Establishing and
Operating Fusion Centers at the
Local, State, and Federal Levels

Law Enforcement Intelligence,
Public Safety, and the
Private Sector

Foreword

The U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) collaborated in the development of these fusion center guidelines. The intent of the partnership is to provide a consistent, unified message and to provide a comprehensive set of guidelines for developing and operating a fusion center within a state or region.

Members of DOJ's Global Justice Information Sharing Initiative (Global) and DHS's Homeland Security Advisory Council (HSAC) supported this project, which involved numerous law enforcement experts and practitioners from local, state, tribal, and federal agencies, as well as representatives of public safety and private sector entities across the country. Their collective knowledge, insight, and willingness to participate resulted in an outstanding product. Strong leadership for the project's focus groups was provided by Peter Modafferi, chair of the Law Enforcement Intelligence Focus Group; John Cohen, chair of the Public Safety Focus Group; and Kenneth Bouche, chair of the Private Sector Focus Group.

This effort would not have been possible without the support and guidance of key individuals. A special thank you is given to the following individuals for their leadership and commitment to this initiative: Regina B. Schofield, Assistant Attorney General, Office of Justice Programs (OJP); Domingo S. Herraiz, Director, Bureau of Justice Assistance (BJA), OJP; J. Patrick McCreary, Associate Deputy Director of National Policy, BJA; Tim Beres, Director, Preparedness Programs Division, Office for Domestic Preparedness, DHS; Dave Brannegan, Program Manager, Office of State and Local Government Coordination and Preparedness, DHS; Daniel Ostergaard, Executive Director, HSAC, DHS; Michael Miron, Jeff Gaynor, and Candace Stoltz, Directors, Intelligence and Information Sharing Working Groups, HSAC; DHS; and Mitt Romney, chairman, Intelligence and Information Sharing Working Group, HSAC, DHS.

The Role of Leadership

In developing our country's response to the threat of terrorism, law enforcement, public safety, and private sector leaders have recognized the need to improve the sharing of information and intelligence across agency borders. Every official involved in information and intelligence sharing has a stake in this initiative. Leaders must move forward with a new paradigm on the exchange of information and intelligence, one that includes the integration of law enforcement, public safety, and the private sector.

Law enforcement, public safety, and private sector leaders are encouraged to embrace the guidelines in this report when establishing a fusion center or participating in one. Information and intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center uses a common set of guidelines. It is the intent of this document to provide guidelines that help ensure fusion centers are established and operated effectively and efficiently in a manner that protects the privacy and civil liberties of citizens. The complete support of public safety leaders at all levels is critical to the successful implementation and operation of fusion centers.

Table of Contents

Executive Summary

The need to develop and share information and intelligence across all levels of government has significantly changed over the last few years. The long-standing information sharing challenges among law enforcement agencies, public safety agencies, and the private sector are slowly disappearing. Yet, the need to identify, prevent, monitor, and respond to terrorist and criminal activities remains a significant need for the law enforcement, intelligence, public safety, and private sector communities.

Through the support, expertise, and knowledge of leaders from all entities involved, the fusion center concept can become a reality. Each official has a stake in the development and exchange of information and intelligence and should act as an ambassador to support and further this initiative. It is the responsibility of leadership to implement and adhere to the *Fusion Center Guidelines*.

In their January 2005 survey, the National Governors Association Center for Best Practices revealed that states ranked the development of state intelligence fusion centers as one of their highest priorities.

The development and exchange of intelligence is not easy. Sharing this data requires not only strong leadership, it also requires the commitment, dedication, and trust of a diverse group of men and women who believe in the power of collaboration.

How can law enforcement, public safety, and private entities embrace a collaborative process to improve intelligence sharing and, ultimately, increase the ability to detect, prevent, and solve crimes while safeguarding our homeland? Recently, an initiative has emerged that incorporates the various elements of an ideal information and intelligence sharing project: fusion centers (or "center"). This initiative offers guidelines and tools to assist in the establishment and operation of centers. The guidelines are a milestone in achieving a unified force among all levels of law enforcement agencies; public safety agencies, such as fire, health, and transportation; and the private sector. Fusion centers bring all the relevant partners together to maximize the ability to prevent and respond to terrorism and criminal acts. By embracing this concept, these entities will be able to effectively and efficiently safeguard our homeland and maximize anticrime efforts.

What Is the Fusion Center Guidelines Initiative?

In 2004 and 2005, many states began creating fusion centers with various local, state, and federal funds. At the time, no standards or guidelines were in existence to assist with interoperability and communication issues with other centers at the state, regional, and federal levels. As a result, centers designed to share information were actually silos of information, incapable of information exchange. In response, the U.S. Department of Justice (DOJ), at the request of its Global Justice

Information Sharing Initiative's (Global) Criminal Intelligence Coordinating Council (CICC), formed the Law Enforcement Intelligence Fusion Center Focus Group (FCFG).[1]

Concurrently, the U.S. Department of Homeland Security's (DHS) Homeland Security Advisory Council (HSAC or Council) Intelligence and Information Sharing Working Group was focusing on prevention and information sharing by developing guidelines for local and state agencies in relation to the collection, analysis, and dissemination of terrorism-related intelligence (i.e., the fusion process). The recommendations resulting from DOJ's initiative and HSAC's efforts laid the foundation for the expansion of the *Fusion Center Guidelines* to integrate the public safety and private sector entities.

Subsequent to publishing Version 1 of the *Fusion Center Guidelines* and the HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report, DOJ and HSAC established two additional focus groups—the Public Safety FCFG and the Private Sector FCFG—in an effort to develop a comprehensive set of guidelines for fusion centers. Participants in the three focus groups[2] included experts and practitioners from local, state, and federal law enforcement agencies; public safety agencies; and the private sector as well as representatives from currently operating fusion centers.[3] In addition, representatives from national law enforcement, public safety, and private sector organizations participated in the focus groups.

These guidelines should be used to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities. The guidelines and related materials will provide assistance to centers as they prioritize and address threats posed in their specific jurisdictions for all crime types, including terrorism. In addition, the guidelines will help administrators develop policies, manage resources, and evaluate services associated with the jurisdiction's fusion center.

The guidelines should be used for homeland security, as well as all crimes and hazards. The full report contains an in-depth explanation of the guidelines and their key elements. Also included in the report are additional resources, model policies, and tools for guideline implementation.

What Is the Fusion Process?

The concept of fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention,

response, and consequence management programs. At the same time, it supports efforts to address immediate or emerging threat-related circumstances and events.

Data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector—and, with analysis, can result in meaningful and actionable intelligence and information. The fusion process turns this information and intelligence into actionable knowledge. Fusion also allows for relentless reevaluation of existing data in context with new data in order to provide constant updates. 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.

Fusion: Turning Information and Intelligence Into Actionable Knowledge

---

Because of the privacy concerns that attach to personally identifiable information, it is not the intent of fusion centers to combine federal databases containing personally identifiable information with state, local, and tribal databases into one system or warehouse. Rather, when a threat, criminal predicate, or public safety need is identified, fusion centers will allow information from all sources to be readily gathered, analyzed, and exchanged, based upon the predicate, by providing access to a variety of disparate databases that are maintained and controlled by appropriate local, state, tribal, and federal representatives at the fusion center. The product of this exchange will be stored by the entity taking action in accordance with any applicable fusion center and/or department policy, including state and federal privacy laws and requirements.

What Is a Fusion Center?

A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (hereafter, NCISP or Plan).[4] The NCISP is the blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. The Plan contains over 25 recommendations that were vetted by law enforcement officials and experts from local, state, tribal, and federal agencies. It embraces intelligence-led policing, community policing, and collaboration and serves as the foundation for the *Fusion Center Guidelines*.

A *fusion center* is defined as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity." Among the primary focuses of fusion centers are the

---

1 Previously named the Fusion Center Intelligence Standards Focus Group.
2 A complete listing of participants from each of the focus groups can be found in Appendix A.
3 Information on currently operating fusion and intelligence centers can be accessed via the National Criminal Intelligence Resource Center at www.ncirc.gov.

4 The *National Criminal Intelligence Sharing Plan* is available at www.it.ojp.gov.

intelligence and fusion processes, through which information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information (e.g., risk assessments and suspicious activity reports) that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity. It is recommended that the fusion of public safety and private sector information with law enforcement data be virtual through networking and utilizing a search function. Examples of the types of information incorporated into these processes are threat assessments and information related to public safety, law enforcement, public health, social services, and public works. Federal data that contains personally identifiable information should not be combined with this data

> Although each fusion center will have unique characteristics, it is important for centers to operate under a consistent framework—similar to the construction of a group of buildings where each structure is unique, yet a consistent set of building codes and regualtions are adhered to regardless of the size or shape of the building.

until a threat, criminal predicate, or public safety need has been identified. These processes support efforts to anticipate, identify, prevent, monitor, and respond to criminal activity. Federal law enforcement agencies that are participating in fusion centers should ensure that they comply with all applicable privacy laws when contemplating the wholesale sharing of information with nontraditional law enforcement entities.

Ideally, the fusion center involves every level and discipline of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. The fusion process should be organized and coordinated, at a minimum, on a statewide level, and each state should establish and maintain a center to facilitate the fusion process. Though the foundation of fusion centers is the law enforcement intelligence component, center leadership should evaluate their respective jurisdictions to determine what public safety and private sector entities should participate in the fusion center. To aid in this assessment, functional categories have been developed, in which similar entities are grouped. These categories are not comprehensive but represent a starting point for fusion center leadership to begin assessing what agencies and organizations should be involved in the center's operations.

The functional categories include:

- Agriculture, Food, Water, and the Environment
- Banking and Finance
- Chemical Industry and Hazardous Materials

- Criminal Justice
- Education
- Emergency Services (non-law enforcement)
- Energy
- Government
- Health and Public Health Services
- Hospitality and Lodging
- Information and Telecommunications
- Military Facilities and Defense Industrial Base
- Postal and Shipping
- Private Security
- Public Works
- Real Estate
- Retail
- Social Services
- Transportation

The *Fusion Center Guidelines* report contains an appendix describing the functional categories and provides examples of the types of information that the entities can provide to fusion centers.

Why Should Fusion Centers Be Established?

The ultimate goal is to provide a mechanism through which government, law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. It is critical for government to accomplish more with less. Fusion centers embody the core of collaboration, and as demands increase and resources decrease, fusion centers will become an effective tool to maximize available resources and build trusted relationships. It is recommended that fusion centers adhere to these guidelines and integrate the key elements of each guideline to the fullest extent, in order to enhance information and intelligence sharing.

Summary of Guidelines and Key Elements[5]

1. **Adhere to the tenets contained in the *National Criminal Intelligence Sharing Plan* (NCISP) and other sector-specific information sharing plans, and perform all steps of the intelligence and fusion processes.**

   ✓ Consult the tenets of the NCISP, and use model standards and policies as a blueprint for establishing or enhancing the intelligence function within the center.

   ✓ Consult the Homeland Security Advisory Council's (HSAC) *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report when incorporating the fusion process in the center.

2. **Collaboratively develop and embrace a mission statement, and identify goals for the fusion center.**

   ✓ Develop the center's mission statement and goals collaboratively with participating entities.

   ✓ Identify customer needs, define tasks, and prioritize functions.

   ✓ Ensure the mission statement is clear and concise and conveys the purpose, priority, and role of the center.

   ✓ Include the name and type of the center, what the center does, and whom the center serves in the mission statement.

3. **Create a representative governance structure that includes law enforcement, public safety, and the private sector.**

   ✓ Ensure all participating agencies have a voice in the establishment and operation of the fusion center.

   ✓ Ensure participating entities are adequately represented within the governance structure.

   ✓ Compose the governing body with officials who have authority to commit resources and make decisions.

4. **Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector.**

   ✓ Maintain a diverse membership to include representatives from local, state, tribal, and federal law enforcement, public safety, and the private sector.

   ✓ Conduct regular meetings with center personnel, and participate in networking groups and organizations.

   ✓ Educate and liase with elected officials and community leadership to promote awareness of center operations.

5. **Utilize Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.**

   ✓ Educate and consult legal advisors early in the fusion center development process.

   ✓ Utilize an NDA for fusion center personnel and participants to aid in the security of proprietary information.

   ✓ Ensure awareness of local, state, and federal public records laws as they relate to NDAs, including the Freedom of Information Act (FOIA).

   ✓ Use an MOU as the foundation for a collaborative initiative, founded on trust, with the intent to share and exchange information.

   ✓ At a minimum, consider including the following elements in fusion center MOUs:
      o Involved parties
      o Mission
      o Governance
      o Authority
      o Security
      o Assignment of personnel (removal/rotation)
      o Funding/costs
      o Civil liability/indemnification issues
      o Policies and procedures
      o Privacy
      o Terms

---

5   Electronic versions of the documents, products, and reports referenced in the following guidelines can be found at www.it.ojp.gov.

- Integrity control
- Dispute resolution process
- Points of contact
- Effective date/duration/modification/termination
- Services
- Deconfliction procedure
- Code of conduct for contractors
- Special conditions
- Protocols for communication and information exchange

6. **Leverage the databases, systems, and networks available via participating entities to maximize information sharing.**
   - ✓ Obtain access to an array of databases and systems. At a minimum, consider obtaining access to driver's license information, motor vehicle registration data, location information, law enforcement and criminal justice systems or networks, and correctional data.
   - ✓ Become a member of a regional or state secure law enforcement network, such as the Regional Information Sharing Systems® (RISS)/Federal Bureau of Investigation's (FBI) Law Enforcement Online (LEO) system, the U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), or the FBI's Law Enforcement Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx).

7. **Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems. Use the U.S. Department of Justice's (DOJ) Global Justice Extensible Markup Language (XML) Data Model and the National Information Exchange Model (NIEM) standards for future database and network development, and consider utilizing the Justice Information Exchange Model (JIEM) for enterprise development.**
   - ✓ Establish formal communications protocols, and ensure effective and efficient information exchange.
   - ✓ Develop and implement a communications plan, and ensure secure and redundant communications.
   - ✓ Ensure communications and systems access policies, including consequences for noncompliance.
   - ✓ Consider utilizing the Organization for the Advancement of Structured Information Standards (OASIS)-ratified Common Alerting Protocol (CAP) to enable the exchange of emergency alert and public warning information over data networks and computer-controlled warning systems.

8. **Develop, publish, and adhere to a privacy and civil liberties policy.**
   - ✓ Develop, display, adhere to, and train personnel on the center's privacy policy.
   - ✓ Consult the Fair Information Practices when developing a privacy policy.
   - ✓ Ensure all other policies and internal controls are consistent with the center's privacy policy.
   - ✓ Establish a process for tracking and handling privacy complaints or concerns.
   - ✓ Develop rules on the use of privately held data systems information.
   - ✓ Adhere to applicable state and federal constitutional and statutory privacy and civil liberties provisions.
   - ✓ Specify that public safety and private sector databases should not be combined with any federal databases that contain personally identifiable information.
   - ✓ Fusion center participants should comply with all local, state, tribal, and federal privacy laws, when applicable.

9. **Ensure appropriate security measures are in place for the facility, data, and personnel.**
   - ✓ Develop, publish, and adhere to a security plan, and ensure proper safeguards are in place.
   - ✓ Ensure security plans are marked, handled, and controlled as sensitive but unclassified (SBU) information.
   - ✓ Obtain appropriate security clearances for personnel within the center and key decision makers who need access.
   - ✓ Conduct background checks on personnel.
   - ✓ Train personnel on the center's security protocols.
   - ✓ Consult Global's *Applying Security Practices to Justice Information Sharing* document and resource materials when developing a security plan.
   - ✓ Consult the Homeland Security Information Act of 2002: Critical Infrastructure Information Act when collecting and storing critical infrastructure-related information.
   - ✓ Consult private industry security personnel when obtaining and storing industry-specific information (e.g., building security plans).
   - ✓ Ensure state laws allow for the security and confidentiality of public and private sector data.

10. **Integrate technology, systems, and people.**
    - ✓ Colocate personnel and/or utilize virtual integration to bring technology, systems, and people together.
    - ✓ Base the selection of a site on the functional needs of the center.
    - ✓ Plan, identify, design, train, implement, and adhere to a physical security plan and a contingency plan.

11. **Achieve a diversified representation of personnel based on the needs and functions of the center.**
    - ✓ Maintain a 24-hour-a-day/7-day-a-week operation when feasible.
    - ✓ Require a minimum term commitment for full-time center personnel.
    - ✓ Identify subject-matter experts from the private sector for utilization when industry-specific threats or crimes are identified (e.g., cyber threats).
    - ✓ Adhere to the *Law Enforcement Analytic Standards* booklet and other relevant analytic publications available through the International Association of Law Enforcement

Intelligence Analysts (IALEIA) when hiring personnel to perform the analytic function.

12. Ensure personnel are properly trained.

- ✓ Adhere to the training objectives outlined in the *National Criminal Intelligence Sharing Plan*.

- ✓ Ensure center personnel meet the minimum training standards outlined in the report *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies*.

- ✓ Ensure center personnel receive training on facility and information security, operations, policies, and procedures.

- ✓ Include cross-educational training regarding the fusion centers and the applicable functional categories, including the types of information that entities can provide to the fusion center and what the center does with the information, once received.

13. Provide a multitiered awareness and educational program to implement intelligence-led policing and the development and sharing of information.

- ✓ Ensure appropriate noncenter personnel involved in the intelligence process are aware of the center's functions, including policymakers, agency heads, and private sector executives.

- ✓ Develop and disseminate outreach and educational materials to officers, analysts, policymakers, and others.

14. Offer a variety of intelligence services and products to customers.

- ✓ Produce strategic and tactical products to support the mission and priorities of the center.

- ✓ Consult the *Law Enforcement Analytic Standards* booklet to ensure development of professional quality analytic products.

- ✓ Ensure that feedback from participating agencies and organizations occurs when products are created and distributed.

15. Develop, publish, and adhere to a policies and procedures manual.

- ✓ Use a standardized format to allow for easy reading, filing, retrieving, and correcting.

- ✓ Implement an annual review of center directives, and purge or revise outdated policies and procedures.

- ✓ Ensure that personnel have access to the latest policies and procedures manual.

16. Define expectations, measure performance, and determine effectiveness.

- ✓ Design performance measures based on the center's core mission, goals, and objectives.

- ✓ Ensure performance measures are valid, reliable, measurable, and quantifiable.

- ✓ Develop an evaluation process to gauge the adequacy, appropriateness, and success of center services.

- ✓ Use performance measures and an evaluation process to make decisions and allocate resources.

- ✓ Utilize performance measures to track progress and ensure accountability.

- ✓ Inform center personnel of performance and progress on a regular basis.

17. Establish and maintain the center based on funding availability and sustainability.

- ✓ Identify center needs and available funding sources, to include local, state, tribal, federal, and nongovernmental sources.

- ✓ Establish an operational budget and adhere to reporting requirements.

18. Develop and implement a communications plan among fusion center personnel; all law enforcement, public safety, and private sector agencies and entities involved; and the general public.

- ✓ Determine primary and secondary modes of communication between the fusion center and participating entities.

- ✓ Incorporate regular testing of the plan to ensure its functionality.

- ✓ Include a mechanism to alert fusion center participants of new information and intelligence.

A companion CD has been developed in conjunction with the Fusion Center Guidelines report. This CD contains sample policies, checklists, resource documents, and links to Web sites that are referenced throughout the report. For copies of the resource CD, contact DOJ's Global at (850) 385-0600. The fusion center resources are also available at DOJ's Global Web site, www.it.ojp.gov/fusioncenter, DHS's Web site, and the Homeland Security Information Network (HSIN).

Introduction—
Fusion Concept and Functions

As criminal and terrorist activity threatens the safety of our nation's citizens and visitors, the ability to quickly exchange relevant information and intelligence becomes increasingly critical. Over the last few years, significant progress has been made in breaking down barriers and improving information exchange. Policymakers and leaders have recognized the importance of creating an environment where intelligence can be securely shared among law enforcement, public safety agencies, and the private sector. Although strides have been made, there is still much work ahead. There is still an urgent need to rigorously refine and accommodate our rapidly changing world.

Many obstacles have been encountered that have impacted the ability to share intelligence, such as the lack of trusted partnerships; disparate, incompatible, and antiquated communications, computer systems, and software; the need to query multiple databases or systems; the lack of communication; the lack of standards and policies; and legal and cultural issues.

These barriers have proven to be difficult hurdles. Yet, there are steps that can be taken to overcome these issues and create a proactive environment for the successful exchange of intelligence.

Fusion Center Guidelines Development

Through the U.S. Department of Justice (DOJ), members of its Global Justice Information Sharing Initiative (Global) have developed recommended guidelines to enhance justice information sharing.[6] Examples include the *National Criminal Intelligence Sharing Plan* (NCISP or Plan), the *Privacy and Information Quality Policy Development for the Justice Decision Maker*, the *Applying Security Practices to Justice Information Sharing*, and the Global Justice Extensible Markup Language (XML) Data Model (Global JXDM). DOJ's Global represents over 30 law enforcement organizations throughout the country, at all levels of government. Global promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

Information systems contribute to every aspect of homeland security. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Databases used for federal law enforcement, immigration, intelligence, public health, surveillance, and emergency management have not been connected in a way that allows us to comprehend where information gaps and redundancies exist.

We must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

The National Strategy for Homeland Security
July 2002

Through the Global Intelligence Working Group (GIWG)—one of Global's four issue-focused working groups—intelligence issues, concerns, and obstacles have been addressed. Global's Criminal Intelligence Coordinating Council (CICC)[7] supported the development of the Law Enforcement Intelligence Fusion Center Focus Group (FCFG) to initiate Phase 1 of the fusion center guidelines development. This group was tasked with recommending guidelines specifically for the law enforcement

---

6   For more information regarding Global, visit www.it.ojp.gov.

7   The CICC was established in response to recommendations contained in the NCISP. The CICC is composed of local, state, and federal entities and advises the U.S. Attorney General on matters relating to criminal intelligence.

intelligence component of fusion centers. The focus group was also tasked with recommending related model policies and procedures to support this initiative. Group members recognized the need and importance of integrating all public safety and private partners.

Concurrently, a parallel effort was under way by the Homeland Security Advisory Council (HSAC) Intelligence and Information Sharing Working Group to develop intelligence and information sharing guidelines, based on specific presidential directives, for local, state, and federal agencies creating fusion centers.[8] These directives provide guidance to local and state entities regarding prevention and response to criminal and terrorist activities.[9] The recommendations and findings resulting from HSAC's Intelligence and Information Sharing Working Group efforts support the expansion of the *Fusion Center Guidelines* to public safety and private sector entities.

Subsequent to the efforts of the Law Enforcement Intelligence FCFG and HSAC, the Public Safety FCFG was created for the purpose of integrating the public safety component into the *Fusion Center Guidelines.* Members of the focus group concentrated on the need for information and intelligence sharing between law enforcement and public safety communities. This group endorsed the guidelines developed by the Law Enforcement Intelligence FCFG and offered suggestions and recommendations to successfully incorporate public safety entities into fusion centers.

The last phase established the Private Sector FCFG, whose mission was to integrate the private sector into the guidelines. With 85 percent of critical infrastructure owned by private entities, their involvement in fusion centers is essential to having a comprehensive all-hazards, all-crimes fusion center. Key points addressed included collaboration between the fusion center and mission-critical private sector entities, as well as identification of private sector capabilities and information needs. In addition, the need for a two-way educational process between the private sector and fusion centers was identified. The purpose of this educational process is to develop an understanding of how each entity operates and how each can enhance operations and functionality with the other.

All levels of government, the private sector, and nongovernmental organizations must work together to prepare for, prevent, respond to, and recover from terrorist and criminal events. Through

the hard work, dedication, and commitment of the individuals participating in these efforts, the appropriate guidelines, tools, and information will be available to all entities involved. In addition, a collaborative environment will result in a consistent, unified approach to prevention and response.

The ultimate goal is to provide a mechanism where law enforcement, public safety, and private sector partners can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. The fusion center is this mechanism; it is key to ensuring the flow of threat- and crime-related information between local, state, regional, and federal partners. The guidelines contained in the report represent the key components and issues to consider when establishing fusion centers.

The Fusion Concept

Law enforcement has always been aware of the key role that information and intelligence play in prevention and response. Although it is impossible to protect every potential target from every conceivable method of attack, a number of strategies can be implemented to maximize this ability. In addition, further refinement in the intelligence and information sharing arena will maximize the ability to respond quickly and efficiently if an incident occurs.

Effective terrorism-related intelligence information and crime prevention, protection, preparedness, and response depend on timely and accurate information about the terrorists, their operations, their support mechanisms and structure, their targets, and their attack methods. This information should serve as a guide for efforts to rapidly identify both immediate and long-term threats; identify persons involved in terrorism-related and criminal activities; and guide the implementation of information-driven and risk-based prevention, response, and consequence-management.

Since September 11, both response and prevention are critical to an overall strategy to secure our homeland and decrease criminal activities. September 11 also confirmed how critical local, state, tribal, and federal law enforcement agencies and public safety and private sector entities are in collecting important information and intelligence that ultimately impacts the nation's overall ability to prevent terrorism-related and criminal activities. In responding

Fusion:

Turning Information and Intelligence Into Actionable Knowledge

---

8   More information on HSAC can be accessed at www.dhs.gov/hsac.
9   Homeland Security Presidential Directive 8 (HSPD-8) was issued with the purpose of establishing policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. This is done by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities of federal, state, and local entities. HSPD-5 addresses the management of domestic incidents and identifies steps for improved coordination in response to incidents. It requires the U.S. Department of Homeland Security to coordinate with other federal departments and local, state, and tribal governments to establish a National Response Plan (NRP) and a National Incident Management System (NIMS). Each of these items plays a role in the establishment of fusion centers and lays a foundation for enhanced information and intelligence sharing among all levels of law enforcement, public safety, and the private sector. For more information regarding HSPD-8, HSPD-5, NRP, and NIMS, visit www.ojp.usdoj.gov/odp/assessments/hspd8.htm.

to September 11 and subsequent incidents (e.g., the anthrax issue), it became apparent how important it is to incorporate nontraditional collectors of data (e.g., fire and health entities) into prevention efforts. Data fusion represents an important part of a mechanism that can dramatically improve information and intelligence sharing between all components and collectors of information.

As a result of the need to exchange diverse data from various sources, fusion emerged as the fundamental process to facilitate the sharing of homeland security- and crime-related intelligence. On the surface, it would appear that defining fusion is difficult. Although the concept is new to many law enforcement, public safety, and private sector communities, fusion is not new to many other industries and the military. In fact, fusion has been discussed and used in transportation and aviation; satellite imaging; meteorology and weather forecasting; sensory imaging; and military and defense activities for years.

Fusion refers to managing the flow of information and intelligence across levels and sectors of government and private industry.[10] It goes beyond establishing an intelligence center or creating a computer network. Fusion supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate or emerging threat-related circumstances and events. Data fusion involves the exchange of information from different sources, including law enforcement, public safety, and the private sector.[11] When combined with appropriate analyses, it can result in meaningful and actionable intelligence and information. The fusion process turns information and intelligence into knowledge. The primary emphasis of fusion is to identify emerging terrorism-related threats and risks as well as to support ongoing efforts to address criminal activities. The fusion process will:

- Allow local and state entities to better forecast and identify emerging crime and public health trends.
- Support multidisciplinary, proactive, risk-based, and community-focused problem solving.
- Provide a continuous flow of intelligence to officials to assist in developing a depiction of evolving threats.
- Improve the delivery of emergency and nonemergency services.

To illustrate the fusion process within a conceptualized fusion center concept, Figure 1 depicts a distributed capability, populated by multiple and diverse information sources. Users access the data via a common interface, extracting, analyzing, and disseminating information based on need and current demands. Although it is anticipated that fusion and fusion centers will primarily be used for preventive and proactive

---

10 Terms and definitions mentioned in this document, including "fusion," are specific to the fusion center initiative. Varying definitions of the same term may be utilized within the law enforcement intelligence, public safety, and private sector fields, and participants in the fusion center initiative should ensure that term definitions do not deconflict. Definitions of terms specified in this document can be found in Appendix F.

11 The fusion of public safety and private sector information with any federal database containing personally identifiable information should be virtual through networking and utilizing a search function. Federal agencies participating in the fusion center should adhere to applicable federal laws and regulations.

Figure 1 – Fusion Process
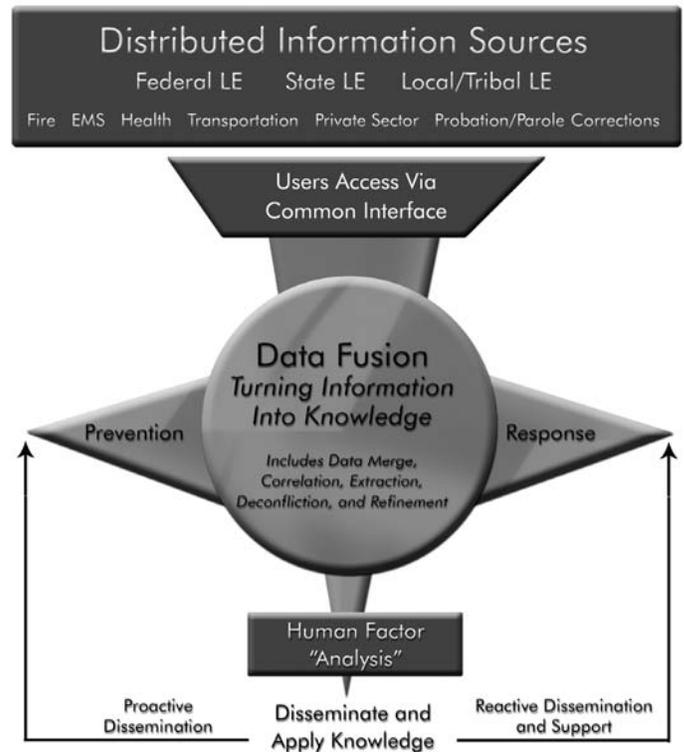
measures, the process will also be critical if an incident occurs, providing information to responders as well as officials, media, and citizens. It is important to note that the fusion process is not a system or database; it is an important part of a mechanism by which participating law enforcement, public safety, and private sector entities can provide and receive enhanced information from a fusion center.

Criminal and terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism-related information. It can come through the efforts of the intelligence community; local, state, tribal, and federal law enforcement authorities; other government agencies (e.g., transportation and health departments); the private sector; and the general public. In order to implement an effective fusion process, a number of issues must be addressed, including the following:

- The use of common terminology, definitions, and lexicon by all stakeholders.
- Up-to-date awareness and understanding of the global threat environment.
- A clear understanding of the linkages between terrorism-related and nonterrorism-related information and intelligence.
- Clearly defined intelligence and information requirements that prioritize and guide planning, collection, analysis, and dissemination efforts.
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process.

- Understanding and eliminating impediments to information collection and sharing.
- Extensive and ongoing interaction with the private sector and with the public at large.
- Connectivity (technical and procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories.
- Extensive participation of subject-matter experts in the analytical process.
- Capacity to ensure aggressive oversight and accountability to protect constitutional protections and civil liberties.

Through the use of fusion centers and by integrating these guidelines, model templates, policies, and tools, the outstanding issues hindering our nation's ability to seamlessly develop and share information and intelligence will be minimized.

Fusion Centers

The ability to coordinate effective responses in the event of a terrorist attack is a significant challenge facing our nation. It is imperative that all appropriate means to combat terrorism, respond to terrorist attacks, and reduce criminal activity be employed. This section will define fusion centers; summarize the basic functions of a fusion center; and provide a summary comparison of fusion centers, intelligence centers, and emergency operations centers.

A fusion center is 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, investigate, apprehend, and respond to criminal and terrorist activity.

The primary components of a fusion center are situational awareness and warnings that are supported by law enforcement intelligence, derived from the application of the intelligence process, where requirements for actionable information are generated and information is collected, integrated, evaluated, analyzed, and disseminated. Other key components resident in the fusion center include representatives of public safety, homeland security, the private sector, and critical infrastructure communities.

Fusion centers are not traditional intelligence centers nor do they perform the same functions as emergency operations centers. Fusion centers are multidisciplinary, whereas intelligence centers

Important intelligence that may forewarn of a future attack may be derived from information collected by local, state, tribal, and federal law enforcement agencies; public safety agencies; and private sector entities through crime control and other normal activities, as well as by people living and working in our communities.

are traditionally law enforcement centric. Emergency Operations Centers (EOC) focus on disaster recovery (both natural and man-made). It is important to note that although these centers are different and have unique missions, they must work together and understand each others' goals and priorities. If an incident occurs, all of these resources will be needed to successfully minimize loss and apprehend suspects. The fusion center provides intelligence to the EOC regarding the disaster or related events. Because of the investment, expertise, and capability integrated within a fusion center, plans and procedures should include how each fusion center will support the jurisdiction's emergency management structure during crises. Furthermore, each fusion center should make provisions for supporting crisis management and recovery operations as laid out in the Incident Command System (ICS), the National Incident Management System (NIMS), and the National Response Plan (NRP).

Fusion centers embody the core of collaboration. Collaboration increases capacity, communication, and continuity of service while decreasing duplication.[12] As demands increase and resources decrease, collaboration becomes an evermore effective tool to maximize resources and build trusted relationships. In a recent survey conducted by the National Governors Association (NGA) Center for Best Practices, responding states ranked the development of a state intelligence fusion center as one of their highest priorities.[13] This is significant and indicates a need to quickly provide information, materials, and guidelines to assist in establishing and operating fusion centers.

As illustrated in Figure 2, the fusion center concept embraces the collaboration of numerous resources, maximizing and streamlining operations, while moving jointly toward a common goal. The figure depicts participating entities using MOUs to define their roles, responsibilities, and contributions toward center operations. These resources funnel into a central location, the fusion center. Here, authorized personnel use the resources and information to assist investigative and intelligence services, homeland security, and public safety operations and to integrate critical infrastructure functions and private sector partnerships. Participants are subject to all the policies and procedures that guide center operations. Appropriate information and intelligence is then disseminated to authorized recipients and used to investigate crimes and proactively address threats.

---

12   C. R. Pete Petersen, M.Ed., *Community Collaboration*, March 4, 2003.
13   NGA Center for Best Practices, *Homeland Security in the States: Much Progress, More Work*, January 24, 2005.

Figure 2—Fusion Center Components
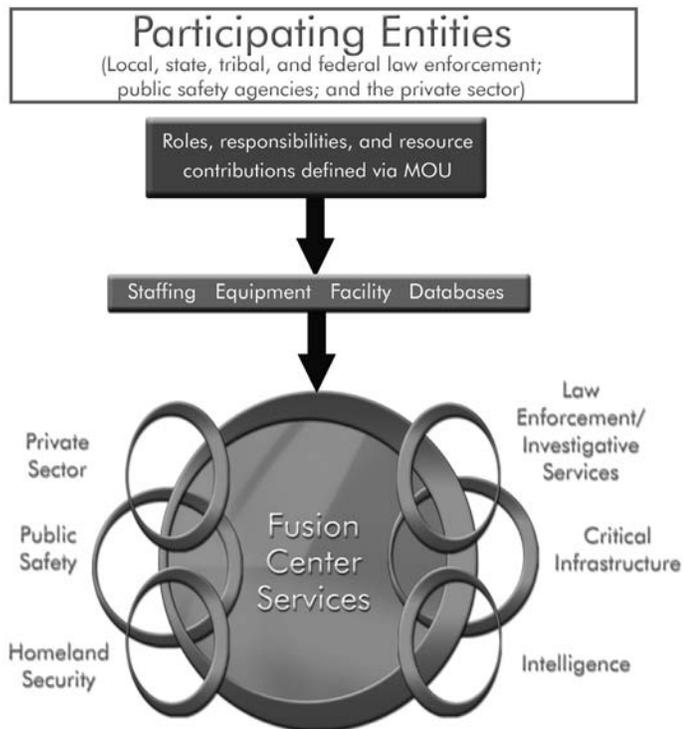
Fusion centers will act as an analytical hub, processing, evaluating, and disseminating critical information for law enforcement, public safety, and private partners, based on a criminal predicate, threat, or public safety need. They will focus on collaboration and analysis and will become a repository for information that flows through the center, while ensuring state and federal privacy laws and requirements are adhered to. Ultimately, fusion centers will become the center for investigative support, information and intelligence sharing, homeland security, and public safety and private sector partners.

Fusion Center Functions

The principal role of the fusion center is to compile, analyze, and disseminate criminal/terrorist information and intelligence and other information (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal/terrorist activity. This criminal information and intelligence should be both strategic (i.e., designed to provide general guidance of patterns and trends) and tactical (i.e., focused on a specific criminal event). To be meaningful, the fusion center must do more than a one-time collection of law enforcement information. It must include developing the capability to analyze on an ongoing basis law enforcement information and intelligence with other important information, such as public health and transportation, based on a criminal predicate, threat, or public safety need. The goal is to rapidly identify emerging threats; support multidisciplinary, proactive, and community-focused problem-solving activities; support predictive analysis capabilities; and improve the delivery of emergency and nonemergency services.

One of the principal outcomes of the fusion process should be the identification of terrorism-related leads—any nexus between crime-related and other information collected by local, state, and private entities and a terrorist organization and/or attack. Many experts believe that there is a high probability of identifying terrorists through precursor criminal activity, including illegal drug operations, money laundering, fraud, terrorism, and identity theft.[14] The fusion process does not replace or replicate mission-specific intelligence and information management. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns and trends that may reflect an emerging threat. Some of the recommended goals and functions for fusion centers include:

- Serve as the primary point of contact to report criminal/terrorist information to the local Joint Terrorism Task Force (JTTF) and DHS's Homeland Security Operations Center (HSOC).
- Include the capability of blending law enforcement information and intelligence.
- Collect, analyze, and disseminate "all-crimes" information, so as to identify emerging patterns and trends. Evaluate and reevaluate the process, new data, and emerging threats.
- Adopt and adhere to a statewide strategy to examine the information exchanges of the states' law enforcement and homeland security partners, including dissemination of information by the state Homeland Security Advisor to law enforcement.
- Maintain an up-to-date statewide risk assessment.
- Serve as a receipt-and-dissemination hub for law enforcement information provided by federal entities, such as that provided by the Federal Bureau of Investigation's Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx), when operational, and DHS's Homeland Security Information Network (HSIN).

Each of these areas can be expanded to include a number of critical tasks and responsibilities. To successfully achieve these goals, the first responder and private community, along with the public, must be a part of the fusion center concept. The integration of nontraditional consumers of information and intelligence is a key component of a fusion center.

The responsibilities of fusion centers are immense. Guidelines, as well as sample policies and templates, must be developed to assist in establishing and operating fusion centers.

Functional Categories

Every level and sector (discipline) of government and the private sector should be integrated into fusion centers. This may seem like a daunting task; however, functional categories have been developed to assist in integration efforts. These categories are not meant to be exhaustive; rather, they provide governance bodies a starting place to begin collaboration with different components and entities. Each fusion center should evaluate its needs, threats, and constituents to determine what entities should be integrated. Entities that comprise the functional categories can provide fusion centers with both

---

14 *The Impact of Terrorism on State Law Enforcement*, June 2005, p. 34.

strategic and tactical information, including crime trends for particular industries and public safety agencies, suspicious activity, and risk assessments. Fusing this information, based on an identified threat, criminal predicate, or public safety need, with law enforcement intelligence will provide centers with a more complete picture of crime and terrorism. The fusion of public safety and private sector information with law enforcement data should be virtual through networking and utilizing a search function, thus ensuring the separation of federal data that contains personally identifiable information.

The overarching functional categories include:

- Agriculture, Food, Water, and the Environment
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Criminal Justice
- Education
- Emergency Services (non-law enforcement)
- Energy
- Government
- Health and Public Health Services
- Hospitality and Lodging
- Information and Telecommunications
- Military Facilities and Defense Industrial Base
- Postal and Shipping
- Private Security
- Public Works
- Real Estate
- Retail
- Social Services
- Transportation

These categories outline the types of law enforcement intelligence and public safety and private sector entities to include in collaboration. Types of information that may be provided to fusion centers include a suspicious fire that a fire department responds to, an unusual sickness reported at a public health department, spikes in cattle disease on a farm, or suspicious banking activity reports.[15] In addition, these entities should be recipients of information and intelligence from fusion centers, including threat alerts and related response efforts.

State Strategy

Fusion involves every level and sector (discipline) of government, private sector entities, and the public—though the level of involvement of some participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process due to the relationship between crime and terrorism and the fact that, in many cases, law enforcement authorities are best suited to coordinate statewide and local fusion. The HSAC working group recommended that fusion centers be established in every state. The fusion process should be organized and coordinated on

a state level, and each state should establish and maintain an analytic center. Furthermore, each state fusion center should regularly collaborate and coordinate with other state fusion centers to prevent information silos from developing within states. This effort will enhance information and intelligence sharing.

The functions within a state fusion center should be based on the intelligence cycle, including requirements, priorities, identified collectors, indicators for the collectors to be aware of, collection mechanisms, methods of analysis, and production and dissemination of reports and assessments to the appropriate recipients. Public safety and private sector entities, along with the general public, are a critical part of this plan and should be incorporated into the intelligence cycle as collectors and recipients of information, based on their information requirements.

Each major urban area may want to establish a similar capacity, ensuring that it is linked with the state center. Other localities, tribal governments, and even the private sector should develop a process to interlink to these state fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activity.

Efforts should be scalable and organized and managed on a geographic basis so adjustments can be made based on changes in the environment. And, while national guidelines should guide the process, the actual technologies and operational protocols used by individual jurisdictions should be based on the specific capabilities.

Information Flow

With the establishment of fusion centers around the country, it is important to have a clear understanding of who should receive and disseminate information and how it flows both vertically and horizontally among all local, state, tribal, and federal government agencies and private entities. Successful counterterrorism efforts require that local, state, tribal, and federal law enforcement agencies, along with public safety and private sector entities, have an effective information sharing and collaboration capability. This will ensure they can seamlessly collect, collate, blend, analyze, disseminate, and use information and intelligence.

Intelligence and information should be provided based on the needs of the user. Although fusion center participants may include emergency management, public health, transportation, public works, and the private sector, each discipline will not need the same level of detail (e.g., fire officials and emergency management officials may not need the specific suspect information that law enforcement requires). Fusion centers should also exchange information with appropriate federal partners such as DOJ (e.g., Federal Bureau of Investigation, Joint Terrorist Task Force, and U.S. Marshals), DHS (e.g., U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and Emergency Alert Networks), High Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISS) centers, the Centers for Disease Control and Prevention (CDC), and other information sharing initiatives.[16]

---

15   An in-depth list of the entities that comprise each of the functional categories and various examples of the types of information these entities can provide to fusion centers can be found in Appendix C.

16   For information to be exchanged, refer to the Information Sharing Environment (ISE) required under the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, http://www.gpoaccess.gov/serialset/creports/intel_reform.html.

Background and Methodology

A Phased Approach

The development of fusion center guidelines was separated into three phases—law enforcement intelligence, public safety, and the private sector. The law enforcement intelligence phase developed the foundation for the guidelines. As each phase was established, previous phase participants were included in focus group meetings. This ensured that the guidelines were applicable to all components within a fusion center. In addition, this allowed for discussions to occur between all component representatives to identify concerns with the guidelines, its methodology, and how to effectively incorporate each component. The activities and recommendations of each focus group will be explained further in the report.

Phase I—Law Enforcement Intelligence Component

Background

Early in 2002, the International Association of Chiefs of Police (IACP) convened a Criminal Intelligence Sharing Summit attended by law enforcement executives and intelligence experts from across the country. Participants agreed that all law enforcement agencies must work together toward a common goal: developing the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies.

The Summit led to the creation of the Global Intelligence Working Group (GIWG). The GIWG, one of four issue-focused working groups under the Global Justice Information Sharing Initiative (Global),[17] was tasked with recommending a national intelligence plan. Members of the GIWG include representatives from law enforcement and justice organizations at all levels of government.

The GIWG promoted intelligence-led policing, recommended leveraging existing systems, and addressed the current and future needs of law enforcement agencies when developing the *National Criminal Intelligence Sharing Plan* (NCISP).[18]

"... we must create new ways to share information and intelligence both vertically, between governments, and horizontally, across agencies and jurisdictions . . . efforts with the Global Intelligence Working Group to create a National Criminal Intelligence Sharing Plan . . . is a helpful and welcome response."

> Former Homeland Security Secretary
> Tom Ridge
> October 23, 2003, Philadelphia, PA

Intelligence is the product of systematic gathering, evaluation, and analysis of raw data on individuals or activities suspected of being, or known to be, criminal. Intelligence-led policing is 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.[19]

The GIWG proposed 28 recommendations and action items for implementation, which are outlined in the NCISP. An event was held at the U.S. Department of Justice on May 14, 2004, to publicly support the recommendations and the Plan. Officials from local, state, and federal law enforcement agencies were present. The recommendations contained in the Plan pertain to a wide spectrum of intelligence issues and concerns, including:

- Standards for management
- Institutionalism and outreach
- Protection of rights and privacy
- Standards for process

---

17 For more information regarding Global, visit www.it.ojp.gov.
18 A copy of the *National Criminal Intelligence Sharing Plan* can be obtained at http://it.ojp.gov/topic.jsp?topic_id=93.
19 Appendix A of the *National Criminal Intelligence Sharing Plan*, October 2003.

- Sharing of classified information
- Standards for training
- Connectivity

Global's Criminal Intelligence Coordinating Council (CICC),[20] in support of DOJ's efforts to develop fusion center guidelines, recommended the creation of the Law Enforcement Intelligence Fusion Center Focus Group to further many of the tenets outlined in the Plan.

"The Plan represents law enforcement's commitment to take it upon itself to ensure that we do everything possible to connect the dots, whether it be a set of criminal dots or a set of terrorist dots."

Former U.S. Attorney General
John Ashcroft
May 14, 2004, Washington, DC

Methodology

The first phase of the *Fusion Center Guidelines* initiative was the establishment of the Law Enforcement Intelligence FCFG. The focus group was composed of representatives from a variety of local, state, and federal law enforcement agencies across the country, including law enforcement personnel involved with developing fusion centers, and offered example policies and materials to assist in this initiative.

Throughout the meetings and subsequent communications, participants were encouraged to discuss and share best practices resulting from the establishment and operation of their centers or initiatives. The focus group recommended that the intelligence component include all crime types and that centers provide an array of intelligence services. The group also recommended

---

20   The Criminal Intelligence Coordinating Council (CICC) was established in response to recommendations contained in the NCISP. The CICC is composed of local, state, and federal entities and advises the U.S. Attorney General on matters relating to criminal intelligence.

that centers be scalable based on the needs of the city, state, or region and should conduct tactical, operational, and strategic intelligence functions in support of criminal investigations.

The focus group's work developed Version 1, containing 17 fusion center law enforcement intelligence guidelines. These guidelines are the foundation for the intelligence component of fusion centers and take intelligence sharing to the next level. In addition, the focus group developed sample policies, tools, and a resource CD to assist agencies in integrating the guidelines. The Version 1 guidelines were presented to and supported by the CICC, the GIWG, the Global Advisory Committee, and DOJ's Justice Intelligence Coordinating Council (JICC). These guidelines were also approved by each component of the U.S. Department of Homeland Security (DHS). Version 1 of the *Fusion Center Guidelines* was published in July 2005.

Concurrent with the efforts of the Law Enforcement Intelligence Focus Group were the efforts of the Homeland Security Advisory Council's (HSAC) Intelligence and Information Sharing Working Group. The HSAC working group developed a report that revolved around integrating the fusion process into fusion centers. The result of the Law Enforcement Intelligence Working Group and the Intelligence and Information Sharing Working Group was a joining of efforts to expand the *Fusion Center Guidelines* to include the public safety and private sector components. HSAC also established a Private Sector Information Sharing Task Force that addressed the obstacles of information sharing between the federal government and the private sector. This task force also provided recommendations to alleviate the identified information sharing obstacles.[21]

Phase 2—Public Safety Component
Methodology

Subsequent to the completion of Version 1 of the *Fusion Center Guidelines*, Phase 2 of the initiative began, which involved incorporating the public safety component into fusion centers. Even in the planning stages, Phase 2 was a collaborative effort between DOJ and DHS. This collaboration demonstrated the commitment of the federal government to ensure a united and comprehensive set of guidelines for integrating public safety with law enforcement into local, state, regional, and federal fusion centers. The public safety component is essential to fusion centers for:

- Precursor information regarding crime, including information on diversion drugs and hazardous material.
- First responders, who can provide nontraditional information to fusion centers (e.g., fire and health departments).
- Information on suspicious criminal-related activity.

Participants in the Public Safety FCFG included members from a variety of public safety components, including fire, health, transportation, agriculture, and environmental protection. Also participating in the meeting were select members of the Law Enforcement Intelligence FCFG.

The first task the focus group addressed was to define what public safety is with respect to a fusion center. The focus group defined

---

21   A copy of this report can be found on the companion *Fusion Center Guidelines* resource CD.

---

public safety entities as government-based agencies that respond to contemplated or completed criminal acts, man-made or natural disasters, public health issues, or intentional acts that threaten or directly impact the essential functions of society. Examples of these functions include economic, transportation, communications, public works, power/energy, and food supply. Also discussed during the meeting were the concept of the fusion center and the definition of the fusion process with a focus on how to incorporate the public safety component into the center and process.

The focus group identified many public safety entities that could potentially be integrated into a fusion center and categorized them into functional categories. The categories are included as an appendix to the guidelines and, although not comprehensive, serve as a starting point for operating fusion centers to utilize when integrating public safety entities.[22] When jurisdictions are establishing a fusion center, the functional categories should be evaluated and the applicable entities should be identified and included as partners.

The consensus of the Public Safety FCFG was that the 17 guidelines in Version 1 provide a thorough explanation and guidance for jurisdictions establishing and operating a fusion center. The focus group recommended adding in Version 2 of the guidelines a more comprehensive explanation of the fusion process and examples of how public safety entities can be incorporated into the process.

Implementation

Collaboration is vital to the success of fusion centers. The public safety component can provide fusion centers with information that will add value to the intelligence and fusion processes. Additionally, fusion centers can provide public safety entities with information and intelligence that impact them, such as bomb threats, health-related information and intelligence, and/or transportation-related information. Public safety entities (fire, EMS, transportation) often impact the lives of citizens, and ensuring that these entities maintain situational awareness and are actively involved in the fusion center is important to protecting the lives of citizens. Fusion center governance members should evaluate the needs of their jurisdiction to identify what public safety entities should be involved in the fusion center with particular focus on health services, government, transportation, education, criminal justice and security, social services, and public works.

Public safety partners should be incorporated into all phases of the intelligence/fusion process. Entities within this sector represent nontraditional information gatherers and can provide fusion centers with both strategic and tactical information, including crime-related trends (e.g., prescription drug fraud and fire investigations); additional response capabilities (fire and hazmat); and suspicious activity (e.g., unusual diseases reported at hospitals). Public safety entities should also be included in the dissemination and evaluation phases.

Because of the groundbreaking efforts of the fusion center, participating entities may need awareness-level training of how the fusion center works, an explanation of the intelligence cycle, and

how public safety entities fit into these efforts. This awareness training should be offered initially to agency heads to receive support for integration and then delivered to the information gatherers and individuals who will support the fusion center.

There are a variety of ways that integration of the public safety component can occur. While the guidelines fully address integration opportunities, the fusion center and public safety agencies should determine whether a full-time representative or a liaison will be used in the center for receiving and sharing information and intelligence.

Phase 3—Private Sector Component
Methodology

Phase 3 of the *Fusion Center Guidelines* initiative involved the integration of the private sector. DOJ and DHS once again collaborated with the development of the Private Sector FCFG. This focus group was comprised of various private sector industry and association representatives, including tourism, banking and finance, maritime, and security. The private sector is a crucial component of fusion centers. Approximately 85 percent of the nation's critical infrastructure is owned by the private sector and

---

"We will build a national environment that enables the sharing of essential homeland security information. We must build a 'system of systems' that can provide the right information to the right people at all times. Information will be shared 'horizontally' across each level of government and 'vertically' among federal, state, and local governments; private industry; and citizens."

Source: The President's National Strategy for Homeland Security

---

vulnerable to crime, such as terrorism and fraud.

According to a study jointly conducted by the Council of State Governments and Eastern Kentucky University, since September 11, 2001, interactions between the private sector and state law enforcement agencies have significantly increased. Specifically, private companies are communicating with agencies about the security of their facilities and workers and their interactions with representatives of corporate security.[23] This interaction further demonstrates the necessity of private sector participation in fusion centers. The private sector owns the facilities that may be targets of crime, including terrorism, and law enforcement has the information and intelligence regarding the criminal event.

---

22 A complete listing of each of the functional categories and corresponding entities, with examples of the types of information that these entities can provide to fusion centers, can be found in Appendix C.

23 *The Impact of Terrorism on State Law Enforcement*, June 2005, p. 23.

The purpose of this focus group was to identify issues and concerns that should be addressed when fusion centers incorporate the private sector. Several impediments to information sharing by the private sector include the potential for unauthorized release of their information, lack of control of data, possibility of proprietary disclosure, and concerns regarding the information being used to impose civil fines in regulatory areas of government. One of the recurring themes identified by the group was the need for ongoing collaboration between the private sector and fusion centers. In addition, the group acknowledged that the integration of the private sector into fusion centers is a groundbreaking endeavor. To ensure successful integration, a two-way education process was recommended between fusion centers and the private sector.

The focus group also recommended expanding the functional categories initially developed by the Public Safety FCFG to include private sector entities. This expansion will promote comprehensive collaboration within fusion centers. The focus group based the categories on the national Information Sharing Analysis Centers (ISAC) components and added categories, as needed.

Furthermore, the focus group agreed on the need to incorporate private sector subject-matter experts into fusion centers to be utilized routinely or as needed, depending on the size and function of the fusion center. Through this integration, centers will have additional resources to use when threats are developed regarding the private sector. Moreover, subject-matter experts can provide fusion centers with threat assessment results, specifically risks that have been identified for various industries. Another recommendation of the focus group was the development and utilization of Non-Disclosure Agreements (NDA) within fusion centers. Focus Group members felt NDAs would provide the private sector with another level of security when sharing information with fusion center personnel.

Data from the private sector is an important element in the fusion process; it aids in the development of accurate and comprehensive products. Even though there are a variety of industries that fall under this component, the greater the involvement, the greater the success of the fusion center.

Implementation

The private sector can offer fusion centers a variety of resources, including industry-specific subject-matter experts who can provide expertise when specific threats have been identified (e.g., cyber security subject-matter experts can provide assistance relating to computer viruses, worms, and hacking incidents); risk assessment information (e.g., the risks associated with certain private sector operations); suspicious incidents and activity information; and critical infrastructure information (e.g., the location of critical infrastructure nodes, operational interdependencies, building blueprints, and what, if any, hazardous materials are housed there).

When integrating the private sector, the governance body should first assess the private sector environment within the jurisdiction of the fusion center to determine what entities should be incorporated into the fusion centers. Questions that center staff should answer include:

- What private sector associations are within the jurisdiction?

- What industries are located within or affect the jurisdiction?
- What are the major economic drivers and employers in the jurisdiction?
- What industries and critical infrastructure services are essential for emergency services or sustaining quality of life for citizens?
- What groups or associations can collectively represent an industry within the fusion centers (e.g., professional associations)?
- What are past, current, and emerging threats and/or risks that affect the private sector, and which specific entities do they affect?
- What are the "mission critical" entities that should be included in fusion center collaboration (e.g., telecommunications and energy)?
- What entities can provide fusion centers with timely and actionable information to incorporate into the intelligence cycle and the center's operations?
- What private sector entities are currently working with government agencies?

Fusion center leadership should coordinate with regulatory agencies to determine what type of information is available from the private sector and can be provided to, or accessed by, the fusion center. These regulatory agencies have already established working relationships with private sector entities and may aid in private sector participation.

When partnering with fusion centers, the private sector should determine how integration will occur. Will the organization supply full-time personnel to the fusion center, will various private sector entities create a rotating private sector desk, or will private sector entities establish a liaison with the fusion center that will receive and share information?

Once the applicable industries and organizations have been identified, it is recommended that fusion center officials conduct a series of meetings with the private sector entities. Fusion center heads may desire to initially meet with chief executive officers, or their equivalent, to provide an overview of what the fusion center is and the importance of collaboration between the fusion center and the private sector. Once company and organization leaders affirm their commitment to fusion centers, private sector security directors and fusion center managers may discuss the plan of integration, including information requirements; who, if any, personnel, would be located within the fusion center; and their respective needs.

Two-way awareness training between the fusion center and the private sector should be implemented, including an overview of what private sector entities can provide to fusion centers; what fusion centers can provide to the private sector; and the purpose of fusion centers, including the *National Criminal Intelligence Sharing Plan* (NCISP) and the intelligence and fusion processes.

To ensure continued participation, regular meetings should be held with private sector entities to keep them informed of activities of the center. It is imperative that feedback occur when private sector entities provide information to fusion centers. Closing the information loop will aid in continued involvement by all participants.

Guideline 1

Adhere to the National Criminal Intelligence Sharing Plan (NCISP) and other sector-specific information sharing guidelines, and perform all steps of the intelligence and fusion processes.

The NCISP and the Intelligence and Fusion Processes

Justification

After the tragic events of September 11, 2001, law enforcement executives and intelligence experts nationwide agreed that law enforcement agencies must work together to develop the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies. The *National Criminal Intelligence Sharing Plan* (NCISP or Plan) was developed in response to this need.

The NCISP provides model standards and policies, recommends methodologies for sharing classified reports, and recommends a nationwide sensitive but unclassified (SBU) communications capability for criminal intelligence sharing. The Plan is a living document that provides local, state, tribal, and federal law enforcement agencies the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence. It is the blueprint that law enforcement agencies can employ to support their crime-fighting and public safety efforts while leveraging existing systems and networks. The Plan is not a system or a network, nor is it technology-based. It is the framework for the development and sharing of intelligence. It supports collaboration and fosters an environment in which all levels of law enforcement work together to improve the safety of our nation.

The NCISP is founded on the concept of intelligence-led policing and encourages law enforcement agencies to embrace and integrate intelligence-led policing elements in their efforts. Proactive instead of reactive, intelligence-led policing allows law enforcement to:[24]

- Describe, understand, and map criminality and the criminal business process.
- Make informed choices and decisions.
- Engage the most appropriate tactics.

- Target resources.
- Disrupt prolific criminals.
- Articulate a case to the public and in court.

Intelligence-led policing also provides advantages to public safety and private sector components, including trends in criminal activity and increased information sharing with law enforcement to address crime prevention efforts.

Criminal intelligence is the result of a process involving planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation of information on suspected criminals and/or organizations. This sequential process is commonly referred to as the intelligence process (or cycle). There are various models of the intelligence process in use; however, most models contain the basic steps depicted in the following graphic:

The Intelligence Process

---

24   Ronald Bain, "The Dynamics of Retooling and Staffing: Excellence and Innovation in Police Management," Canadian Police College, 2003.

Intelligence Process

The intelligence process is the means of developing raw information into finished intelligence products for use in decision making and formulating policies/actions. The first step, planning and direction, involves identifying the need for data. Agency members should engage in a process of deciding what they want to know (or what they need to collect) before they collect it, or they may obtain indiscriminate, unfocused information.

Collection is the gathering of the raw data needed to produce intelligence products. Data may be collected from many sources, including but not limited to public records, the Internet, confidential sources, incident reports, and periodicals.

The next step, processing and collation, involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined.

Analysis transforms the raw data into products that are useful. This is also the function that separates "information" from "intelligence." It is this vital function that makes the collection effort beneficial. Without this portion of the process, we are left with disjointed pieces of information to which no meaning has been attached. The goal is to develop a report that connects information in a logical and meaningful manner to produce

an intelligence report that contains valid judgments based on analyzed information.[25]

Dissemination is also vital. Without disseminating the intelligence developed, it is pointless to collect it. To be useful, the intelligence disseminated must be timely and credible. Dissemination must also be evaluated based on a right to know and the need to know. The right to know means the recipient has the legal authority to obtain the information pursuant to court order, statute, or decisional law. The need to know means the requestor has the need to obtain information to execute official responsibilities.[26] When dissemination occurs, it is imperative to include all components of fusion centers, including the public safety and private sectors.

The final step involves evaluation/reevaluation of the process performed and the products produced. Evaluation/reevaluation assesses current and new information, assists in developing an awareness of possible weak areas as well as potential threats, and strives to eliminate previously identified weaknesses that have been hardened as a result of the fusion process. Overall, this step provides an opportunity to review the performance or effectiveness of the fusion center's intelligence function.[27]

As previously indicated, fusion centers have improved law enforcement's ability to fight crime and terrorism. Ensuring that each step within the process is followed will facilitate the production of useful intelligence. Nontraditional collectors of information, e.g., the private sector, fire, public works, and public health, are vital to successfully complete the intelligence process. While law enforcement has intelligence information and expertise, the public safety and private sectors have the information systems, processes, and infrastructure that may be targets of crime and terrorism. Further, fusion, through managing the flow of information and intelligence across all levels and sectors of government, integrates the intelligence process to accomplish this sharing. The intelligence process provides a framework for the fused information to be turned into intelligence. Fusion centers utilize the intelligence process to analyze threat-related intelligence and information. These centers are not simply information collection hubs but venues to bring together appropriate partners to prevent crime- and terrorism-related incidents.

The Fusion Process

The stages of the fusion process generally correlate with the intelligence cycle. The Homeland Security Advisory Council's (HSAC) *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report details the stages of fusion and how to implement the process.[28] The first stage, the management and governance stage, establishes the foundation for fusion in that it overviews the need for a

---

25   Bob Morehouse, "The Role of Criminal Intelligence in Law Enforcement." Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., 2000, pp. 1-12.
26   Ibid, p. 9.
27   *The National Criminal Intelligence Sharing Plan*, 2003, p. 7.
28   This report, including a comprehensive explanation of the fusion process, can be found in its entirety in Appendix D.

management structure, who the stakeholders are, and fusion center goals and objectives.

The second stage, planning and requirements development, lays the foundation for the types of information that will be collected. This phase establishes where information will come from and the types of information the fusion center will collect. It also provides collection limitations and privacy issues that affect collection and sharing of information.

Collection is the third stage of the process during which the planning and requirements development stage becomes operational. This is when information is collected from various sources, including law enforcement agencies, public safety agencies (e.g., health, fire, and transportation), and the private sector. This stage is essential for fusion centers to be effective.

The fourth stage, analysis, is similar to the analysis phase in the intelligence cycle in that it is during this stage that the information collected is turned into actionable intelligence. One of the goals of the fusion center during this stage is to identify trends or information that will prevent a terrorist attack or other criminal activity.

The fifth stage is dissemination, tasking, and archiving. During this stage, the information that has been collected and analyzed is then disseminated to stakeholders.

The sixth stage is reevaluation. The purpose of this stage is for the fusion center and stakeholders to ensure that what is being collected, analyzed, and disseminated is factual, timely, and relevant. It is during this stage that tweaks and improvements are made to the fusion process.

The last stage is the modification of the requirements stage (Stage 2). After reevaluation occurs and improvements or changes are identified, this stage allows the improvements to be implemented and the process refined.[29]

Often, gaps in the intelligence process exist. To assist in closing these gaps, the Federal Bureau of Investigation (FBI) developed a template to assist agencies in identifying and tracking intelligence gaps. A summary of the FBI's Intelligence Requirements and a copy of the template can be found in *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Carter, November 2004).[30] A copy of this guide is included on the resource CD. It is recommended that fusion centers create a formal intelligence and information requirements process that prioritizes and guides the intelligence function.

Issues for Consideration

When implementing portions of the NCISP, consider these steps to help establish or enhance an intelligence component of a fusion center:

- Recognize your responsibilities and lead by example.
- Establish a mission statement and a policy to address developing and sharing intelligence data within your agency.
- Connect to your state criminal justice network and regional intelligence databases, and participate in information sharing initiatives.
- Ensure privacy is protected in policy and practice.
- Access law enforcement Web sites, subscribe to law enforcement listservs, and use the Internet as an information resource.[31]
- Provide your agency members with appropriate training on the criminal intelligence process.
- Become a member in your Regional Information Sharing System (RISS) center.
- Become a member of the FBI's Law Enforcement Online (LEO).
- Partner with public and private infrastructure owners and operators.
- Participate in local, state, and national intelligence organizations.
- Participate in the U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN) Program.
- Ensure the fusion center is fully utilizing the jurisdiction's existing networks and information repositories for criminal and hazard information.

Available Resources on Fusion Center CD

- 10 Simple Steps to help your agency become a part of the *National Criminal Intelligence Sharing Plan*
- HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*
- Law Enforcement Intelligence Unit (LEIU) Audit Checklist
- *National Criminal Intelligence Sharing Plan* report

---

29 *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report.
30 Available on the Community Oriented Policing Services (COPS) Web site at www.cops.usdoj.gov/Default.asp?Item=1404.

31 Prior to entering the public Internet as a law enforcement officer or intelligence organization, consult with jurisdiction and department legal advisors to ensure compliance with any policy or regulation concerning law enforcement intelligence use of the Internet for information sharing. Furthermore, using the official government identity and information system for Internet searching can pose a security risk to the agency network and subject of the search. Explore different ways to avoid such risks with competent technical and legal authorities.

Guideline 2

Develop and embrace a mission statement and identify goals for the fusion center.

Mission Statement and Goals

Justification

A mission statement is a written statement of the organization's purpose, such as enhancing public safety, sharing information, or resolving criminal investigations. It is important to have a mission statement because it focuses efforts and is the foundation of all the decisions that follow. A mission statement can also inspire people in the organization and inform customers of the benefits and advantages of what the organization offers and is the first step in educating entities about the center and its services.

If a center has a clear understanding of its short- and long-term goals, it will be easier to integrate efforts. Goals are what you want to accomplish. Objectives are how you are going to get there. Goals should be measurable and observable. They should have specific achievable steps (objectives) with built-in accountability for accomplishment. Goals should be high enough to challenge the center but realistic enough to be attainable. Universal law enforcement goals include four major desired outcomes:

1. The reduction of the incidence of crime.
2. The suppression of criminal activity.
3. The regulation of noncriminal conduct.
4. The provision of services.[32]

Fusion centers will have many demands placed on them, and it is important to have clear priorities. For example, in order to properly develop a mission statement and goals, centers should prioritize tasks such as analytical services, homeland security issues, and investigative support.

Issues for Consideration

When creating a mission statement and goals, consider:

- Developing the center mission statement and goals collaboratively with participating entities as this will create ownership and assist in identifying the primary role(s) of the organization.

- Identifying center customers and their needs and defining center priorities prior to drafting the mission statement and goals.

- Prioritizing the intelligence function to address threats posed in specific fusion center jurisdictions.

- Integrating intelligence-led policing to support customer needs, define tasks, and prioritize functions.

- Utilizing vision statements and/or guiding principles to focus efforts.

- Using the center mission to promote the organization and support grant requests and funding.

- Including the mission statement in the Memorandum of Understanding (MOU) (see Guideline 5).

- Including five to ten points that outline the benefits of public safety and private sector participation in the fusion process.

Elements of Mission Statements

Mission statements should be clear and concise. They should include the primary purpose, priority, and roles of the center. Mission statements should communicate the essence of the organization so that stakeholders and the public are clear on the purpose and intent of the center. Ensure that the mission statement includes the name of the agency or organization, the type of agency, what the agency does, and whom the agency serves. It is critical that the appropriate time and commitment be devoted to developing an adequate mission statement. A good mission statement will provide strategic vision and direction for the center.

Once the mission statement is created and approved, it should not require revision very often. The goals and objectives developed by the center should all be linked to the mission statement. These will be the short-term measures used to gauge whether the center is fulfilling the stated mission. However, if the mission statement becomes inappropriate, irrelevant, or outdated or if the center's direction changes, the mission statement should be revised accordingly.

---

32   www.communitypolicing.org/goal.html.

Example Mission Statements

Upstate New York Regional Intelligence Center (UNYRIC)

To advance the efficient, timely, and accurate exchange of information between all New York state law enforcement agencies. The UNYRIC focuses on all aspects of criminal activity in the 54 counties outside the New York City area and interacts with law enforcement agencies nationwide.

Arizona Counter Terrorism Information Center (ACTIC)

To protect the citizens by ensuring the resiliency of critical infrastructure operations throughout Arizona by enhancing and coordinating counterterrorism intelligence and other investigative support efforts among private sector and local, state, tribal, and federal law enforcement agencies.

Rockland County Intelligence Center (RCIC)

To provide intelligence to law enforcement agencies based upon the collection, evaluation, and analysis of information that can identify criminal activity. This intelligence can be presented in the form of:

- Strategic intelligence, which addresses existing patterns or emerging trends of criminal activity.
- Tactical intelligence, which pertains to a specific event that can be used immediately.

Georgia Information Sharing and Analysis Center (GISAC)

To serve as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence relating to Georgia.

State Terrorism Threat Assessment Center (STTAC)—California

To coordinate the collection of antiterrorism intelligence data, the dissemination of that intelligence to law enforcement agencies, and the use of antiterrorism intelligence resources.

Sample Mission Statements

The following are sample templates that centers may use when developing a mission statement:

The fusion center is a public-private partnership, consisting of local, state, tribal, and federal law enforcement and public safety agencies and the private sector. It acts as an information sharing gateway with the intent to assist law enforcement [homeland security agencies or agencies tasked with homeland security functions] to detect, prevent, and solve crimes.

The fusion center is a public-private partnership among local, state, tribal, and federal law enforcement and public safety agencies and the private sector. It collects, evaluates, analyzes, and disseminates information and intelligence to the law enforcement community [homeland security agencies or agencies tasked with homeland security functions] in a timely, effective, and secure manner.

Available Resources on Fusion Center CD

- *A Staircase to Strategic Planning: Mission*, The Community Policing Consortium, www.communitypolicing.org/mission.html

Guideline 3

Create a representative governance structure that includes law enforcement, public safety, and the private sector.

Governance

Justification

Governance may be defined as the set of organizational regulations and standards exercised by management to provide strategic direction and ensure objectives are achieved, risks are managed appropriately, and resources are used responsibly.[33] Establishing a governance structure creates a supported environment that frames the ability for the center to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy. Governance creates a centralized body to review and endorse issues affecting operations. Members acting as the governance body are ambassadors to the program and carry the message to their agencies and constituents. Governance provides a forum for participants to voice concerns, offer suggestions, and make decisions. It enhances relationships, increases effectiveness, and provides leadership and cohesiveness among participants.

The governance structure ensures an equal opportunity for all participating agencies and users to have ownership in the decision-making process. The governing body should be inclusive to law enforcement, public safety, and private sector partners, thereby ensuring the effectiveness of the fusion center. This can be achieved through assessing the jurisdiction to determine what components, and entities within the components, should be included in the fusion center and governance body. Through the governance structure, agencies can strategically plan for center operations and future enhancements, as well as identify obstacles and offer resolutions.

Issues for Consideration

When creating a governance structure, consider:

- Allowing participants to have input in the establishment of a governance structure composed of law enforcement, public safety, and private sector stakeholders.
- Collaborating with the Joint Terrorism Task Force (JTTF), the Attorney General's Anti-Terrorism Advisory Council (ATAC), the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and other state entities, local authorities, and relevant entities to establish process.
- Composing the governing body of high-level officials who have the power and authority to commit their respective agency's resources and personnel to the center.
- Identifying private sector organizations in the jurisdiction to include in the governance body.
- Establishing an advisory committee composed of private sector leadership, who will provide representation and advice to the governing body.
- Including members from the Information Sharing and Analysis Centers (ISAC).[34]
- Defining the management structure to include what entity oversees the centers, manages the operations, and coordinates daily activities.
- Maintaining a governance structure that is reasonable in size yet ensures representation of all agencies that comprise the center.
- Creating an effective and timely mechanism to communicate decisions made by the governing body to participants and center personnel.
- Evaluating how political issues and climate may impact center support and operations.
- Establishing operational and technical committees.
- Establishing an oversight committee to ensure, among other things, that the intelligence process is properly followed.
- Establishing a privacy committee that will liaise with community privacy advocacy groups to ensure civil rights and privacy protection.
- Developing bylaws for operations of the governance structure.

---

33   Office of Justice Programs (OJP) Web site, www.it.ojp.gov.

34   ISACs are sector-specific centers that coordinate the sharing of terrorism-related information. More information on ISACs can be found at www.dhs.gov.

Committees

Governing bodies may employ committees to help execute and adhere to center policies and procedures, as well as to identify, review, develop, and/or implement new programs or policies. Executive committees set policy, make critical decisions, and commit resources. Operational committees may be asked to focus on specific policies, such as purge and retention or privacy (see Guideline 8). These types of committees may be asked to develop funding strategies or identify grant opportunities. Technical committees will focus on technical standards, critical infrastructure operation, and security. Under these committees, subcommittees may be used to conduct detailed research and analysis, ultimately to bring recommendations to the governing body for review and endorsement.[35]

To aid in the complete integration of the private sector into the governing body, it is recommended that an advisory committee be established. This committee, composed of private sector organizations and associations, will ensure that critical private sector entities, as well as private security managers, are represented both in the fusion center and in the governance structure.

Fusion centers should consider establishing an oversight committee that reports directly to the governance body. This committee will be responsible for providing oversight on the day-to-day operations of the fusion center, including proper utilization of the intelligence and fusion processes.

Example Governance Structures

Rockland County Intelligence Center (RCIC)

The county executive, sheriff, Office of Fire and Emergency Services, and the Police Chiefs Association of Rockland County are permanent members of the governance body for the Rockland County Emergency Operations Center (EOC). In the event of an emergency, the center, operating within the parameters of the National Incident Management System (NIMS), requests additional personnel (health, public utilities, and private security) to respond to the center, as needed. These personnel have been previously identified and trained as center representatives and are utilized based on the type of emergency, e.g., public health, terrorism, or weather-related.

The RCIC Oversight Committee is comprised of police chiefs chosen by the Rockland County Police Chiefs Association (local representatives), the county sheriff, and district attorney (county representatives).

All agencies represented in both the EOC and the RCIC meet on a regular basis to discuss areas of concern and work collectively to enhance the effectiveness of law enforcement and the county's emergency preparedness initiatives.

Iowa Law Enforcement Intelligence Network (LEIN)

Iowa LEIN is governed by a seven-member executive board, six of whom are local law enforcement officers who are elected annually by their fellow LEIN members from across the state. The seventh member and chairperson of the executive board is the state LEIN coordinator (a special agent with the Iowa Department of Public Safety's Intelligence Bureau).

## State Terrorism Threat Assessment Center (STTAC)—California

The State Terrorism Threat Assessment Center (STTAC) is a partnership of the California Department of Justice, the California Highway Patrol, the California Office of Homeland Security, and other state and federal agencies. It provides statewide assessments, information tracking, pattern-analysis products, and geographic report linkages, as well as regional investigative support throughout the state. It also provides California's senior leaders with situational awareness of identified threats along with constant access to the latest local, state, and national intelligence products.

To complement the STTAC, California has created four mutually supporting Regional Terrorism Threat Assessment Centers (RTTAC). Their areas of responsibility mirror those of the four Federal Bureau of Investigation (FBI) Field Offices in the state. In some cases, they are colocated with the FBI's Joint Terrorism Task Forces to help minimize reporting conflicts, while facilitating the coordination of information among the STTAC, RTTACs, and the FBI.

Governance Template

The following example offers centers a starting point for developing a governance structure. Figure 3 illustrates a three-tiered approach. The bottom level represents staff members assigned to perform the fusion/intelligence process and provide investigative support. These members may come from a variety of agencies and represent the core of center operations. Here, data integration and analysis will take place. Personnel may include intelligence analysts and officers. The middle section represents the day-to-day management of the center. It also includes administrative staff, such as computer support staff and

Figure 3—Fusion Center Governance Structure Example

---

35   Kelly J. Harris, *Governance Structures, Roles and Responsibilities*, September 2000 (Updated/Reissued 2004).
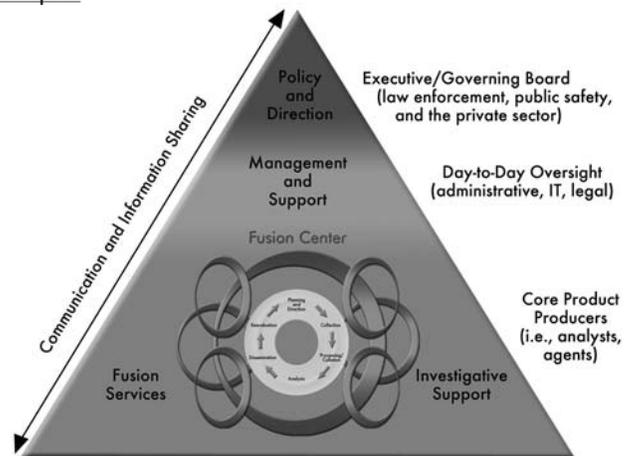
legal services. In some cases, this section may include a facility manager. The top section represents policy and direction. This section is smaller, indicating a select group of individuals from each participating entity who have been designated as part of the governing structure or board. The illustration shows information flowing top down and bottom up.

Developing Bylaws

According to *The Legal Guide for Association Board Members*, bylaws are defined as "an important association corporate legal document that constitutes the agreement between the association and its members. Properly drafted bylaws set forth the essential organizational and operational provisions governing the association."[36] Bylaws are just one example of a governing mechanism that a center may utilize to enforce organizational rules. A bylaws sample document is provided on the resource CD.

Parliamentary Procedures

The governance board may want to make use of parliamentary procedures to create an effective governing process. Procedures such as *Robert's Rules of Order* can be very helpful in introducing, debating, and deciding on issues. There are a number of Web sites, such as www.rulesonline.com that contain the full text and/or summary information regarding *Robert's Rules of Order* and parliamentary procedures.

Available Resources on Fusion Center CD

- Bylaws Sample Template
- Board Guidelines, www.mapnp.org/library/boards/boards.htm
- Global Justice Information Sharing Initiative Advisory Committee Bylaws, http://it.ojp.gov/documents/GACBylaws.pdf
- Organization and Association Resource List
- Parliamentary Procedures, www.rulesonline.com

---

36   James G. Seely, *The Legal Guide for Association Board Members*, Schneider, 1995, p. 71.

Guideline 4

Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety, and the private sector.

Collaboration

Justification

To maximize intelligence sharing, all levels of law enforcement and public safety agencies and the private sector must communicate and collaborate. The objective is to leverage resources and expertise while improving the ability to detect, prevent, and apprehend terrorists and other criminals. Fostering a collaborative environment builds trust among participating entities, strengthens partnerships, and provides individual as well as a collective ownership in the mission and goals of the center. The *National Criminal Intelligence Sharing Plan* speaks to this as well: "Sharing is founded upon trust between the information provider and the intelligence consumer. Such trust is most often fostered on an interpersonal basis; therefore, law enforcement task forces and other joint work endeavors succeed where colocated, interspersed personnel from different agencies and job types convene for a common purpose."[37]

Fostering a collaborative environment is not only important to sharing, collecting, developing, and disseminating intelligence but also to sharing decisions and ownership. It discovers solutions and expands capacity. In an environment where some resources are decreasing while demands are increasing, collaboration has become even more essential. The purpose of collaboration is to increase capacity, communication, and continuity of service while decreasing duplication.[38] A key to the success of fusion centers is to ensure that feedback occurs between the fusion center and the entities that provide information and intelligence. Inherent in a collaborative environment is two-way communication; entities that provide information to fusion centers should also receive information from fusion centers. This will result in buy-in from all participants and will aid in the success of the information sharing environment. Fusion centers should also continually seek outreach opportunities to ensure that public safety agencies and the private sector are represented, thereby meeting the needs of their constituents.

Successful collaboration is contingent upon a trusting environment. Fusion centers should seek to establish an information sharing system that aids in collaboration, while ensuring the security of the information within the system and the system itself. This environment should also be equipped to handle various types of information that public safety and the private sector submit, including public, sensitive, proprietary, and secret information. This environment may include e-mail, a virtual private network, a secured Internet site, listservs, or face-to-face meetings. Collaboration begins with interpersonal relationships, and fusion centers should institutionalize these relationships through ongoing dialogue and information sharing. Issue-based collaborative techniques may be utilized by the fusion center when a specific threat is identified. These techniques allow the private sector to change its participation within the fusion center, based on the identified threat. For example, a transportation entity may have a liaison in the fusion center, but if a threat is identified that affects transportation, that organization may provide full-time participation until the threat is neutralized.

There are a variety of public safety and private sector entities to include in fusion centers. Each jurisdiction has different needs, and collaboration will be based on these needs. Fusion centers should seek to network with various public safety and

---

37   *National Criminal Intelligence Sharing Plan*, November 2004, p. 9.
38   C. R. Pete Petersen, M.Ed., "Community Collaboration," March 4, 2003, www.communitycollaboration.net.

private sector organizations and associations. The greater the effort by the fusion center, the greater the incorporation and partnership with public safety and the private sector. Examples of these organizations and associations include InfraGard, Sector Coordinating Councils (SCC), [39] Information Sharing and Analysis Centers (ISAC),[40] and the United States Public-Private Partnership (USP3).[41] Overarching functional categories have been developed in which individual agencies, companies, and organizations can be grouped together. Though not comprehensive, these categories and accompanying entities serve as a foundation and will aid fusion centers in determining what entities should be involved in the center. Governance bodies should identify the needs and vulnerabilities, organizations with a large employee base, and major economic drivers within the jurisdiction of the fusion center. The goal is to determine what entities should participate and be integrated into the fusion center. To ensure the effectiveness of collaboration within the fusion center, lines of communication should be established with the various entities that make up the categories according to the needs of the fusion center and jurisdiction. A list of the functional categories and associated entities is located in Appendix C of this report.

An example of effective collaboration is the Texas Coastal Region Advisory System (TCRAS). TCRAS is a Joint Terrorism Task Force (JTTF) initiative and is used to quickly disseminate information to law enforcement partners, as well as other companies and agencies that are responsible for critical infrastructure operations in the area.[42] TCRAS demonstrates an effective information sharing environment that incorporates the law enforcement, public safety, and private sector components of a fusion center.

Issues for Consideration

Collaboration Principles

A successful collaboration must continually provide value to its participants, customers, and constituency. To foster and enhance collaboration, consider implementing the following principles:

- Maintaining a diverse membership to include representatives from local, state, tribal, and federal law enforcement; all sectors of public safety; and key private sector companies and organizations.

- Including private sector associations when incorporating the private sector. Two examples are FloridaFirst and ChicagoFirst, banking coalitions created to work with government agencies to help financial institutions prepare for national disasters and terrorism.[43]

- Utilizing a phased approach when integrating private sector entities to accurately identify and address the needs of the entities.

- Developing and participating in networking groups and organizations that exist locally, regionally, statewide, nationally, and internationally.

- Working with JTTF, Anti-Terrorism Advisory Council (ATAC), the U.S. Department of Justice (DOJ), DHS, other state and local entities, and other relevant organizations or groups.

- Compiling a contact list of public safety and private sector representatives, including after-hours numbers.

- Conducting regular meetings for the purpose of collaboration and information sharing.

- Establishing procedures for maintaining the continuity of personal, organizational, and institutional relationships.

- Educating and training the law enforcement, public safety, and private sector communities on the intelligence and fusion processes and fusion center operations.

- Educating and liaising with elected officials, private sector executives, and other community leaders to promote awareness of the fusion center functions.

- Ensuring feedback to entities that provide information to fusion centers (e.g., the results of the information that has been provided to the fusion center).

- Ensuring, at a minimum, contact information is collected and up to date for mission critical entities (e.g., utilities, public works, and telecommunications).

Available Resources on Fusion Center CD

- "Community Collaboration," www.communitycollaboration.net

---

39   The roles of Sector Coordinating Councils (SCC) are to serve as a single forum into the respective sector for the entire range of homeland security issues; institutionalize the sector's coordination of policy development, sector-wide strategy, and planning; ensure program promulgation and implementation; monitor sector progress; provide provisions of best practices and guidelines; develop requirements for information sharing, research, and development; and serve as the point of cross-sector coordination (*Homeland Security Information Sharing Between Government and the Private Sector*, August 10, 2005, p. 17).
40   Additional information on SCCs and ISACs can be found at www.dhs.gov.
41   The United States Public-Private Partnership (USP3) (formerly known as the U.S. Department of Homeland Security's (DHS) HSIN-CI) was implemented as a DHS program that is regionally administered and governed by its private and public members. Current membership is approximately 40,000, ninety percent of which are from the private sector, who are actively using the programs vertical and horizontal information sharing strategies for local, regional, and national routine information sharing and all-hazards 24/7 alerts and warnings. Due to its success, DHS and the Federal Bureau of Investigation (FBI) will continue to jointly sponsor and grow the program nationally, with a goal of 200,000 members.
42   Additional information on TCRAS can be found at www.tcras.org.

---

43   Jim Freer, "Banks Band Together," *The South Florida Business Journal*, October 2005, www.bizjournals.com/southflorida/stories/2005/10/17/daily1.html.

Guideline 5

Utilize Memorandums of Understanding (MOUs), Non-Disclosure Agreements (NDAs), or other types of agency agreements, as appropriate.

Memorandum of Understanding (MOU) and Non-Disclosure Agreement (NDA)

MOU

It is recommended that fusion centers be governed and managed in accordance with an MOU. An MOU, a necessary tool for information sharing, defines the terms, responsibilities, relationships, intentions, and commitments of each participating entity; the agreement also provides an outline of the who, what, where, when, why, and how of the project. Partners should commit to the program policies by signing the MOU. In addition to MOUs, some initiatives utilize agency, individual, and data sharing user agreements.

Issues for Consideration

When negotiating and drafting MOUs, consider:

- Identifying and understanding the legal and practical implications of the MOU.
- Defining the roles and responsibilities of the participating agencies.
- Embracing and encouraging trusted relationships.
- Including language requiring that all assigned personnel maintain access to their own agency's data.

Example MOUs

At a minimum, include the following elements in the MOU:

- Involved parties
- Mission
- Governance
- Authority
- Security
- Assignment of personnel (removal/rotation)

- Funding/costs
- Civil liability/indemnification issues
- Policies and procedures
- Privacy guidelines
- Terms
- Integrity control
- Dispute resolution process
- Points of contact
- Effective date/duration/modification/termination
- Services
- Deconfliction procedure
- Special conditions
- Protocols for communication and information exchange
- Protocols for background checks on fusion center participants

NDA

The fusion center determines risks to the private sector and analyzes suspicious activity information. This function requires the sharing of sensitive information from the private sector to the fusion center. To aid in sharing this sensitive information, a Non-Disclosure Agreement may be used. The NDA provides private sector entities an additional layer of security, ensuring the security of private sector proprietary information and trade secrets. The development of an NDA and a clear understanding of what it does and does not cover are critical to private sector participation.

One of the functions of the NDA is to provide a mechanism for fusion center leadership, participants, and personnel to protect information. NDAs will vary by jurisdictions, based on the types of private sector entities participating in the fusion center. Centers should specify the types of information covered in an NDA, e.g., strategic and risk assessment information. Tactical information, such as suspicious activity reports, should not be included in an NDA because this information may be shared with law enforcement outside of the fusion center (e.g., the Joint Terrorism Task Force (JTTF), Field Intelligence Group, the state police, or other appropriate agencies). Information that the

private sector may not want disseminated should be specified in the NDA. This information may include trade secret information (critical to a business operation), proprietary information (customer lists, throughput rates), and sensitive security information (guard schedules, site plans, security plan access). In addition, fusion centers should specify how this information is protected when creating an NDA. Subject-matter experts may provide fusion centers with intelligence related to their respective sectors without disclosure of trade secrets or proprietary information. But if this type of information is provided, fusion centers should be sensitive to the storing of the information without approval from the providing entity.

NDAs do not supersede public records laws or legal processes. Therefore, fusion centers should be cognizant of local, state, and federal public records laws that may supersede an NDA, such as state sunshine laws, the Freedom of Information Act (FOIA), and federal and state privacy laws and requirements. If the center has a legal committee, this committee should be able to provide input into the development and use of an NDA. In addition, it is recommended that fusion centers and their leadership encourage appropriate policymakers to legislate the protection of private sector data provided to fusion centers.

Issues for Consideration

When developing an NDA, consider:

- Identifying and understanding the legal and practical implications of an NDA.
- Defining what information will be treated as confidential.
- Specifying what entities can receive confidential information.
- Indicating how long the NDA will be in effect.
- Identifying the types of information that the NDA will cover.
- Identifying repercussions for violation of the NDA.
- Clearly specifying local, state, and federal public records laws within the NDA.

- Specifying what information should be shared and protected (e.g., proprietary and trade secrets).
- If trade secrets or proprietary information is provided, an NDA may include the following caveats:
  - ✓ The information being provided is owned by the private sector partner and is provided for a limited purpose of determining a specific risk associated with the entity.
  - ✓ It is the private sector partner's responsibility to identify the information as proprietary.
  - ✓ Fusion centers should take into account local, state, and federal FOIA laws in an effort to ensure that information identified as proprietary may not be disclosed beyond the immediate recipient group without written consent of the providing private sector partner.

Available Resources on Fusion Center CD

- 28 CFR Part 23 Sample MOU
- Arizona Counter Terrorism Information Center MOU
- California Public Records Exemption
- Canada Department of Defense (DOD) MOU Guidelines
- DHS Non-Disclosure Agreement, www.fas.org/sgp/othergov/dhs-nda.pdf
- Florida Statute 119.071
- Freedom of Information Act, www.usdoj.gov/04foia
- Joint Terrorism Task Force MOU
- Massachusetts Statute
- MOU Sample Template
- Rockland County Intelligence Center MOU
- Upstate New York Regional Intelligence Center MOU

Guideline 6

Leverage the databases, systems, and networks available via participating entities to maximize information sharing.

Database Resources

Justification

During the focus group process, participants reviewed a number of information and intelligence sharing initiatives. Most of the initiatives have access to some local, state, and federal databases, as well as other organizations or data sets. Centers may want to evaluate the types of databases that participating agencies have available. Gaps should be identified and researched. Leveraging the databases and systems available via participating entities will help maximize information sharing. This is an opportunity to access previously unavailable information. It is recommended that ownership and control of law enforcement information shared through the center remain with the originating agency. Data owners should be responsible for the quality of data shared. Access to data can be controlled in a variety of

ways, including fusion center leadership controlling who has access or data originators controlling access levels. For more information about the security of data, see Guideline 9 (Security). Another option is for the center to house their information. If a center chooses this option, it is important for the necessary policies and procedures to be in place to govern use and access.

Fusion centers should consult with public safety and private sector personnel to determine if any information sharing databases may be available within their respective jurisdictions. Special consideration should be given to the development of policies and procedures that ensure public safety and private sector information is not combined with federal data that contains personally identifiable information, and when a criminal predicate, threat, or public safety need is identified, access to this information will be virtual through networking and utilizing a search function. Additionally, fusion center participants should ensure compliance with all local, state, and federal privacy and civil liberties laws and statutes.

Issues for Consideration

When accessing databases, consider obtaining access to a variety of databases and systems, such as:

- Driver's license
- Motor vehicle registration
- Location information (411, addresses, and phone numbers)
- Law enforcement databases
- National Crime Information Center (NCIC), Nlets–The International Justice and Public Safety Information Sharing Network, and the Terrorist Screening Center (TSC)
- Criminal justice agencies
- Public and private sources (Security Industry databases, Identity Theft databases, Gaming Industry databases)
- Regional Information Sharing Systems (RISS)/Law Enforcement Online (LEO), U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), including the United States Private-Public Partnership (USP3)—formerly HSIN-CI. (Note: RISS, LEO, and DHS's HSIN are currently collaborating on a network capability.)

- Organizational and association resources (InfraGard, The Infrastructure Security Partnership)[44]
- Corrections
- Sex offender registries
- Violent Criminal Apprehension Program (VICAP)
- Health- and Public Health-Related Databases (Public Health Information Network, Health Alert Network)

Also important are such issues as:

- Controls and safeguards for data access levels
- Technical specification of databases (structured/unstructured data)
- Identification and leveraging of partner resources
- Ownership of the data in the fusion center
- Data quality and data reliability

System/Network Resources

The following are available resources for law enforcement entities. This list is not meant to be all inclusive. Additional resources and Web sites may exist to assist fusion centers.

El Paso Intelligence Center (EPIC)—EPIC established a Southwest Border Intelligence Service Center with a concentration on drug movement and immigration violations. Members of EPIC have access to a wide range of intelligence, including information from the U.S. Drug Enforcement Administration and U.S. Immigration and Customs Enforcement (ICE). www.usdoj.gov/dea/programs/epic.htm

Federal Bureau of Investigation's (FBI) LEO Program—LEO is a national, interactive computer communications system and information service, an intranet exclusively for the law enforcement community. www.fbi.gov/hq/cjisd/leo.htm

FBI's National Date Exchange (N-DEx)—N-DEx will provide the first implementation of structured search and index capabilities for the U.S. Department of Justice's (DOJ) Law Enforcement Information Sharing Program. All kinds of data (e.g., structured, full-text, multimedia) will be available through N-DEx, although searching, matching, and linking will only be possible on well-defined entities (people, vehicles, locations, weapons, phone numbers, etc.), not arbitrary text (full-text data). The initial focus is on structured incident data but will be expanded to other structured data (extracted entity data from full-text documents). N-DEx's focus is on large agencies and aggregated data sources, such as RICs, but will expand to any law enforcement agency.

---

44 The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI concerning various counterterrorism, counterintelligence, and criminal matters. This information sharing is accomplished by 84 InfraGard chapters that are linked with the 56 FBI field office territories and their FBI Special Agent Coordinators. Any critical infrastructure owners and operators can join InfraGard and participate in local chapter training and education initiatives; receive sensitive, unclassified information updates; and participate in meetings. All InfraGard applicants must submit to a records check, including a criminal history check, prior to becoming a member, in order to ensure the program is composed of well-intentioned, law abiding citizens. For more information, visit www.infragard.net.

FBI's Regional Data Exchange (R-DEx)—R-DEx provides an interface to Regional Intelligence Centers (RICs) to enable searching of unstructured documents and for retrieving matching documents. R-DEx serves two main functions: providing RICs with access to DOJ's data and enabling a RIC's user to perform full-text searches over DOJ unstructured documents for the region, in addition to the state and local documents accessed internally.

Financial Crimes Enforcement Network (FinCEN)—FinCEN supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. Its objective is to provide United States policymakers with strategic analysis of domestic and worldwide money-laundering developments, trends, and patterns. FinCEN controls over 150 million reports filed under the Bank Secrecy Act and other similar laws. www.fincen.gov

High Intensity Drug Trafficking Areas (HIDTA)—This program provides federal funds to problem areas to help eliminate or reduce drug trafficking and its harmful consequences. Analysts at HIDTA centers have access to a variety of databases and systems that are available to law enforcement. www.whitehousedrugpolicy.gov/hidta/index.html

Homeland Security Information Network (HSIN)—HSIN provides a secure Internet-based technology that allows real-time information sharing at the sensitive but unclassified level. It is the collaborative system used by the DHS Operations Center to collect and disseminate information between DHS and local, state, tribal, and federal agencies involved in combating terrorism. HSIN also includes public safety and private sector connectivity (USP3), homeland security, and other information. Access to secret information will be available in the near future on HSIN-Secret. www.dhs.gov/dhspublic/display?content=3350

International Association of Crime Analysts (IACA)—IACA helps crime analysts around the world improve their skills and make valuable contacts, helps law enforcement agencies maximize use of crime analysis, and advocates for standards of performance and technique within the professions. www.iaca.net

International Association of Law Enforcement Intelligence Analysts (IALEIA)—IALEIA's mission is to professionalize analysis in law enforcement, the military, and private industry. IALEIA has published a number of booklets and holds major conferences, local or regional chapter meetings, and training sessions. www.ialeia.org

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 criminal/fugitives and stolen properties. www.usdoj.gov/usncb

Law Enforcement Intelligence Unit (LEIU)—The purpose of LEIU is to record and exchange confidential criminal information on organized crime not previously available through regular police communication channels. Membership in LEIU is open

to local or state law enforcement agencies having a criminal intelligence function. The applicant must be sponsored by a current member. LEIU may be reached at the State Terrorism Threat Assessment Center, Bureau of Investigation, Intelligence Operations Program, Central Coordinating Agency, Post Office Box 163029, Sacramento, California 95816-3029. www.leiu-homepage.org/index.php

National Crime Information Center (NCIC)—NCIC is a nationwide information system that links together local, state, tribal, and federal criminal justice agencies. NCIC's capabilities include an enhanced name search, fingerprint searches, information on persons on probation or parole, a convicted sex offender registry, and a registry of individuals incarcerated in the federal prison system. www.fbi.gov/hq/cjisd/ncic.htm

National Drug Intelligence Center (NDIC)—The NDIC supports national policy and law enforcement decisions with timely strategic domestic drug intelligence assessments, focusing on the production, trafficking, and consumption trends and patterns of all illicit drugs inside United States national borders and territories. www.usdoj.gov/ndic

National White Collar Crime Center (NW3C)—NW3C provides a national support network for local and state law enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime. NW3C is a member-affiliated organization comprised of law enforcement agencies, state regulatory bodies, and local and state prosecution offices. Support services are offered in five main categories: economic and computer crime training, intelligence and analytical services, case funding for designated cases, research, and fraud-compliant referral and analysis through its National Fraud Complaint Management Center/Internet Fraud Complaint Center. www.nw3c.org and www.training.nw3c.org

Nlets—The International Justice and Public Safety Information Sharing Network—Nlets is an interstate law enforcement network for the exchange of law enforcement and related justice information. www.nlets.org

RISS Automated Trusted Information Exchange (ATIX)—RISS ATIX™ provides users with secure interagency communications and information sharing resources for exchanging public safety and law enforcement information. www.rissinfo.com/rissatix.htm

RISSNET™—RISSNET provides the six RISS centers with a secure criminal intelligence network for communications and information sharing by local, state, tribal, and federal law enforcement agencies. www.rissinfo.com

Guideline 7

Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems. Use the U.S. Department of Justice's (DOJ) Global Justice Extensible Markup Language (XML) Data Model (Global JXDM) and the National Information Exchange Model (NIEM) standards for future database and network development, and consider utilizing the Justice Information Exchange Model (JIEM) for enterprise development.

Interconnectivity

Justification

Law enforcement entities must communicate. The ultimate goal is to eliminate barriers to communications and intelligence development and exchange. Communication barriers come in a number of forms—e.g., incompatible or disparate computer systems, lack of trust, lack of interoperability, lack of a common terminology, and lack of funding. Centers should establish formal protocols (policies and procedures) and standards to enhance communications, as well as create effective and efficient vehicles for exchanging information. Center personnel and leadership should communicate frequently and be responsive to the needs, concerns, and ideas of both internal and external partners. The information contained in this guideline pertains to verbal, written, and electronic communications.

It is recommended that fusion centers leverage existing systems and those currently under development and allow for future connectivity to other state, local, tribal, and federal systems. Furthermore, centers should be aware of and educated on Global JXDM. Any new database development should be Global JXDM-compliant and meet existing standards. It is important to note that

DOJ and the U.S. Department of Homeland Security (DHS) are integrating the use of Global JXDM into grant recipient criteria.

Global JXDM is a comprehensive product that includes a data model, a data dictionary, and an XML schema that is sponsored by DOJ. Its development is supported by the Global XML Structure Task Force (GXSTF), which works closely with researchers at the Georgia Tech Research Institute (GTRI). The Global JXDM is an 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. The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, Global JXDM enables access from multiple sources and reuse in multiple applications.

Issues for Consideration

- When establishing connectivity and communications, consider:
- Striving for compatibility not commonality.
- Including both technical and managerial portions of connectivity.
- Using Web-enabled technology when available.
- Using a distributed structure when appropriate.
- Developing mechanisms to communicate internally with participating agencies.
- Developing a policy to ensure proper communication with leaders and policymakers, the public and private sector, media, and citizens.
- Ensuring secure and redundant communications.
- Establishing an electronic notification capability for fusion center participants.
- Maintaining a stand-alone security system (mobile).
- Implementing a communications plan.

- Identifying the requirements for private sector and public safety systems and networks.
- Adhering to need-to-know/right-to-know stipulations.
- Developing outreach material to help increase awareness among policymakers, media, and citizens.
- Conducting training on proper communication and center policy.
- Meeting regularly with personnel and offering intelligence exchange sessions.
- Remembering that communication goes beyond just in-house communication.
- Incorporating the protocols for communication and information exchange in the MOU (Guideline 5).

Justice Information Exchange Model

It is important to document and analyze information exchange at the planning stage of a project and to create a blueprint at the enterprise level (among agencies, levels of government, and a variety of disciplines) for electronically sharing data that capitalizes on efficiency, accuracy, and timeliness. This is regardless of whether interfaces between systems for sharing intelligence consist of simple queries and responses or are more sophisticated transactional processes that build central index entries or populate data warehouses. This design should be created by business experts from the participating organizations, under the direction of policy leaders and with the assistance of technologists. It should be based on a disciplined examination of current business practices, existing technology, and paper and electronic exchange of intelligence that already is occurring.

The Justice Information Exchange Model (JIEM) can assist fusion centers in performing these important tasks. Created by SEARCH, The National Consortium for Justice Information and Statistics, and supported by the Office of Justice Programs' (OJP) Bureau of Justice Assistance (BJA), JIEM documents the processes, triggering events, and conditions that govern information exchanged at the enterprise level. It models the data that flows or should flow between organizations. JIEM was developed to collect requirements from practitioners for justice information sharing initiatives, specifically to assist justice system leaders in analyzing and documenting existing information exchange at the enterprise level. JIEM was also developed to assist in designing new electronic exchange processes as a part of an integrated justice initiative and in adopting and implementing national business, data, and technology models to save time, effort, and money. It is a conceptual framework that presents the flow of information between agencies, defines the key events that trigger the need to share information, identifies the agencies involved in the exchange, and describes the nature of the information exchange, irrespective of whether one is analyzing a justice or nonjustice system exchange. JIEM helps justice and public safety practitioners to articulate requirements that can be communicated to technologists who develop systems and interfaces.[45]

JIEM is linked with DOJ's Global JXDM, allowing easy importing of model components to design electronic documents. Soon it will be linked with the ability to import and export XML schema and other Information Exchange Package Documentation (IEPD) artifacts that are essential to implementing the Global JXDM. This will eventually enable justice agencies to seamlessly generate (and, if need be, regenerate) Global JXDM-compliant information exchanges from the business rules encapsulated in JIEM, ensuring that they can be rapidly adapted to the needs of an increasingly dynamic environment. JIEM is also being enhanced to support the exchange of information; not only within domains (as in the justice domain today) but between different domains, such as justice, emergency management, transportation, and intelligence; in support of emerging organizations, such as fusion centers.[46]

National Information Exchange Model

The U.S. Department of Justice's (DOJ) Office Justice Programs' (OJP) Bureau of Justice Assistance (BJA) is collaborating with DHS to utilize the Global JXDM as the base for the deployment of the National Information Exchange Model (NIEM). NIEM will provide the foundation and building blocks for national-level interoperable information sharing and data exchange that will integrate the public safety and private sector entities to the already established law enforcement information exchange. The tentative date for NIEM to be operational is October 2006.[47]

In addition to NIEM and JIEM, other options for interconnectivity include developing and utilizing a secure Internet site to post alerts, calendars that may include training information and significant dates, and a chat interface. Another option is a Web portal to connect the fusion center with private sector and public safety partners that will allow for a single sign-on and can provide situational awareness reports, threats, and warnings. It also has the capability for e-mail notifications. Interconnectivity also includes face-to-face communication, including regular meetings with other intelligence centers to share information and intelligence. Interconnectivity aids in institutionalizing the relationships between the fusion center and the public safety and private sector partners. However, fusion centers and their partners should be aware of privacy issues when developing information sharing networks, systems, or Web sites.

Distributed Versus Centralized Systems

Currently, both distributed and centralized systems are being used successfully for law enforcement information and intelligence sharing. There are benefits and challenges to both models.

A distributed model allows participating entities to control their data. Data is not commingled or housed in a data warehouse. Agencies are responsible for the quality of the data and the accessibility of their information. The distributed structure can streamline policy development and minimize privacy concerns, while providing the same functionality as a centralized model.

---

45   Additional information on JIEM can be found at www.search.org/programs/info/jiem.asp.

46   The SEARCH report, *Information Exchange Analysis and Design*, can be found in Appendix E of this report.

47   For more information on NIEM, visit www.niem.gov.

The distributed model is also reliable and can maximize resources. Distributed systems are scalable and offer aggregate computer power. However, security issues, resource distribution, demand, and computing power can limit the distributed model.[48]

A centralized system places all information in one location. Collection of information and refreshing of data can be complicated with a centralized structure. However, often the functionality of the centralized system is greater and allows for increased speed.

A white paper prepared by the Integrated Justice Information Systems (IJIS) Institute provides a comparative analysis of the distributed and centralized system based on five components: cost, governance and data ownership, performance and functions, scalability, and security and privacy. This document is included on the resource CD. Centers should evaluate both structures to determine the best fit. As described above, it is the recommendation of the *Fusion Center Guidelines* that systems can be distributed or centralized; however, federal data that contains personally identifiable information should be separate from other types of information the fusion center receives, including public safety and private sector information.

Service-Oriented Architecture

Information sharing is a long-standing practice among justice agencies, particularly within the law enforcement community. As society becomes more mobile, the importance of sharing data to improve police effectiveness grows exponentially. The Web and the technologies that support it have enabled information sharing to go beyond exchanges among specific partners to embrace the whole of the justice community. This includes law enforcement, prosecutors, defense counsel, courts, probation, and corrections, and a host of corollary disciplines, such as homeland security, fire, emergency services, health, education, transportation, and motor vehicle licensing. Service-oriented architecture (SOA) incorporates six fundamental principles for the sharing of information in the criminal justice community:

- The architecture must recognize innumerable independent agencies and funding bodies from the private sector through local, state, tribal, and federal governments.
- Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions.
- The infrastructure must be able to accommodate an infinite range of scales, from small operations with few participants in a rural county to national processes that reach across local, state, tribal, federal, and even international boundaries.
- Information sharing must occur among data sources that differ widely in software, hardware, structure, and design.
- Public sector technology investment must reflect and incorporate the lessons and developments of the private sector.
- The infrastructure design must be dynamic, capable of evolving as the information sharing requirements change and the technology is transformed.

This concept of design allows the original data owners to control

their own data, both in terms of who is allowed to access it and in ensuring the integrity of the data. It allows agencies to retain the investment they have made in their existing systems and at the same time gain access to valuable information contained in other agency systems. It uses the technology of the Internet, which is user-friendly and readily understood by most.

In 2004, DOJ's Global Infrastructure/Standards Working Group (GISWG) published a document entitled *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA).* Based on the report, Global recognizes that SOA is the recommended framework for development of a justice information sharing system. The report indicates that a system should be designed and developed around the basic components of the operational procedures or business practices of an agency. These components are then combined into a larger, loosely related structure that, in turn, can be combined into an even larger entity. The SOA design must be available to all agencies and support the evolution of change and new technology, with support for start-up, maintenance, and future upgrades to the information sharing systems that are based on the SOA framework. A complete copy of the report is contained on the accompanying resource CD.

Organization for the Advancement of Structured Information Sharing Systems (OASIS)—Ratified Common Alerting Protocol (CAP)

It is recommended that, where possible, fusion centers use the OASIS-ratified CAP to enable the exchange of emergency alert and public warning information over data networks and computer-controlled warning systems. Using CAP also adds an element of redundancy to the systems and networks. By limiting transport-specific nomenclature, CAP remains fully compatible with existing public warning systems, including those designed for multilingual and special-needs populations, as well as with XML applications, such as Web services. CAP data elements have been incorporated in DOJ's Global JXDM. Other agencies, such as DHS's Federal Emergency Management Agency (FEMA), have embraced the CAP and are in the process of integrating it into all alert and warning systems.

Available Resources on Fusion Center CD

- *A Critical Look at Centralized and Distributed Strategies for Large-Scale Justice Information Sharing Applications* (a white paper prepared by the IJIS Institute)
- *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*, http://it.ojp.gov/ documents/200409_Global_Infrastructure_Report.pdf
- Global Justice XML Data Model (Global JXDM), www.it.ojp. gov/gjxdm
- Justice Information Exchange Model, www.search.org/ programs/info/jiem.asp
- Model Intelligence Database Policy

---

48   Texas A&M University Computer Science Department. Introduction to Distributed Systems, 2001.

Guideline 8

Develop, publish, and adhere to a privacy and civil liberties policy.

Privacy and Civil Liberties

Justification

The *National Criminal Intelligence Sharing Plan* (NCISP) stresses the need to ensure that constitutional rights, civil liberties, civil rights, and privacy are protected throughout the intelligence process. In order to balance law enforcement's ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be in place.

Process

Privacy and civil liberties protection should be considered in the planning stages of a fusion center. As systems are designed, analysis should be made and protections should be developed for personally identifiable information to ensure its protection.

DOJ's Global Justice Information Sharing Initiative (Global) has developed the *Privacy Policy Development Guide* and the *Privacy and Civil Rights Policy Template for Justice Information Systems* to aid justice practitioners with developing or revising an agency's privacy policy. Furthermore, the guide assists agencies in articulating privacy obligations in a manner that protects the justice agency, the individual, and the public and makes it easier to do what is necessary—share critical justice information. These documents are contained as attachments to the guidelines.

The Global documents utilize, and any fusion center should consider, the Fair Information Practices which are the accepted baseline for privacy protection worldwide. The following is a summary of the Fair Information Practices:

1. **Collection limitation principle**. There should be limits to the collection of personal data, and any data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data quality principle**. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date.

3. **Purpose specification principle**. The purposes for which personal data is collected should be specified no later than at the time of data collection. Its subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use limitation principle**. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Principle 3 except (a) with the consent of the data subject or (b) by the authority of law.

5. **Security safeguards principle**. Personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure.

6. **Openness principle**. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual participation principle**. An individual should have the right to (a) obtain confirmation of whether or not the data controller has data relating to him; (b) have the data related to him within a reasonable time, cost, and manner and in a form that is readily intelligible to him; (c) be given an explanation if a request made under (a) and (b) is denied and be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. **Accountability principle**. A data controller should be accountable for complying with measures that give effect to the principles stated above.

   The NCISP recommends that privacy policies should:

   - ✓ Eliminate unnecessary discretion in decision making, guide the necessary discretion, and continually audit the process to ensure conformance with the policy.

   - ✓ Ensure legitimacy—when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented.

   - ✓ Clearly define the parameters of the policy.

✓ Acknowledge and address important issues that currently are not included in some existing criminal intelligence policies.

✓ Identify the decision points within the intelligence process and provide appropriate guidance and structure for each.

Issues for Consideration

Issues to consider when drafting a privacy policy include:

- Adding introductory language that clearly states the privacy practices of the center.

- Describing the information collected and how information is stored.

- Establishing a common lexicon of terms for dealing with role-based access.

- Defining and publishing how the information will be used.

- Drafting a clear, prominent, and understandable policy. Avoid communicating in complicated or technical ways.

- Displaying the privacy policy for both center personnel and customers.

- Ensuring that all other policies and internal controls are consistent with the privacy policy.

- Establishing a business practice of notifying government agencies of suspected inaccurate data.

- Adhering to applicable state and federal constitutional and statutory civil rights provisions.

- Partnering with training centers on privacy protection requirements and conducting periodic privacy security audits.

- Consulting with a privacy committee (see Guideline 3) to ensure that citizens' privacy and civil rights are protected.

- When utilizing commercially available databases, ensuring the usage is for official business and the information obtained is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data.

- Determining if there are security breach notification laws within the jurisdiction and following those laws, if applicable.

Adhering to a Privacy Policy

There are a number of mechanisms that centers can develop or establish that will assist them in adhering to their privacy policy. Some of these include:[49]

- Establish a privacy oversight committee (see Guideline 3) or appoint a privacy officer.

- Develop or update privacy training and orientation for all employees.

- Develop a mechanism for ongoing information privacy awareness.

- Establish a process for tracking and handling privacy complaints or concerns.

- Develop a consistent sanction policy for failure to comply with the privacy policy for all individuals in the organization.

- Recognize the overlap in privacy activities and security activities, and coordinate both within the organization.

- Ensure all center personnel are adequately trained in using the privacy policy.

- Seek legal counsel.

Available Resources on Fusion Center CD

- Audit Checklist (LEIU), www.it.ojp.gov/documents/LEIU_audit_checklist.pdf

- Global's *Privacy and Information Quality Policy Development for the Justice Decision Maker*, http://it.ojp.gov/documents/200411_global_privacy_document.pdf

- National Criminal Justice Association—*Justice Information Privacy Guideline*, www.ncja.org/pdf/privacyguideline.pdf

- *Privacy and Civil Rights Policy Templates for Justice Information Systems*

- Privacy Policy Sample Template

- *Privacy Policy Development Guide*

---

49 Beth Hjort, "A HIPAA Privacy Checklist (AHIMA Practice Brief)," *Journal of AHIMA 72*, Number 6, 64A-C, 2001.

Guideline 9

Ensure the appropriate security measures are in place for the facility, data, and personnel.

Security

Justification

Security pertains to information, documents, databases, facility, and personnel and includes measures such as authorization, encryption, access control, and confidentiality. In determining how most appropriately to protect data, there are many policy and technical issues for data owners to consider. It is important that policy issues be decided upon before technical issues are developed.

The private sector is affected by market forces, shareholder value, and various rules and regulations regarding the sharing and storage of information, including antitrust laws and the Freedom of Information Act (FOIA). The Homeland Security Act of 2002 states that the Critical Infrastructure Information Act grants an exemption from FOIA for the U.S. Department of Homeland Security (DHS) when private sector companies provide critical infrastructure information for the purposes of homeland security-related issues.

In addition, the Critical Infrastructure Information Act provides for the protection of critical infrastructure information submitted to DHS and subsequently shared with local and state agencies for the purposes of ensuring the resilience of critical infrastructure operations or in furtherance of an investigation of a criminal act.[50] When private sector entities submit critical infrastructure information to the fusion center, the center must ensure the information is protected from unauthorized disclosure. Fusion center leadership should be aware of local, state, and federal laws regarding the release of information, including state sunshine laws and FOIA.

Facility and personnel security should also be a part of the center's security plan. Appropriate security clearances should be obtained for personnel within the fusion center and key decision makers who need access. Security plans should be marked, handled, and controlled as sensitive but unclassified information. Some questions to consider when developing a security policy and plan include:

- Who does the data owner want to have access?
- How should users access the data?
- What access methods are necessary for the users' jobs?
- Should audits be used to ensure proper use of data?
- Should centers conduct background checks on personnel?
- What security needs exist for the facility?
- What security is needed for the data?
- Should a system-logging mechanism be used?

Issues for Consideration

When developing security protocols, consider:

- Adopting established models for secure information and intelligence sharing, such as Regional Information Sharing Systems (RISS), Law Enforcement Online (LEO), Regional Data Exchange (R-DEx), and Homeland Security Information Network (HSIN).
- Addressing limited/restricted access, authorization, authentication, and encryption.
- Applying security policies to both physical and electronic forms of information.

---

50   Homeland Security Act of 2002, Critical Infrastructure Information, www.dhs.gov/interweb/assetlibrary/CII_Act.pdf.

- Using the *Applying Security Practices to Justice Information Sharing* document.
- Determining access levels and maintaining a policy on the level of information released.
- Verifying access based on criteria established by governance structure.
- Creating a form to be submitted by the agency authorizing access/supervisory approval.
- Conducting background checks on personnel.
- Utilizing local or state lead law enforcement agency background check standards on public safety and private sector participants, to the extent permissible by state law.
- Clearly defining in the Memorandum of Understanding (MOU) all background check criteria or guidelines to law enforcement, public safety, and private sector partners.
- Consulting the *National Criminal Intelligence Sharing Plan* (NCISP) (Recommendation 28) when developing a background check policy.
- Using applicable security guidelines for access control.
- Providing relevant security clearances.
- Creating and providing a training component on center security protocols.
- Utilizing relevant local, state, and federal building security requirements.
- Utilizing relevant portions of 28 CFR Part 23 as it relates to security.
- Appointing a privacy officer as a central point for compliance and oversight.

Centers may also consider maintaining a security officer who is responsible for evaluating and providing information about the security program to management and communicating security requirements and concerns to the organization. The security officer conducts security training and awareness and prepares a policy on security. Any breach issues would be reported to and investigated by the security officer. The security officer should also coordinate background checks on center personnel. Background checks are important because, although the information and intelligence disseminated by the fusion center may be unclassified, it is still sensitive, and therefore all appropriate methods of information protection should be undertaken, including background checks. The NCISP states that "background requirements for access to the nationwide sensitive but unclassified communications capability by law enforcement personnel shall be consistent with requirements applied to the designation and employment of sworn personnel, as set by the participating state or tribal government."[51] Consideration should be given to colocating with other intelligence centers, such as High Intensity Drug Trafficking Areas (HIDTA) or other law enforcement facilities, in order to share security responsibilities.

Applying Security Practices to Justice Information Sharing provides details on how to safeguard critical elements of information sharing initiatives, as well as the infrastructure and integrity of data, systems, facilities, and personnel. According to the document, the following issues should be considered when developing and adhering to security policies:

- Identify potential physical threats to departmental computer systems and networks.
- Establish policies and procedures to thwart potential physical threats.
- Conduct audits to monitor employee compliance with department policies and procedures.
- Consider including the following physical security policies in the organization's overall security policy:
  - ✓ Identify unauthorized hardware attached to the department computer system; make routine checks of system hardware for unauthorized hardware.
  - ✓ Limit installation of hardware and software owned by employees on department desktop workstations.
  - ✓ Identify, tag, and inventory all computer system hardware.
  - ✓ Conduct regular inspections and inventories of system hardware.
  - ✓ Conduct unscheduled inspections and inventories of system hardware.
  - ✓ Implement policies that instruct employees/users on how to react to intruders and how to respond to incidents where an intrusion has been detected.
- Require background checks on all employees every five years.

Federal regulation 28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded, multijurisdictional criminal intelligence systems, and it provides the following guidelines regarding security:

- The database, manual or electronic, shall be located in a physically secured area that is restricted to designated authorized personnel.
- Only designated authorized personnel will have access to information stored in the database.
- All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility and physical location housing the database.
- All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- All hard-copy submissions and/or manual files will be secured by lead agency-designated authorized personnel when not being used and at the end of each shift.
- Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access will be adopted.
- When direct remote terminal access is authorized by participating agencies, policies and procedures addressing the following additional security measures shall be adopted:
  - ✓ Identification of authorized remote terminals and security of terminals.

---

51   NCISP, pp. 24-25.

- ✓ Identification and verification of an authorized access officer (remote terminal operator).
- ✓ Identification of levels of dissemination of information as directed by the submitting agency.
- ✓ Rejection of submissions unless critical data fields are completed.
- ✓ Technological safeguards on access, use, dissemination, and review and purge.
- ✓ Physical security.
- ✓ Training and certification of participating agency personnel.
- ✓ Audits and inspections of participating agencies, including file data-supporting submissions, security of access terminals, and policy-and-procedure compliance.
- ✓ Documentation for audit trails of the entire operation.

Available Resources on Fusion Center CD

- *Applying Security Practices to Justice Information Sharing*, http://it.ojp.gov/documents/asp/introduction/index.htm
- Critical Infrastructure Information Act of 2002, www.dhs.gov/interweb/assetlibrary/CII_Act.pdf
- National Institute of Standards and Technology (NIST) template and example policies, http://csrc.nist.gov/fasp
- *Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs*, U.S. Department of Homeland Security, May 2005

Guideline 10
Integrate technology, systems, and people.

Facility, Location, and Physical Infrastructure

Justification

Ensuring that participants are integrated is a key element of the fusion center. It is important to bring technology, systems, and people together. Integrating these components streamlines operations, creates an effective and efficient environment, and increases productivity. There are a number of ways to integrate participants. Two options are presented for consideration—colocating and virtual integration. Colocating personnel in one facility is the preference.

Colocating participating entities improves communication and breaks down barriers. Often, lack of resources and funding can impede the ability to colocate. However, it is recommended that participating agencies strive to locate personnel in the same facility, when possible. Colocation consolidates resources and equipment. In addition, it fosters an environment to develop and exchange information and intelligence.

If colocating is not a feasible option for a fusion center, participating entities may consider virtual integration, that involves linking the information sharing and communications systems so personnel can seamlessly access and exchange information. Fortunately, technology has improved greatly over the years and continues to generate new and innovative capabilities. Virtual integration can be an effective technology solution for integrating personnel and processes.

Regardless of the option a fusion center chooses, it is important to ensure flexibility and scalability, allowing for each step of the intelligence process to be conducted.

Issues for Consideration

The Law Enforcement Intelligence Fusion Center Focus Group (FCFG) preferred that participating entities be colocated. However, they also recognized the logistical issues and obstacles affecting the ability to colocate. In addition, the focus group recognized that not colocating also has benefits, such as

the ability for mobile capacity, contingency operations during emergencies, and flexibility in offering services and support. The Public Safety FCFG acknowledged that with the inclusion of public safety entities, colocation may not always be feasible. Liaisons may be established with the various public safety entities that can be made operational when the need arises.

Furthermore, the Private Sector FCFG noted that due to the vast number and types of private industry within a jurisdiction, colocation may not be attainable. Instead, the focus group developed options for integrating private sector entities. One option is to institute a rotating private sector desk. This will allow different entities full-time participation within the fusion center to both understand the workings of the fusion center and participate in the processes that take place. By initiating a rotating desk, various private sector entities will have the ability to participate and validate their investment in the fusion center. Another option for integrating the private sector is to identify subject-matter experts within the private sector who can provide fusion centers with expertise as the need arises. For example, when a threat is made on the transportation industry, identified subject-matter experts from various transportation entities can be contacted by the fusion center to determine how the threat will impact the jurisdiction and industry.

A number of logistical issues must be addressed when deciding on a facility and location for a fusion center. The primary issues, not in priority order, include:

- Connectivity
  - ✓ Will the fusion center, emergency operations center, or other partners be connected? If so, how?
- Scalability
  - ✓ Ensure the facility allows for future and emergency expansion.
- Security
  - ✓ Ensure security for the facility, data, personnel, and visitors (see Guideline 9).
- Redundancy
  - ✓ Ensure redundancy for the infrastructure, resources, personnel, systems, etc.
- Emergency Power
- Continuity of Operations Plan (COOP)
- Threat/Vulnerability Assessments
  - ✓ Use private sector subject-matter experts to determine risks based on threat assessments.
- Political Issues
  - ✓ Recognize that the political climate will be different for each center.
  - ✓ Work with and inform political officials and policymakers regularly.
- Access
  - ✓ Ensure center personnel have seamless access to each other.
- Personnel
  - ✓ Ensure full and equal representation at local, state, and federal levels.
  - ✓ Ensure representation from law enforcement, public safety, and private sector components.
- Authority/Regulations
  - ✓ Follow appropriate policy, statutes, Concept of Operations (CONOPS), and other guidelines.
- Roles and Responsibilities
  - ✓ Clearly define personnel responsibilities, including roles during emergency situations.

Site Selection

When selecting or building a site for a fusion center, it is important for the site to be based on the functional needs of the center. At a minimum, a site should be designed based on the following functional elements:

- Collection/data management
- Analysis
- Command and control/executive
- Deconfliction
- Communication and dissemination

- Facilities management
- Feedback

If the center plans on managing multiple sites, additional consideration should address connectivity and collaboration issues.

The following list contains some key components to assist agencies in developing a plan to locate, acquire, and/or renovate, and maintain a facility:

- Identify facility needs.
- Identify a facility project team to manage facility issues.
  - ✓ Ensure that center personnel are involved in site selection.
- Communicate with center leadership.
- Identify and secure needed funding (see Guideline 17).
- Conduct a space-needs analysis.
  - ✓ Utilize existing resources, when possible.
- Consult the U.S. General Services Administration's *Facilities Standards for the Public Buildings Service* when building a facility to house the fusion center.
- Conduct site visits.
  - ✓ Consider geographical and environmental issues, as well as convenience and location.
  - ✓ Consider the survivability of the building.
- Conduct a mission/operational continuity assessment.
- Develop a transition plan and timetable for occupancy.
- Work with technical personnel to ensure that connectivity and security issues are established.
- Train staff regarding facility, security measures, and policy requirements.
- Conduct Continuity of Operations exercises to ensure the operational resiliency of the center.
- Ensure plans and/or procedures are in place for regular facility evaluation and building maintenance.

Physical Security

Physical security includes all elements that make up the facility: it protects people, property, and processes. Centers should plan, identify, design, train, and implement all appropriate security measures; adhere to them; identify and create a program that identifies physical assets, threats, and vulnerabilities; assess and prioritize risks; and identify ways to resolve and respond to concerns or breaches.[52] A physical security plan should have, at a minimum, the following components:[53]

- Risk assessment
- Operating procedures
- Training, testing, and rehearsal plan
- Managing threats
- Communications plan

---

52   David Hochman, *Disruption Defense: Facility Security Breaches*, 2002.
53   U.S. General Services Administration, 3d ed., www.gsa.gov, 2004.

- Occupant Emergency Plan (OEP)
- COOP

Centers may consider maintaining a facility/security manager or officer who is responsible for preparing the facility security policy, monitoring and adhering to the policy, and training center personnel regarding the security policy and protocols. Training of users is critical. Users must understand their role and responsibility in adhering to a security plan, as well as how to notify the appropriate management when issues or concerns arise regarding security, such as lost badges or noncompliance (see Guideline 9).

Contingency Plan

The Law Enforcement Intelligence FCFG recommended that fusion centers identify a skeleton model for emergency operations. Centers should develop a contingency plan. A contingency plan enables the sustained execution of mission-critical processes and information technology systems during an extraordinary event that causes these systems to fail.

In addition, it is recommended that fusion centers develop and adopt a COOP to perform essential functions at an alternate location during an emergency. COOP enables each level of government and jurisdiction to preserve, maintain, and/or reconstitute its capability to function effectively in the event of a threat, disaster, or emergency. Consult the U.S. Department of Homeland Security (DHS) Federal Emergency Management Agencys' (FEMA) *Interim Guidance on Continuity of Operations Planning for State and Local Governments,* dated May 2004.

Security Clearances

Most information needed by state or local law enforcement can be shared at an unclassified level. However, in those cases where it is necessary to share classified information, it can usually be accomplished at the "Secret" level. Resources regarding security clearances are included on the resource CD. Law enforcement should be cognizant of classification levels when distributing information to public safety and private sector entities. One of the goals of the fusion center is to enhance information sharing, and information classification barriers should be minimized. Rather than rely on clearances, fusion centers should attempt to declassify information and intelligence, when possible, to disseminate to public safety and private sector partners.

Centers also need a secure operation to perform classified work. Centers may consider use of the Sensitive Compartmented Information Facility (SCIF) concept. An SCIF is defined as an accredited area, room, group of rooms, building, or an installation where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and processed. SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency.[54]

Available Resources on Fusion Center CD

- Executive Orders 12068, 12958, and 13292 Regarding Classified Information
- FBI Security Clearance and Frequently Asked Questions
- GSA's *Facilities Standards for the Public Buildings Service*
- *IACP Police Facility Planning Guidelines: A Desk Reference for Law Enforcement Executives*, www.iacp.org/documents/pdfs/Publications/ACF2F3D%2Epdf
- National Institute of Standards and Technology, "Contingency Plan Template," http://csrc.nist.gov/fasp/FASPDocs/contingency-plan/contingencyplan-template.doc

---

54   Criminal Intelligence Glossary of Terms, November 2004.

Guideline 11

Achieve a diversified representation of personnel based on the needs and functions of the center.

Human Resources

Justification

Selecting personnel depends upon the needs and functions of the center. The center will conduct, at a minimum, all aspects of the intelligence process. Staff will need the ability to perform analytical functions and provide strategic and tactical assistance. It is important for the center to recruit the highest quality individuals and to ensure center personnel are assigned appropriately. For example, leadership should ensure qualified personnel are selected for key objectives such as collection and analysis. Personnel should demonstrate attention to detail, integrity, good interpersonal communication skills, and the ability to accept and learn from constructive criticism.

Public safety and private sector personnel should be included in staffing. Leadership should be cognizant of the integration of public safety and private sector partners and their importance to the success of operations, though entities for each component may provide personnel in different ways (full-time representation, a part-time representative, or a liaison). Public safety and private sector participation may fluctuate based on identified threats or ongoing operations. For instance, if an information technology (IT) threat is identified, public safety/private sector partners who are experts in the IT field may change from a liaison-type membership to full-time personnel until that threat is neutralized or unsubstantiated. Or, if hazardous material moves through the fusion center jurisdiction once a month, public and private sector partners associated with hazardous materials may become full-time personnel within the fusion center during this operation.

Fusion center management should consider exchanging personnel with private sector partners to aid in training and understanding how each component functions. Cross-training will aid in providing fusion center analysts with an understanding of the private sector, including what threats affect them, how threats are handled, and the types of information that the private sector can provide to fusion centers. Private sector personnel assigned to the fusion center will understand fusion center operations and information requirements.

Furthermore, the governance body should continually evaluate center membership and partners. In short, the fusion center represents a fluid environment, and as new businesses and organizations are established within the jurisdiction, the governance body should reach out to these organizations.

Issues for Consideration

When staffing a fusion center, consider:

- Recruiting personnel based on a Concept of Operations (CONOPS) and center mission and goals.
- Maintaining a 24-hour-a-day/7-day-a-week operation with appropriate staffing levels.
- Ensuring appropriate command structure and leadership.
- Establishing a permanent full-time civilian (non-law enforcement) position to provide continuity and consistency in the long term (i.e., facility manager/center director).
- Maintaining a small core staff dedicated to specific functions, such as administration, information technology, communications, and graphics.
- Creating units of operation (or crime desks), such as intelligence, criminal investigations (e.g., violent crimes, drugs, and gangs), analytical, and homeland security.
- Identifying and utilizing subject-matter experts from law enforcement, public safety, and the private sector.
- Ensuring equal/proportional representation of personnel from participating entities.
- Maintaining legal counsel dedicated to the fusion center to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and liaison with the development of policies, procedures, guidelines, and operational manuals.
- Liaising with the local prosecutor's office.
- Securing appropriate number and types of security clearances for personnel and identifying clearances based on local, state, and federal requirements.
- Requiring a minimum term commitment for full-time center personnel.

- Ensuring a Memorandum of Understanding (MOU) addresses human resources management and issues.
- Institutionalizing professionalism.
- Establishing a mechanism to manage temporary personnel.
- Using a personnel checklist when assigning or removing personnel from the center (see Sample Checklist on resource CD).

Example Staffing

Arizona Counter Terrorism Information Center (ACTIC)

The ACTIC will operate on a 24-hour-a-day/7-day-a-week basis and will function as a multiagency, all-hazard effort staffed by members of the Department of Public Safety and other local, state, and federal agencies.

California State Terrorism Threat Assessment Center (STTAC) and Regional Terrorism Threat Assessment Centers (RTTAC)

The STTAC and four RTTACs are all-crimes, all-hazards fusion centers that integrate local Joint Terrorism Task Forces (JTTFs), FBI Field Intelligence Groups (FIG), Terrorism Early Warning Groups (TEWG), and other state agencies in their operations. Terrorism Liaison Officers (TLO) are designated at local agencies and have network access to the California Joint Regional Information Exchange System (CAL JRIES) to link local operations and information gathering with the STTAC and RTTACs.

Rockland County Intelligence Center (RCIC)

RCIC provides services to all law enforcement agencies and is composed of sworn officers from Rockland County law enforcement agencies. The Intelligence Center officers are assigned specialized "desks." Each desk focuses on a specific type of criminal activity, including burglary/robbery, counter-terrorism, factual data analysis, firearm tracking, identity crimes, organized crime, and street gangs.

Georgia Information Sharing and Analysis Center (GISAC)

GISAC's day-to-day operations, facilities, personnel, finances, and administration are managed by Georgia Bureau of Investigation supervisors. There are a total of 18 personnel assigned.

Statewide Terrorism Intelligence Center (STIC)—Illinois

STIC operates three 24-hour-a-day/7-day-a-week shifts, with a half-hour overlap on each shift for shift-change briefing. Each shift is staffed with one full-time watch officer and four contractual terrorism research specialists (TRS). STIC maintains additional supervisory and operational staff on the day shift. Each employee works a 37.5-hour workweek. Minimum staffing is one supervisor and two TRSs, Monday through Friday, and two TRSs on weekends.

Staffing Model Templates

While most staffing models do not focus specifically on law enforcement personnel, there are some guidelines that leadership can use to help adequately staff a fusion center. During the focus group meetings, the following categories of staffing were recommended. These categories include:

- Collection function—collection management process
- Analytical services
- Technical support
- Communications liaison for dissemination and sharing externally
- Leadership/command—supporting intelligence-led policing

This staffing model follows the functions within the intelligence process. Focus group members recommended that the intelligence process dictate the number and level of staffing. It is also important to consider the need for supervisory and management positions, as well as training and information technology support personnel.

Standards for Analysts

In support of the *National Criminal Intelligence Sharing Plan* (NCISP), the International Association of Law Enforcement Intelligence Analysis (IALEIA) published the *Law Enforcement Analytic Standards* booklet, which is included on the accompanying resource CD. The booklet contains standards regarding education, training, continuing education, professional development, certification, and analytic attributes. It is recommended that centers follow these standards when hiring analysts, preparing individuals for the position of analyst, and/or enhancing an individual's skills and abilities (see Guideline 14, Intelligence Services and Products, for more information).

Available Resources on Fusion Center CD

- *Law Enforcement Analytic Standards*, http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf
- Personnel Sample Checklist

Guideline 12
Ensure personnel are properly trained.

Training of Center Personnel

Justification

Training helps personnel maximize the ability to effectively utilize tools in support of center functions. It is recommended that fusion centers adhere to the training objectives outlined in the *National Criminal Intelligence Sharing Plan* (NCISP). In addition, it is recommended that personnel working within the center meet the core training standards developed by the Global Intelligence Working Group (GIWG) and Counter-Terrorism Training Coordination Working Group (CTTWG). Each of the six training classifications identified by the GIWG (intelligence analyst, intelligence supervisor, law enforcement officer, law enforcement executive, intelligence officer/collector, and train-the-trainer) have unique standards. Center personnel should also receive an overview of center operations, policies and procedures, and any unique protocols or communication needs. The National Governors Association (NGA) Center for Best Practices published a paper, *State Intelligence Fusion Centers: Recent State Actions*, which surveyed the types of resources that the states need to complete development of or improve their intelligence fusion centers.[55] Numerous responses included the need for additional training—specifically, training for analysts and supervisors.

Public safety and private sector integration into fusion centers presents new training obstacles and opportunities. Though law enforcement has traditionally been the primary intelligence component in crime prevention, the introduction of public safety and the private sector into the intelligence process requires additional training on the intelligence and fusion processes. In addition, cross-educational training should occur between the fusion center and the public safety and private sector entities in order to give each an understanding of the respective business practices within each component, what they can provide to fusion centers, and what they need from fusion centers.

Fusion center personnel should consider participating in tabletop exercises (TTX), functional exercises, and full-scale exercises that private sector organizations may stage. These exercises

will assist fusion centers in institutionalizing partnerships with public safety and the private sector through strategic and tactical integration and will also aid in testing the communications plan (see Guideline 18). Fusion center participation in these types of exercises will also aid in identifying the information requirements of the fusion center, private sector, and public safety entities.

---

55   National Governors Association, Center for Best Practices, *State Intelligence Fusion Centers: Recent State Actions*, 2005.

The public safety and private sector components represent nontraditional gatherers of information and present an opportunity to enhance and increase the amount and types of data that fusion centers receive. Because these entities are nontraditional and may not be aware of the intelligence cycle and the information requirements of the fusion center, fusion centers should provide training to fusion center staff and public safety and private sector liaisons. This training explains the types of information that nontraditional gatherers should be aware of, the importance of this information, how to gather the information, and who to report it to.

Issues for Consideration

When reviewing training, consider:

- Identifying training needs of center personnel.
- Providing specialized training, as appropriate.
- Providing training on the fusion center operations, NCISP, intelligence cycle, and the fusion process.
- Providing information collection training for fusion center participants.
- Providing training in tactical and strategic intelligence.
- Seeking accredited or standards-compliant training programs for government personnel.
- Utilizing private security entities for subject-matter training (e.g., cyber security).
- Emphasizing analysis and its link to intelligence-led policing.
- Developing materials and integrating outreach efforts.
- Adhering to other training mandates.
- Ensuring that personnel assigned to specific crime desks receive crime-specific training.
- Utilizing scenario-based training, simulations, games, and tabletop and field exercises.
- Participating in public safety and private sector tabletop, functional, and full-scale exercises.
- Participating in college- and university-sponsored intelligence and analyst training programs.

NCISP Training Objectives and Minimum Training Standards

In November 2003, the Criminal Intelligence Training Coordination Strategy (CITCS) Working Group was established to develop a recommended intelligence training coordination strategy. The CITCS recognized that there were voids in existing criminal intelligence training and duplication of effort in terms of training development and delivery. The CITCS met throughout 2004 and finalized their recommendations in June 2004. The CITCS recommendations are contained in the report entitled *Minimum Criminal Intelligence Training Standards for United*

States Law Enforcement and Other Criminal Justice Agencies and have been endorsed by the GIWG Training/Outreach Committee, the Criminal Intelligence Coordinating Council (CICC), the CTTWG, and the Global Advisory Committee. The report is included on the resource CD. These recommended minimum criminal intelligence training standards were developed for the following training classifications:

- Intelligence analyst
- Intelligence manager
- Law enforcement executive
  - ✓ General law enforcement officer (basic recruit and in-service)
  - ✓ Intelligence officer/collector
  - ✓ Train-the-trainer

These efforts are significant, not only in implementing the tenets of NCISP but also in building awareness, institutionalizing the importance of criminal intelligence, increasing the value of intelligence personnel, fostering relationships among the law enforcement community, improving the ability to detect and prevent acts of terrorism and other crimes, and creating a safer home for citizens.

The U.S. Department of Homeland Security (DHS), Office of State and Local Government Coordination and Preparedness, is currently developing training in the field of intelligence and information sharing capabilities. Once finalized, this training will be available for widespread utilization by state and local governments, as well as all relevant fusion center participants.[56]

It is also recommended that center staff receive training regarding facility security and operations and information security, as well as the center's policies and procedures.

Available Resources on Fusion Center CD

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov
- Homeland Security Presidential Directive 5 (HSPD-5), www.whitehouse.gov/news/releases/2003/02/20030228-9.html
- Homeland Security Presidential Directive 8 (HSPD-8), www.fas.org/irp/offdocs/nspd/hspd-8.html
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org/
- International Association of Directors of Law Enforcement Standards and Training (IADLEST), www.iadlest.org/
- *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies,* www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf
- National White Collar Crime Center (NW3C), www.nw3c.org

---

56   More information about the training opportunities available can be found at the Office for Domestic Preparedness
Web site at www.ojp.usdoj.gov/odp/.

Guideline 13

Provide a multitiered awareness and educational program to implement intelligence-led policing and the development and sharing of information.

Multidisciplinary Awareness and Education

Justification

In addition to training center personnel (see Guideline 12), a center should provide general awareness training for all those involved in intelligence, regardless of whether they are assigned directly to the center. All investigative or intelligence personnel, as well as nontraditional gatherers of information—such as fire, emergency management, and health personnel—should receive training. Personnel should be equipped to identify suspicious activities or threats and provide information to fusion center personnel, as appropriate. Further, nontraditional partners should be provided with situational awareness training, specifically, training that aids in the identification of activities and events that may be related to a criminal enterprise. In addition, policymakers and legislators should understand the center's mission and goals in order to effectively support center efforts, make decisions regarding funding and resource allocation, and respond appropriately during emergencies. Part of this process is developing outreach materials and ensuring that training is ongoing and relevant.

The training objectives and recommended minimum criminal intelligence training standards developed in support of the *National Criminal Intelligence Sharing Plan* (NCISP) apply to this standard (also see Guideline 12, Training of Center Personnel). Recommended minimum criminal intelligence training standards have been developed for the following training classifications:

- Intelligence analyst
- Intelligence manager
- Law enforcement executive
- General law enforcement officer (basic recruit and in-service)
- Intelligence officer/collector
- Train-the-trainer

Training standards for analysts, officers, and collectors should include elements regarding how to identify and collect intelligence. In addition, the recommendations for managers and executives offer guidelines and information pertaining to the importance of intelligence, process collecting, and analyzing and disseminating intelligence; how to manage and support an intelligence function; and how to develop and adhere to appropriate policies. Nontraditional collectors of intelligence, public safety entities such as fire, health, and agriculture, and the private sector should have awareness training, including information gathering. Many local, state, and private organizations provide awareness-level training. Centers should identify appropriate training mechanisms and provide outreach to personnel.

The general public should be knowledgeable and prepared. This level of public awareness and education requires a focused and concentrated effort. Options for leadership to inform the public about fusion centers include participation at town hall meetings, city commission meetings, or media interaction (newspaper articles, television news stories). It is important in order for the public to support the fusion center to understand its purpose and mission.

Issues for Consideration

When reviewing awareness training, consider:

- Tailoring training based on the needs of individual personnel (i.e., law enforcement officers and executive, public safety, and private sector representatives).
- Identifying what elements intelligence personnel need regarding center operations.
- Developing materials and integrating outreach efforts.
- Communicating with all agencies serviced by the center to ensure appropriate training.
- Prioritizing the intelligence function to address threats posed in specific fusion center jurisdictions.
- Integrating intelligence-led policing to support customer needs, define tasks, and prioritize functions.
- Utilizing computer-based training for nontraditional information gatherers (e.g., security officers).

- Ensuring training includes awareness of privacy issues associated with information collection, storage, and dissemination.

Available Resources on Fusion Center CD

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov

- HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report

- *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies*, www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf

Guideline 14
Offer a variety of intelligence services and products to customers.

Intelligence Services and Products

Justification

The majority of the initiatives reviewed during the focus group's processes operate 24 hours a day, 7 days a week and act as a clearinghouse for information and/or intelligence sharing. The intelligence process acts as the framework but does not limit information sharing to intelligence product dissemination. As such, personnel utilize the intelligence process while producing analytical services, such as crime-pattern analysis, association analysis, telephone-toll analysis, flowcharting, financial analysis, and strategic analysis. Fusion centers should take into account the needs and requirements of their respective jurisdictions when producing products and services.

As a result of sharing information throughout the intelligence process, the initiatives provide an array of intelligence products, such as intelligence reports, briefs, threat assessments, charts, graphs, and mapping. Thus, it is important that center personnel, especially analysts, be familiar with computer applications that have information storage capabilities which allow the user to sort, query, and filter information; applications for presenting information; and applications for linking and flowcharting.

Some initiatives have compartmentalized their operations by creating divisions, such as investigations, intelligence, and administration. This structure may assist in identifying and assigning responsibilities, as well as holding personnel accountable. It is important to know who the program's customers are and what types of services and products they need.

Issues for Consideration

It is recommended that law enforcement intelligence programs produce both strategic and tactical products to support the mission and priorities of the center. A major purpose of intelligence analysis is management decision making. Consider providing the following services and products:

- Investigative and tactical response
- Proactive strategic analysis

- Intelligence support for investigations
- Visual investigative analysis
- Alerts and notifications
- Deconfliction
- Target identification
- Critical infrastructure analysis
- Training opportunities
- Geospatial imaging
- Criminal backgrounds and profiles
- Case correlation
- Crime-pattern analysis
- Association, link, and network analysis
- Telephone-toll analysis
- Flowcharting
- Financial analysis
- Intelligence reports and briefings
- Threat assessments
- Terrorism calendar

Centers should prioritize their intelligence function, based on specific threats in their jurisdictions/regions, and integrate intelligence-led policing to support customer needs, define tasks, and prioritize functions. When specific threats are identified, centers should partner with agencies and organizations that can aid in analysis, e.g., computer analysis and forensic analysis. For example, if a government network has been hacked into, then computer resources from law enforcement and the private sector may help the investigation and analysis.

Standards for Analytical Products

The *National Criminal Intelligence Sharing Plan* (NCISP) recommends that the agency chief executive officer and the manager of intelligence functions should "support the development of sound, professional analytic products (intelligence)." One way to accomplish this is to recommend that products meet substantive criteria. The International

Association of Law Enforcement Intelligence Analysts' (IALEIA) *Law Enforcement Analytic Standards* booklet provides standards for analysis that correspond to the intelligence process. These standards focus on:

- Planning
- Direction
- Collection
- Legal constraints
- Evaluation
- Collation
- Analytic accuracy
- Computerized analysis
- Analytic product content
- Analytic outcomes
- Dissemination plan
- Analytic report
- Analytic product format
- Analytic testimony
- Data source attribution
- Analytic feedback
- Analytic production evaluation

It is recommended that analysts or individuals fulfilling the analytic function adhere to the standards outlined in the booklet. A copy of the booklet is included on the resource CD.

Infrastructure Assessment and Resources

A significant role for any fusion center concerned with homeland security, is tracking critical infrastructure and assessing the likelihood of it being the target of a terrorist attack. It is imperative that there is collaboration between center personnel and private sector partners when risk assessments are being conducted regarding the private sector. The private sector has detailed knowledge of its information, processes, and infrastructure, and its subject-matter experts and security personnel can identify accurate and comprehensive risks. Fusion centers may also analyze risks within the jurisdiction, including those risks associated with public safety and private security. Risk assessments, when performed in conjunction with private sector security and subject-matter experts, will aid the center in identifying key infrastructure when threats are present. Fusion centers may also be tasked with cataloging critical infrastructure; developing a methodology to track intelligence relating to threats, exploitable vulnerabilities, and the consequences of loss of those facilities; maintaining and sharing with partners a list of special events that may pose a threat (e.g., high visibility and large crowds); and developing a mechanism to update this information regularly.

Center personnel must utilize the relationships between regulatory government agencies and the private sector when conducting risk assessments, these relationships have already been established and expertise identified. For the nonregulated industry, center personnel should meet with industry officials to identify the critical infrastructure and what is available. These meetings will also lay the foundation for developing trusted relationships with subject-matter experts. The fusion center should be aware that information gathered by regulatory agencies may be protected by regulations and, therefore, not be subject to dissemination.

In addition, the center may develop assessments of the vulnerabilities and security protocols for critical facilities. This may range from simply maintaining the assessments completed by others to actually participating in on-site assessments. Either way, it is important that the center receive risk assessments to aid in threat identification and prevention. The fusion center may consider working with the area Joint Terrorism Task Force (JTTF), Anti-Terrorism Advisory Council (ATAC), Information Sharing and Analysis Center (ISAC), and the U.S. Department of Homeland Security (DHS), including the USP3 portal, as well as other state and local authorities, to design and implement operational resiliency objectives to include protective measures that mitigate vulnerabilities. Included in the resource documents is a section from the Florida Department of Law Enforcement (FDLE) *Terrorism Protection Manual* that covers critical infrastructure assessments. Industry-specific subject-matter experts should be used to aid in infrastructure assessments and the identification of risks associated with the private sector. Subject-matter experts have the knowledge and training to identify and assess critical infrastructure associated with the private industry and are valuable assets for fusion centers. Furthermore, working with subject-matter experts will demonstrate continued collaboration between private industries and fusion centers and will foster trust and the creation of successful partnerships. If fusion centers are tasked with conducting critical infrastructure assessments, every effort should be made to protect the results of these assessments. This information is sensitive and must not be released to nonauthorized personnel. Center management should be aware of local, state, and federal laws regarding the storing and release of this information.

The DHS Office of Preparedness and Office of Intelligence and Analysis (OPOIA) helps deter, prevent, and mitigate consequences in "all-hazard" environments, assessing threats, exploitable vulnerabilities, and consequences. Developed as a result of the Critical Infrastructure Information Act, the OPOIA can aid centers with assessments, risk analysis, and compilations of critical infrastructure assets. More information regarding these programs can be viewed at www.dhs.gov.

Available Resources on Fusion Center CD

- DHS's *National Response Plan*, December 2004
- *Terrorism Protection Manual*, FDLE, February 28, 2003

Guideline 15
Develop, publish, and adhere to a policies and procedures manual.

Policies and Procedures

Justification

Fusion centers should use a formalized policies and procedures manual. A comprehensive manual offers a number of advantages.[57] It demonstrates that the center has provided direction to its employees and that personnel follow approved procedures in carrying out their duties. In addition, policies and procedures indicate that the governing body has been proactive in planning, instead of reactive or waiting until an incident occurs to write policy. The policies and procedures manual is the foundation for communications within the center and among personnel. By developing, publishing, and adhering to a policies and procedures manual, the expectations for personnel are outlined, creating consistency and accountability while reducing liability and enhancing overall professionalism. A policies and procedures manual also serves as a central repository for all center directives. It is important for personnel to easily locate the center's most recent procedures.

Issues for Consideration

When designing a policies and procedures manual, consider:[58]

- Outlining the roles and responsibilities of all parties involved.
- Including language that information should only be used for criminal investigations.
- Including the center's mission, goals, objectives, policies, procedures, rules, and regulations.
- Tailoring the manual to meet the needs of the center.
- Ensuring personnel have easy access to the manual. Providing employees a copy of the manual and/or providing an online manual.
- Using a standardized format to allow for easy reading, filing, retrieving, and correcting.

- Implementing an annual review of center directives and purging or revising outdated policies and procedures.
- Establishing a contractor's code of conduct.
- Citing of the policy and procedures manual in the Memorandum of Understanding (MOU) and Non-Disclosure Agreement (NDA) (Guideline 5).
- Outlining how and from whom intelligence requirements are determined; e.g., the private sector has intelligence requirements for protection of its facilities.
- Ensuring understanding of and compliance with local and state confidentiality laws and how to appropriately safeguard data.
- Citing privacy policies (local, state, and federal), including the separation of information, to ensure understanding of and compliance with the privacy guideline.

Suggested Policies and Procedures

Begin by identifying existing guidelines, statutes, policies, and procedures that affect center operations and ensure adherence to regulations, such as 28 CFR Part 23 and the Critical Infrastructure Information Act. Personnel should be trained on and understand all center processes and policies and procedures

---

57   Michael Carpenter, M.A., M.A.T., "Put It in Writing: The Police Policy Manual," *FBI Law Enforcement Bulletin*, Vol. 69, No. 10, October 2000.
58   Ibid.

and adhere to them at all times. Areas that may require policies and procedures include:

- Intelligence process (see Guideline 1, NCISP).
- Intelligence collection requirements.
- Security for data, facility, personnel, and systems (for more information, see Security (Guideline 9); Facility, Location, and Physical Infrastructure (Guideline 10); and Human Resources (Guideline 11).
- Communications (for more information, see Interconnectivity [Guideline 7]).
- Privacy (for more information, see Guideline 8, Privacy and Civil Liberties).
- Accountability and review.
- Sanctions and violations of policies and procedures.

28 CFR Part 23

Agencies that use federal funds to set up or maintain a criminal intelligence database (and share information between jurisdictions) may need to comply with the regulations of 28 CFR Part 23. The regulations require agencies to have policies and procedures in place regarding intelligence operations. The specifics of the policies are left to the individual agencies. A copy of this regulation is included on the accompanying resource CD. Additional information may also be found at www.iir.com/28cfr.

In addition to the regulations of 28 CFR Part 23, the *National Criminal Information Sharing Plan* (NCISP) also recognizes the following documents and guidelines for creating and implementing a policies and procedures manual: the *Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines and the Justice Information Privacy Guideline*.

Available Resources on Fusion Center CD

- 28 CFR Part 23, www.iir.com/28cfr/Overview.htm
- *Evaluation Checklists for Intelligence Units*, Paul R. Roger
- IACP's *Criminal Intelligence Model Policy*
- Law Enforcement Intelligence Unit's (LEIU) *Criminal Intelligence File Guidelines*, http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf
- *Justice Information Privacy Guideline*, www.ncja.org/pdf/privacyguideline.pdf
- *Privacy Policy Development Guide*, http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Guideline 16
Define expectations, measure performance, and determine effectiveness.

Center Performance Measurement and Evaluation

Justification

It is important to have a process that systematically reviews performance. Performance measurement review is critically important to the health of an organization. The review must accurately reflect existing performance and operate to initiate improvement. Reviewing an entity's objectives is required to ensure integrity of the measurement process and to justify continued investment in the organization or project. An effective and verifiable performance measurement-and-review process can address these concerns. The performance measures addressed under this standard refer to the center's performance, not those of an individual. Personnel issues are addressed under Guideline 11, Human Resources.

Due to the unique structure of fusion centers, traditional law enforcement performance measures may not adequately gauge center performance. Performance measures should be designed based on the center's core mission, goals, and objectives and should reflect services generated from all areas of the center. It is also important to note that performance measures and funding are often related. Management should consider this relationship when developing measures and reviewing/submitting funding requests. Performance measures offer quantitative validation for management and policymakers regarding the effectiveness of the fusion center. Furthermore, performance measures may demonstrate to law enforcement, public safety, and the private sector the effectiveness of housing a multidisciplinary intelligence function in one location, which may result in continued funding for the center.

Centers might also consider developing an evaluation process, which differs from performance measurement. Performance measures assess center services and accomplishment of its mission. Evaluation, on the other hand, reflects judgments regarding the adequacy, appropriateness, and success of a particular service or activity.[59] In other words, performance measures focus on the "what" while evaluation focuses on the "why."

Issues for Consideration

When establishing performance measures and evaluating effectiveness, consider:

- Defining the expected performance.
- Developing outputs and outcomes that measure the expected performance.
- Coordinating the development and review of measures and performance with participating agencies.
- Developing meaningful relevant and quantifiable measures.
- Creating measures that are based on valid and reliable data.
  - ✓ Validity—ask the question: "Does the information actually represent what we believe it represents?"
  - ✓ Reliability—ask the question: "Is the source of the information consistent and dependable?"
- Creating both internal and external measures where internal measures pertain to administrative purposes.
- Establishing reasonable standards and targets.
- Leveraging which systems and databases statistically capture data.
- Utilizing automation to capture, store, and report performance.
- Reporting and reviewing on performance regularly (i.e., board or managers' meetings) and adjusting operations, as appropriate.
- Publicizing performance to the public, policymakers, and customers.
- Creating accountability and deterring the consequences for not meeting targets.
- Surveying customers.
- Integrating feedback and suggestions into fusion center operations.
- Developing a strategic plan to guide operations.

---

59   Charles R. McClure, *Performance Measures*, School of Information Studies, Syracuse University, 1996.

- Continually evaluating performance measures to extend beyond the criminal justice information sharing environment, to include public safety and the private sector.
- Liaising with the U.S. Department of Homeland Security (DHS), Office of State and Local Government Coordination and Preparedness, regarding the Target Capabilities List.

Elements of Good Performance Measures

Generally accepted guidelines for developing performance measures include:

- Using standard terms and definitions.
- Gauging progress towards agency goals and benchmarks or other high-level outcomes.
- Focusing on key issues.
- Having reasonable targets.
- Basing on accurate and reliable data.
- Being easily understood and measuring performance in a single area.
- Being timely.
- Limiting subjectivity—being objective.

Using Performance Measures

Once performance measures are developed, baseline data will need to be obtained during the first year of operation. Baseline data assists managers in determining the standards for future years. Measures should reflect center goals and be quantifiable. Standards should be challenging to achieve but also realistic. Management should review performance regularly and inform center personnel of progress. By keeping employees informed and involving them in the performance-measure process, they will be motivated to work collectivity to reach targeted goals. Performance measures can be tied to funding and resource requests and have a significant impact on support and future endeavors.

Available Resources on Fusion Center CD

- Office of Management and Budget, www.omb.gov
- Target Capabilities List, Version 1.1, www.ojp.usdoj.gov/odp/docs/TCL1_1.pdf

Guideline 17

Establish and maintain the center based on funding availability and sustainability.

Funding

Justification

Funding is critical to establishing fusion centers, directly impacting a center's longevity and ability to effectively and efficiently operate. Often, new initiatives receive start-up funds through government programs and/or grants. This seed money is an excellent means of beginning new projects or programs. Unfortunately, some efforts end because initial funding has been spent and no additional funding was identified or obtained to continue the project. For the long term, it is essential that centers take responsibility for funding to ensure sustainability. Fusion centers that have been surveyed regarding their ongoing needs repeatedly cite funding as a priority in the development and sustainment of the center.[60] It is recommended that management identify the needs of the center and identify available funding sources from local, state, federal, and nongovernmental sources.

Fusion center leadership should seek to link the performance of the center to funding. As seed money ends, performance measures may be an effective tool for fusion centers to use in securing funding. Performance measures that cover notifications and intelligence services and products demonstrate the success and return on investment of a fusion center.

Issues for Consideration

When reviewing funding needs and sources, consider:

- Basing funding on center priorities.
- Leveraging existing resources/funding from participating entities.
- Ensuring resource commitment of participating entities is addressed in the Memorandum of Understanding (MOU).
- Identifying supplemental funding sources (i.e., seized assets/ forfeitures, local and state government appropriations, state and federal grants, and private sources).
- Establishing an operational budget.

- Adhering to reporting requirements (i.e., annual report).
- Ensuring fusion center sustainability.
- Identifying return on investment for fusion center partners (e.g., defining what partners will receive as a result of participation).

Center Expenses

To effectively operate a fusion center, a number of cost elements must be identified and addressed in a budget. Some of these expenses can be shared among participating agencies. The following is a sample list of budgetary expenses that will require funding:

- Salary
- Vehicles
- Equipment
- Supplies/commodities
- Facility
- Furnishings
- Information technology support
- Communication equipment
- Training
- Travel
- Contractual (copier, delivery)
- Printing
- Physical security (personnel, sensors, special rooms for federally classified information, and related systems)
- Communications (high-bandwidth, federally classified information)

Available Resources on Fusion Center CD

- Summary of Funding Resources
- The U.S. Government's Official Web Portal, www.firstgov.gov

---

60   NGA, Center for Best Practices, "State Intelligence Fusion Centers: Recent State Actions," 2005.

Guideline 18

Develop and implement a communications plan within the fusion center; among all involved law enforcement, public safety, and private sector agencies and entities; and with the general public.

Communications Plan

Justification

Communication is essential to fusion center operations. Fusion center leadership must be able to communicate with center personnel and representatives, should the need arise. With the inclusion of public safety and private sector partners, communication needs become complex. Public safety and private sector entities may not always be present in the fusion center daily activities but are key partners in its operation. With a variety of communication options, centers should develop levels of communication, backup communication procedures, and emergency contact protocols. Since September 11, there has been a focus on interoperability within the law enforcement community and among first responders (e.g., fire and EMS). It is important to have interoperability between fusion center representatives. If communications systems are not interoperable, the effort will be futile. The general public is also an integral part of the communications plan. They may report information and events to the fusion center, and in the event of a terrorist attack or crime incident, the public must be kept informed of the situation.

Various types of communication include:

- E-mail
- Electronic notification to pagers and cell phones
- Hard line telephone
- Secured line telephone
- Satellite telephone
- Fax machine
- Video teleconferencing
- Handheld radio
- Password-protected Web page for posting information
- Face-to-face
- Alert notification systems
- Wi-Fi
- Mesh networks

Personnel and partners within the fusion center should be aware of the different types of information that may be communicated within the fusion center, including public, sensitive, proprietary, and secret. These different classification types should determine how fusion centers share information. Fusion center personnel should have a clear understanding of what the classifications are and how they apply to information sharing.

When fusion centers develop a communications plan, leadership should anticipate that in the event of a terrorist attack or large-scale emergency, phone lines will quickly be tied up or disabled and phone service lost; therefore, alternate communication means should be included in the communications plan. For example, if landline and all phone voice circuits are jammed, the use of text messaging may be a viable option. Similarly, if power is available and voice circuits are jammed, Internet messaging can be utilized. The communications plan should also include personnel recall procedures and, for those entities that do not supply a full-time member to the fusion centers, liaison call-out procedures.

Fusion centers should identify a public information officer (PIO) to aid in the coordination of public and media inquiries into the fusion center. In the event of a disaster (man-made or natural), a PIO will aid in ensuring that fusion center staff are not hindered from conducting their duties and redirected to answering media queries. A PIO may also perform in a proactive awareness capacity, informing the media and the public of ongoing operations and success stories within the fusion center.

Issues for Consideration

When identifying communications needs, consider:

- Determining how fusion center components will communicate during a disaster.
- Identifying an alternative power source for communications when traditional utilities are unavailable.
- Creating a tier system for communications based on threat level.
- Ensuring the existing communication capabilities between components and entities are interoperable.

- Ensuring that all entities have appropriate communication tools (e.g., video-teleconferencing equipment, pagers, or cell phones with text-messaging capabilities).

- Incorporating current communications plans that are utilized by law enforcement and emergency services (including hospitals, EMS, and fire).

- Obtaining a cache of radios for fusion center personnel to use in emergency situations.

- If the communications plan includes radio communication, meeting with law enforcement to identify a fusion center radio channel (e.g., special events channel or special operations channel).

- Setting aside a phone line only accessible to fusion center personnel and partnering entities for emergency communications.

- Including a section that addresses testing the plan to ensure operability and maintenance of current contact information for fusion center participants.

- Creating redundancy in the communications plan.

- In advance of an emergency, consulting with the local telephone provider about available backup and alternative communications options for the fusion center, including mobile cellular sites.

- Equipping the center with a satellite phone to ensure communication beyond the local radio net when, in an emergency, standard connectivity is lost.

Available Resources on Fusion Center CD

- *State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning*, Chapter 4, http://www.fema.gov/pdf/plan/4-ch.pdf

Next Steps

Fusion centers should strive to institutionalize the relationships established with its law enforcement, public safety, and private sector partners. It is through these relationships that the center will be truly effective in the prevention and deterrence of crime and terrorism. As relationships are institutionalized, mistrust and fear of information disclosure will diminish and effective and efficient information and intelligence sharing will be seamless. Furthermore, in the event of a disaster or major crime incident, these relationships will be vital in successfully investigating the crime or getting essential services back online. In order for the relationships within the fusion center to be institutionalized, fusion center governance should have ongoing dialogue with public and private sector leadership and agency heads. Fusion centers should become involved in existing industry networks and organizations, such as credit card fraud networks. Through these established networks, fusion centers can demonstrate effectiveness in using the intelligence and fusion processes.

Training must also occur between center personnel and their public and private partners for successful integration. This training includes awareness of the intelligence and fusion processes, the types of information and intelligence crucial to crime prevention, the function of the fusion center and how it operates, and an understanding of the types of information that the public and private sector entities can provide to the center. Fusion center training should also include joint tabletop, functional, and full-scale exercises with law enforcement, public safety, and private sector partners. These exercises will aid

in identifying the role and the information requirements of both the fusion center and the components and will also test the communications plan.

Fusion centers represent a capability for law enforcement, public safety, and private sector entities to securely develop and share information and intelligence in an innovative, effective, and efficient manner. Many of the issues impacting fusion centers have been addressed in this report, specifically those affecting their intelligence function. Undeniably, as centers are established, additional issues will arise, best practices will emerge, and future needs will be identified. This document is not meant to be all inclusive; instead, the recommendations contained herein are the foundation for a much larger and complex enterprise. As this process continues, the members of the three focus groups remain committed to sharing information about fusion center development, operations, and services with all levels of law enforcement. Further developments and materials will be provided on the Office of Justice Programs (OJP) Web site at www.it.ojp.gov.

As recommended in this report, fusion centers should be established in all states to allow for the maximum capability of intelligence and information exchange. Although these guidelines are not meant to be mandatory, focus group members urge funding agencies and others to promote and adhere to these minimum guidelines.

Moving from a reactive response approach to a proactive and preventive approach will improve law enforcement's ability to detect and prevent crime and public safety personnel's capability to respond to emergencies. The fusion center concept is an opportunity to bring together critical resources and produce meaningful information and intelligence for dissemination to the right people at the right time for the right reasons. Through collective and collaborative implementation, the center, its personnel, and the citizens the center serves will benefit.

A key benefit of fusion centers is minimizing duplication. The U.S. Department of Homeland Security (DHS), the U.S. Department of Justice (DOJ), and the states must be cognizant of existing fusion centers and those currently under development (including the Urban Area Security Initiative [UASI] regions) and leverage and enhance the centers that currently exist.

Distribution of the *Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector* is important for the maximum effectiveness of fusion centers. It is recommended that DOJ and DHS spearhead efforts to ensure that the guidelines are distributed to all key components and entities of fusion centers, including law enforcement, public safety, and private sector entities.

Appendix A
Focus Group Participants and Acknowledgements

Law Enforcement Intelligence Fusion Center Focus Group Participants

Norm Beasley, Lieutenant Colonel
Arizona Counter Terrorism Information
    Center

Kenneth A. Bouche, Colonel
Illinois State Police

Roger Bragdon, Chief
Spokane, Washington, Police Department

David Carter, Ph.D.
Michigan State University

Stephen Clark
Georgia Emergency Management Agency

Daniel Cooney, Captain
Upstate New York Regional Intelligence
    Center

C. Patrick Duecy
CPD Consultants, LLC

John T. Elliff
Federal Bureau of Investigation

Dennis Ellis, Lieutenant
Indiana State Police

William Fennell, Program Manager
U.S. Drug Enforcement Administration

Max Fratoddi
Counterdrug Intelligence Executive
    Secretariat

Bob Hardin, Inspector
Georgia Bureau of Investigation

**Chris Holmes, Deputy Program
Manager**
ManTech Information Systems and
    Technology
U.S. Department of Homeland Security

Cliff Karchmer, Director
Police Executive Research Forum

Clark Kimerer, Deputy Chief
Seattle, Washington, Police Department

Mark Marshall, Chief
Smithfield, Virginia, Police Department

Jerry Marynik, Administrator
State Terrorism Threat Assessment
    Center
California Department of Justice

Mary Meyer, Officer
Minnesota Department of Public Safety

Peter A. Modafferi, Chief
Rockland County, New York, District
    Attorney's Office

Doug Poole, Acting Chief
U.S. Drug Enforcement Administration

Russ Porter, Chief
Iowa Department of Public Safety

Don Robertson
Georgia Bureau of Investigation

Richard A. Russell, Director
U.S. Department of Homeland Security

Kurt Schmid, Senior Advisor
Office of National Drug Control Policy

**Clark Smith, Senior Information
Technology Specialist**
U.S. Department of Justice

Mike Snyders, Lieutenant Colonel
Illinois State Police

Nicholas Theodos, Major
New Jersey State Police

Mark Zadra, Chief of Investigations
Florida Department of Law Enforcement

Public Safety Fusion Center Focus Group Participants

Richard Andrews, Senior Director
National Center for Crises and Continuity
Coordination

Robert Belfiore, Chief
Port Authority of New York and New
Jersey

Grea Bevis, Bureau Chief
Florida Department of Environmental
Protection

Kenneth A. Bouche, Colonel
Illinois State Police

Michael Caldwell, M.D., M.P.H.
National Association of County and City
Health Officials
Dutchess County, New York, Health
Department

John Cohen, Policy Advisor
Massachusetts Executive Office of Public
Safety

Thomas Frazier, Executive Director
Major Cities Chiefs Association

Donna Hunsaker, Ph.D.
Kentucky Medical Examiner

John Hunt, Major
New Jersey State Police

Bart R. Johnson, Colonel
New York State Police

Art Johnstone, Director
Florida Department of Agriculture and
Consumer Services

Clark Kimerer, Deputy Chief
Seattle, Washington, Police Department

Fred LaMontagne, Chief
Portland, Maine, Fire Department

Peter A. Modafferi, Chief
Rockland County, New York, District
Attorney's Office

Thomas J. O'Reilly, Administrator
New Jersey Office of the Attorney General

Joseph M. Polisar, Chief
Garden Grove, California, Police
Department

Thomas J. Richardson, Captain
Seattle, Washington, Fire Department

Mark Zadra, Chief of Investigations
Florida Department of Law Enforcement

Private Sector Fusion Center Focus Group Participants

Richard Andrews, Senior Director
National Center for Crises and Continuity
Coordination

**Drew Arena, Assistant General
Counsel for Legal Compliance**
Verizon Communications

Roy Barnes, Manager
General Motors Corporation

**Earnest A. Blackwelder, Senior Vice
President**
Business Executive for National Security

Kenneth A. Bouche, Colonel
Illinois State Police

John Cohen, Senior Advisor
Massachusetts Executive Office of Public
Safety

**Michael Cohen, Deputy Regional
Director**
Citigroup Security and Investigative
Services

Jack Faer, President
Fidelity Investments

Shawna French-Lind
Wal-Mart Stores, Inc.

Bart R. Johnson, Colonel
New York State Police

Art Johnstone, Director
Florida Department of Agriculture and
Consumer Services

Lynne D. Kidder, Vice President
Business Executives for National Security

**Maurice McBride, Secretary and
Attorney**
National Petrochemical and Refiners
Association

Kathleen McChesney, Vice President
The Walt Disney World Company

Freeman Mendell, First Assistant
Information Technology Systems

**Laurence Mulcrone, Director of
Security and Safety**
McCormick Place/Navy Pier

**Colin Nurse, National Technology
Officer, State and Local Government**
Microsoft Corporation

Thomas J. O'Reilly, Administrator
New Jersey Office of the Attorney General

Russell Porter, Assistant Director
Iowa Department of Public Safety

Daniel Rattner, Principal
D. M. Rattner and Associates

**Richard Ryan, Assistant Deputy
Director, Corporate Security**
Archer Daniels Midland Company

Dan Sauvageau, Vice President
Fidelity Investments

Thomas Seamon, Chair
Private Sector Liaison Committee
Chairman
International Association of Chiefs of
Police

Acknowledgements

Appendix B
Fusion Center CD Resources

Guideline 1—The NCISP and the Intelligence and Fusion Processes

- 10 Simple Steps to help your agency become a part of the *National Criminal Intelligence Sharing Plan*
- HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*
- Law Enforcement Intelligence Unit (LEIU) Audit Checklist
- *National Criminal Intelligence Sharing Plan* report

Guideline 2—Mission Statement and Goals

- *A Staircase to Strategic Planning: Mission*, The Community Policing Consortium, www.communitypolicing. org/mission.html

Guideline 3—Governance

- Bylaws Sample Template
- Board Guidelines, www.mapnp.org/ library/boards/boards.htm
- Global Justice Information Sharing Initiative Advisory Committee Bylaws, http://it.ojp.gov/documents/ GACBylaws.pdf
- Organization and Association Resource List
- Parliamentary Procedures, www. rulesonline.com

Guideline 4—Collaboration

- "Community Collaboration," www. communitycollaboration.net

Guideline 5—Memorandum of Understanding (MOU) and Non-Disclosure Agreement (NDA)

- 28 CFR Part 23 Sample MOU
- Arizona Counter Terrorism Information Center MOU
- California Public Records Exemption
- Canada Department of Defense (DOD) MOU Guidelines
- DHS Non-Disclosure Agreement, www.fas.org/sgp/othergov/dhs-nda.pdf
- Florida Statute 119.071
- Freedom of Information Act, www. usdoj.gov/04foia
- Joint Terrorism Task Force MOU
- Massachusetts Statute
- MOU Sample Template
- Rockland County Intelligence Center MOU
- Upstate New York Regional Intelligence Center MOU

Guideline 6—Database Resources

- El Paso Intelligence Center (EPIC), www.usdoj.gov/dea/programs/epic. htm
- FBI's LEO Program, www.fbi.gov/hq/cjisd/leo.htm
- FBI's N-DEx Program
- FBI's R-DEx Program
- Financial Crimes Enforcement Network (FinCEN), www.fincen.gov
- High Intensity Drug Trafficking Areas (HIDTA), www.whitehousedrugpolicy. gov/hidta/index.html
- Homeland Security Information Network (HSIN), www.dhs.gov/ dhspublic/display?content=3350
- International Association of Crime Analysts (IACA), www.iaca.net
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org
- International Criminal Police Organization (INTERPOL), www. usdoj.gov/usncb
- Law Enforcement Intelligence Unit (LEIU), www.leiu-homepage.org/ index.php
- National Crime Information Center (NCIC), www.fbi.gov/hq/cjisd/ncic.htm
- National Drug Intelligence Center (NDIC), www.usdoj.gov/ndic
- National White Collar Crime Center (NW3C), www.nw3c.org and www. training.nw3c.org
- Nlets—The International Justice and Public Safety Information Sharing Network, www.nlets.org
- RISS Automated Trusted Information Exchange (ATIX), www.rissinfo.com/ rissatix.htm
- RISSNET™, www.rissinfo.com

Guideline 7—Interconnectivity

- *A Critical Look at Centralized and Distributed Strategies for Large-Scale Justice Information Sharing Applications* (a white paper prepared by the IJIS Institute)
- *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)*, http://it.ojp.gov/documents/200409_Global_Infrastructure_Report.pdf
- Global Justice XML Data Model (Global JXDM), www.it.ojp.gov/gjxdm
- Justice Information Exchange Model, www.search.org/programs/info/jiem.asp
- Model Intelligence Database Policy

Guideline 8—Privacy and Civil Liberties

- Audit Checklist (LEIU), www.it.ojp.gov/documents/LEIU_audit_checklist.pdf
- Global's *Privacy and Information Quality Policy Development for the Justice Decision Maker*, http://it.ojp.gov/documents/200411_global_privacy_document.pdf
- National Criminal Justice Association—*Justice Information Privacy Guideline*, www.ncja.org/pdf/privacyguideline.pdf
- *Privacy and Civil Rights Policy Templates for Justice Information Systems*
- Privacy Policy Sample Template
- *Privacy Policy Development Guide*

Guideline 9—Security

- *Applying Security Practices to Justice Information Sharing*, http://it.ojp.gov/documents/asp/introduction/index.htm
- Critical Infrastructure Information Act of 2002, www.dhs.gov/interweb/assetlibrary/CII_Act.pdf
- National Institute of Standards and Technology (NIST) template and example policies, http://csrc.nist.gov/fasp
- *Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs*, U.S. Department of Homeland Security, May 2005

Guideline 10—Facility, Location, and Physical Infrastructure

- Executive Orders 12068, 12958, and 13292 Regarding Classified Information
- FBI Security Clearance and Frequently Asked Questions
- GSA's *Facilities Standards for the Public Buildings Service*
- *IACP Police Facility Planning Guidelines: A Desk Reference for Law Enforcement Executives*, www.iacp.org/documents/pdfs/Publications/ACF2F3D%2Epdf
- National Institute of Standards and Technology, "Contingency Plan Template," http://csrc.nist.gov/fasp/FASPDocs/contingency-plan/contingencyplan-template.doc

Guideline 11—Human Resources

- *Law Enforcement Analytic Standards*, http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf
- Personnel Sample Checklist

Guidelines 12 and 13—Training of Center Personnel/Multidisciplinary Awareness and Education

- Counter-Terrorism Training Coordination Working Group (CTTWG) Web site, www.counterterrorismtraining.gov
- HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report
- Homeland Security Presidential Directive 5 (HSPD-5), www.whitehouse.gov/news/releases/2003/02/20030228-9.html
- Homeland Security Presidential Directive 8 (HSPD-8), www.fas.org/irp/offdocs/nspd/hspd-8.html
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org/
- International Association of Directors of Law Enforcement Standards and Training (IADLEST), www.iadlest.org/

- *Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies,* www.it.ojp.gov/documents/minimum_criminal_intel_training_standards.pdf
- National White Collar Crime Center (NW3C), www.nw3c.org

Guideline 14—Intelligence Services and Products

- DHS's *National Response Plan*, December 2004
- *Terrorism Protection Manual*, FDLE, February 28, 2003

Guideline 15—Policies and Procedures

- 28 CFR Part 23, www.iir.com/28cfr/Overview.htm
- *Evaluation Checklists for Intelligence Units*, Paul R. Roger
- IACP's *Criminal Intelligence Model Policy*
- Law Enforcement Intelligence Unit's (LEIU) *Criminal Intelligence File Guidelines*, http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf
- *Justice Information Privacy Guideline*, www.ncja.org/pdf/privacyguideline.pdf
- *Privacy Policy Development Guide*, http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Guideline 16—Center Performance Measurement and Evaluation

- Office of Management and Budget, www.omb.gov
- Target Capabilities List, Version 1.1, www.ojp.usdoj.gov/odp/docs/TCL11.pdf

Guideline 17—Funding

- Summary of Funding Resources
- The U.S. Government's Official Web Portal, www.firstgov.gov

Guideline 18—Communications Plan

- *State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning*, Chapter 4, http://www.fema.gov/pdf/plan/4-ch.pdf

Organization Links

- CopNet, www.copnet.org
- Defense Information Systems Agency, www.disa.mil
- FBI Terrorism Information, http://www.fbi.gov/terrorinfo/counterrorism/waronterrorhome.html
- International Association of Crime Analysts (IACA), www.iaca.net
- International Association of Law Enforcement Intelligence Analysts (IALEIA), www.ialeia.org
- Integrated Justice Information Systems Institute, www.ijis.org

- National Association of Counties, www.naco.org
- National Association of State Chief Information Officers, www.nascio.org
- National Governors Association's Project on Justice Information Sharing, www.nga.org
- Office of Management and Budget, www.omb.gov
- Office of Justice Programs, U.S. Department of Justice, www.it.ojp.gov
- Regional Information Sharing Systems®, www.rissinfo.com

- SEARCH, The National Consortium for Justice Information and Statistics, www.search.org
- Terrorism Research Center, www.terrorism.com
- U.S. Department of Defense News, www.defendamerica.mil
- U.S. Department of Homeland Security, www.dhs.gov
- U.S. Department of Justice, www.justice.gov
- U.S. Department of State, www.state.gov/s/ct

Appendix C
Functional Categories

Collaboration and integration are key to the success of fusion centers. The Public Safety and Private Sector Fusion Center Focus Groups (FCFGs) developed overarching functional categories composed of the different entities that make up these components. The categories are not comprehensive but provide a starting point for fusion centers to utilize when integrating the different facets of law enforcement, public safety, and the private sector. Individual fusion centers should identify the critical entities within their particular jurisdiction to incorporate into the center. The categories include:

- Agriculture, Food, Water, and the Environment
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Criminal Justice
- Education
- Emergency Services (Non-Law Enforcement)
- Energy
- Government
- Health and Public Health Services
- Hospitality and Lodging
- Information and Telecommunications
- Military Facilities and Defense Industrial Base
- Postal and Shipping
- Private Security
- Public Works
- Real Estate
- Retail
- Social Services
- Transportation

Information received from these categories and associated entities should be used for threat and crime prevention. Applicable local, state, and federal laws should be followed when information is provided to fusion centers. In addition, this information may be used for criminal investigations with an identified criminal predicate.

Agriculture, Food, Water, and the Environment

This category is composed of entities that focus on the food and water supply chain, from the raising/production of food and water to the distribution to consumers. Entities within this category can provide fusion centers with a variety of strategic and tactical information. It may include critical infrastructure information regarding the location of agriculture-related entities, including the location of livestock and processing plants, as well as types of chemicals used at processing plants and how they are stored; the location of water storage facilities and suspicious activity surrounding these facilities; and any unusual tampering of food products. In addition, these entities can provide fusion centers with information regarding suspicious incidents that may occur relating to agriculture and agricultural-related crime trends. Subject-matter experts can provide fusion centers with resources and expertise when agricultural-related threats are identified.

Listed below are various entities that fusion centers should consider for integration.

- U.S. Department of Agriculture (USDA), www.usda.gov/
- U.S. Department of Health and Human Services, www.hhs.gov
- U.S. Environmental Protection Agency, www.epa.gov
- State agriculture departments
- Food/water production facilities (farm/ranch/preharvest)
- Food/water processing facilities
- Grocery stores/supermarkets
- Restaurants
- Information Sharing Analysis Centers (ISAC)
  - ✓ Agriculture
  - ✓ Food
  - ✓ Water
- Food and Agriculture Sector Coordinating Council

Banking and Finance

This category is composed of financial entities, including banks, investment firms, credit companies, and government-related financial departments. Entities within this category can provide fusion centers with information related to the banking industry, including suspicious activity, critical infrastructure information, and crime trends (e.g., fraud, identity theft, and suspicious activity reports). Entities within this category may also provide fusion centers with tactical information, including information to aid

in ongoing criminal investigations, e.g., account information and credit history (with applicable legal authorization). The entities include:

- U.S. Department of the Treasury, www.ustreas.gov
  - ✓ Financial Crimes Enforcement Network (FinCEN), www.fincen.gov
- State financial departments
- Banking companies
- Investment companies
- Credit card companies
- Credit report companies
- Securities firms
- Financial services ISAC
- Financial Services Sector Coordinating Council www.fsscc.org/

Chemical Industry and Hazardous Materials

This category is composed of entities that are responsible for the production, storage, transportation, and delivery of chemicals and other hazardous materials. These entities may provide fusion centers with information on types of chemicals and hazardous materials, how chemicals and hazardous materials may affect a contaminated area, suspicious activity relating to the chemical industry or hazardous materials, and critical infrastructure information. The entities include:

- U.S. Environmental Protection Agency (EPA), www.epa.gov
- U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov/
- State environmental departments (e.g., Natural Resources and Environmental Protection)
- Fire departments and/or local hazardous material response agencies
- Chemical industry
- Chemtrec: 24/7 Emergency Communications Center for the chemical industry
- Chemical industry ISAC
- National Petrochemical and Refiners Association, www.npradc.org/
- American Chemistry Council,

www.americanchemistry.com
- Pharmaceutical companies

Criminal Justice

These are components of local, state, tribal, and federal governments and are responsible for the management of criminal conviction, incarceration, reform, and reintegration (i.e., law enforcement, courts, and corrections). This category can provide fusion centers with a variety of information, including crime trends and threat assessments. In addition, this component can provide booking photos, biographical information, and historical criminal activity regarding persons, businesses, and organizations. Criminal justice entities can provide fusion centers with strategic and tactical information and intelligence.

The following is a compilation of organizations that should be considered when integrating the criminal justice sector into fusion centers. This list is not exhaustive but should be used as a foundation. Also provided are examples of the types of information available to share. The entities include:

Law Enforcement Agencies: Can provide fusion centers with a variety of information, including crime trends, drug and threat assessments, case information (violent crime, economic crime, narcotics, and terrorism), seizure information, and criminal activity, both historical and current, on persons, businesses, organizations, and locations.

- Local law enforcement
  - ✓ City and county
  - ✓ College and university police departments
- State law enforcement
  - ✓ Highway patrol
  - ✓ State agencies with investigations bureaus
- Tribal law enforcement
- Federal law enforcement
  - ✓ Federal Bureau of Investigation
  - ✓ U.S. Marshals Service
  - ✓ U.S. Drug Enforcement Administration
  - ✓ Bureau of Alcohol, Tobacco, Firearms and Explosives
  - ✓ U.S. Immigration and Customs Enforcement

- ✓ U.S. Secret Service
- ✓ U.S. Postal Inspection Service
- ✓ U.S.P.S. Office of Inspector General
  - ○ Court System: Can provide information on criminal cases, criminal history, dispositions, and biographical information on targets.
- County clerk of courts
- Criminal justice information systems
- U.S. courts

Corrections Agencies: Can provide fusion centers with booking photos, last known addresses, gang information, names of associates and relatives (visitors), and biographical information.

- County jail
- State prison system
- Federal Bureau of Prisons

Probation and Parole Agencies: Can provide information regarding employment information of suspects and current addresses of suspects.

- Probation officers
- Parole board

Education

This category is composed of organizations and businesses that are responsible for the education of children and adults. Entities within this component can provide fusion centers with information regarding suspicious activities occurring on and around school grounds, as well as information on critical infrastructure and associated risk assessments. In addition, in the event of a terrorist incident or crime relating to schools, it is important for fusion centers to have established partnerships to aid in communication and information flow. The entities include:

- Day care centers
- Preschools
- Primary and secondary schools
- Postsecondary schools
  - ✓ Colleges and universities
- Technical schools

Emergency Services (Non-Law Enforcement)

Entities within this category are components of local, state, tribal, and federal governments and are responsible for the protection and safety of lives and property within a jurisdiction. Commonly one of the first responders to an incident, the Emergency Medical Services category can provide both strategic and tactical information. Below is a list of emergency services entities; this list is not comprehensive but provides fusion centers with a foundation to build on. The entities include:

Fire: Can provide assessments on types of fires, how specific fires are started, and ongoing fire investigation information.

- Local fire departments
- Private fire departments
- U.S. Fire Administration, www.usfa.fema.gov
- U.S. Fire Marshal
- Forestry departments

Emergency Medical Services (EMS): Can provide information regarding types of injuries occurring at an incident and suspicious activity that EMS technicians may observe while performing official duties.

- Local fire departments
- Hospital
- Private EMS services

Hazardous Materials: Can provide information on different types of hazardous materials and hazardous material spills, as well as incident and operations data.

- Local fire departments
- Environmental Protection Agencies
- U.S. Department of Transportation, Office of Hazardous Materials Safety, http://hazmat.dot.gov/
- Private hazardous material contractors

Emergency Management: Can provide information on location of critical infrastructure, notifications of declared emergencies, and threat assessments.

- Emergency management directors
- Federal Emergency Management Agency

Civil Air Patrol: Can offer a variety of services, including homeland security missions, counterdrug missions, and search-and-rescue operations.

Health: Depending on the incident (e.g., white powder incidents), health department representatives may take part in response efforts. See the Health and Public Health Services category for additional health information.

Energy

This category contains entities that focus on the development and distribution of energy-related products. These entities can provide strategic and tactical information, including critical infrastructure information, risk assessments, and suspicious incidents. This list is not comprehensive, and the energy component should be evaluated in each jurisdiction to determine fusion center needs. The entities include:

- U.S. Department of Energy, www.energy.gov
- Nuclear power plants
- Electricity companies
- Utilities
- Oil companies
- Natural gas companies
- North American Electric Reliability Council

Government

This category is composed of entities that enable the government to carry out its official duties, including licensing and regulation of entities (people, businesses, and organizations). These entities vary but should be considered for inclusion into fusion centers. The following list is not exhaustive, and the fusion center should determine what entities to include.

Game and Fish: Can provide fusion centers with information on suspicious activity as it relates to boating, such as information regarding criminal investigations (e.g., drug interdiction and vessel identification).

Government Administration: Can provide various types of information pertaining to tax and title, critical infrastructure, emergency planning, and civil records, including property appraiser, mortgages, deeds, and civil suits.

Motor Vehicle Administration: Can provide tactical information to fusion centers regarding driver's license information, motor vehicle registration, vehicle body files, and suspicious information concerning attempts to obtain driver's licenses.

Parks and Recreation Departments: Can provide information regarding suspicious activity in and around local parks.

U.S. Division of Forestry: Can provide information regarding suspicious activities within a national park involving persons, vehicles, and fires.

Health and Public Health Services

These entities are composed of local, state, tribal, and federal government agencies and the private sector and are responsible for protecting and improving the health of citizens. The following is a compilation of organizations that should be considered when integrating the health services sector into fusions centers. This list is not exhaustive but should be used as a foundation for collaboration.

This category can provide strategic and tactical information. In addition, these entities have access to information regarding critical health services within a certain community or nationwide. This information can identify the readiness of a given area to respond to a safety threat. Health services agencies may also provide information to fusion centers regarding prescription drug trends, disease outbreaks, and vital statistics information. Agencies within this category also monitor and track medicine and vaccine supplies and are capable of identifying gaps in availability.

A variety of these agencies should be considered for participation in certain fusion center situations. For example, in rural areas, veterinary hospitals may be the only medical facilities available. In times of crises, many of these hospitals will be capable of serving as triage centers. The veterinary profession is also a critical link to the health and productivity of animal agriculture, including the fight against agroterrorism. The entities include:

Health Departments: Can provide information on disease trends, local disease outbreaks, and vital statistics.

- Local and state health departments
- U.S. Department of Health and Human Services, www.hhs.gov

Hospitals: Can provide information regarding suspicious incidents and patient information. In addition, hospitals are vital in response efforts to gauge types of injuries, total number injured, and hospital capacity.

Disease Control: Can provide disease assessments, information regarding disease outbreaks, and information on laboratories that can assist with response and recovery efforts.

- Local and state health departments
- Centers for Disease Control and Prevention (CDC), www.cdc.gov

Food Safety: Can provide information regarding food and waterborne diseases, including reporting of suspicious incidents and investigative efforts.

- Health departments
- Centers for Disease Control and Prevention, www.cdc.gov/foodborneoutbreaks/
- U.S. Department of Agriculture, www.fsis.usda.gov/Fact_Sheets/index.asp

Medical Examiners/Death Investigators: Can provide information regarding suspicious deaths, types of death, and causes of death.

Mental Health Facilities: Can aid in response and recovery efforts.

Pharmaceutical: Can provide stockpile information and information relating to critical infrastructure and suspicious activity surrounding chemical plants.

Primary Care Physicians: Can provide information regarding suspicious injuries and diseases and biographical information.

Veterinary: Can provide information relating to suspicious activities regarding disease outbreaks in animals and can aid in response efforts.

- Center for Veterinary Medicine, www.fda.gov/cvm/default.html

Hospitality and Lodging

These entities focus on sports, entertainment, tourism, and recreation. Entities within this category may provide information regarding suspicious persons or activity, critical infrastructure information, investigative information (e.g., access to Closed Circuit Television [CCTV]), and trends in crime-related activity. The entities include:

- Gaming industry
- Sports authority
- Sporting facilities
- Amusement parks
- Cruise lines
- Hotels, motels, and resorts
- Convention centers

Information and Telecommunications

This category is composed of the information technology and communications-related industry, including computer operating systems, hardware and software companies, Internet service providers, and telephone companies. This category can provide a variety of information. Information technology entities can provide expertise and information on computer trends, including viruses, computer-hacking incidents, and cyber security initiatives. Telecommunications entities can provide information on critical infrastructure, suspicious incidents, and ongoing case support with proper authorization. These entities include:

Information Technology
- State technology offices
- InfraGard, www.infragard.net/
- Computer and software companies
- IT Sector Coordinating Council

Communications
- Media transmission towers
- Communications Infrastructure Sector Coordinating Council

Telecommunication
- Internet service providers
- Electronic mail providers

- Federal Communications Commission (FCC)
- Telecommunications companies
  - ✓ Wireless
  - ✓ Hard-line

Cyber Security
- Information Technology ISAC
- Research and Education Networking ISAC
- Multi-State ISAC
- United States Computer Emergency Readiness Team (US-CERT), www.us-cert.gov
- National Cyber Security Division (NCSD) Law Enforcement and Intelligence Branch

Military Facilities and Defense Industrial Base

These entities may provide military expertise, critical infrastructure information, and information relating to response efforts and suspicious incidents around military bases. This category includes:

Military Base Security: Can provide information relating to suspicious incidents that occur on and around military bases, information on persons who have attempted to gain access to the base without permission, and critical infrastructure information.

National Guard: Can provide information regarding critical infrastructure, risk assessments concerning military entities, and information related to weapons of mass destruction (WMD).

Defense Contractors: Companies providing products and services to support military operations.

Postal and Shipping

This category consists of entities whose primary responsibility is the delivery of mail and packages, from both a public and private perspective. The Postal and Shipping category can provide tactical and strategic information regarding types of mail-outs private companies are distributing that may look suspicious, suspicious packages that are being mailed out, and ongoing criminal investigations. The post office can, with proper authorization, provide information

to fusion centers about the types of mail that are being sent to target homes or businesses. The entities include:

- U.S. Post Office
- Shipping companies

Private Security

When establishing a fusion center, private security entities should be considered because they may be able to provide critical infrastructure information, suspicious activity reports, and business continuity plans. The entities include:

- Corporate security offices
- Private security companies
- Alarm companies
- Armored car companies
- Investigative firms

Public Works

These entities are responsible for infrastructure created for public use. Entities within this category may provide information regarding suspicious activity and critical infrastructure, as well as subject-matter experts who may help identify risks associated with public works. The entities include:

- State department of transportation
- Water management districts
- Sanitation
- Waste management
- Road construction companies

Real Estate

These entities focus on the real estate-related industry. Entities within this category can provide information regarding suspicious activities (e.g., suspicious fires, persons, and activities) and ongoing case-related information with proper authorization. The entities include:

- Apartment facilities
- Facility management companies
- Housing authorities
- Real Estate ISAC

Retail

These companies and organizations are involved in the retail industry; this can include shopping malls, wholesale stores, distribution centers, and online stores. These entities may provide information on suspicious activity in and around the shopping complex, identification of vulnerabilities associated with the complex, critical infrastructure information, and investigative leads, including CCTV information. The entities include:

- Malls
- Retail stores
- Shopping centers

Social Services

These entities are composed of local, state, tribal, and federal government agencies and the private sector and are responsible for providing services that help improve people's standard of living.

This category can provide information regarding the function and responsibilities of many available programs and services. Social service agencies can be the source of a variety of information, including welfare fraud. These programs and services can provide community support, education, and planning assistance in preparation for and response to a potential terrorist attack. The entities include:

State and Child Welfare: Can provide information regarding welfare fraud, electronic benefits transfer fraud, biographical information on targets of investigations and, with proper authorization, employment-related information on targets.

- U.S. Department of Health and Human Services
- Department of Children and Families

Mental Health Facilities: Can aid in response and recovery efforts.

Transportation

Each level of government (local, state, tribal, and federal) and the private sector have transportation entities whose responsibilities include aviation, rail, public transportation, highway, and maritime services. Both governmental and private transportation entities should be considered when jurisdictions are establishing a fusion center. The following is a compilation of organizations that should be considered when integrating the transportation sector. This list is not exhaustive but should be used as a foundation.

This category can provide access to information regarding the various transportation corridors throughout the United States. Further, it can offer both strategic and tactical information that can be incorporated into the intelligence and fusion processes. Transportation-related agencies can identify the risks and vulnerabilities of potential target areas, such as roads and railways that have direct access to hazardous waste sites and ports that house information on the types of ships that are docked and the cargo they carry. The entities include:

Aviation: Can provide information regarding airport critical infrastructure, suspicious activity, items that have been confiscated, accident analyses, and types of cargo that are being shipped.

- Transportation Security Administration (TSA), www.tsa.gov
- Office of Aviation Safety (Component of National Transportation Safety Board [NTSB]), www.ntsb.gov
- Federal Aviation Administration (FAA), www.faa.gov
- Aviation Safety Reporting System (ASRS), http://asrs.arc.nasa.gov/
- State department of transportation
- State aeronautics commission
- Airport authority
- Commercial airline carriers
- Private shipping companies (e.g., FedEx and UPS)

Highway: Can provide information on critical infrastructure, traffic crashes, interdiction efforts, illegal products that have been seized, and cargo information.

- Federal Highway Administration (FHWA), www.fhwa.dot.gov
- Federal Motor Carrier Safety Administration (FMCSA), www.fmcsa.dot.gov
- National Highway Traffic Safety Administration (NHTSA), www.nhtsa.dot.gov
- Office of Highway Safety (Component of NTSB), www.ntsb.gov/Surface/highway/highway.htm
- State department of transportation
- Turnpike authority
- Public transit

Maritime: Can provide information on port critical infrastructure, vessel information, cargo information, suspicious activity, and contraband seizures.

- U.S. Coast Guard, http://www.uscg. mil/USCG.shtm
- Maritime Administration (MARAD), www.marad.dot.gov/index.html
- Saint Lawrence Seaway Development Corporation (SLSDC), www.seaway. dot.gov
- Office of Marine Safety (Component of NTSB), www.ntsb.gov/surface/marine/ marine.htm
- Port authority
- Ports council
- Bridge and tunnel authority
- Harbor master and/or commander

Rail: Can provide information on critical infrastructure (e.g., the location of rail lines) and types of cargo being shipped, including hazmat information. Various private sector rail entities also have law enforcement components.

- Federal Railroad Administration (FRA), www.fra.dot.gov
- Federal Transit Administration (FTA), http://transit-safety.volpe.dot.gov
- Surface Transportation Board (STB), www.stb.dot.gov
- Office of Railroad, Pipeline, and Hazardous Materials Safety (Component of NTSB), www.ntsb. gov/railroad/railroad.htm
- State department of transportation
- Rail authority
- American Railroad Association

Appendix D
HSAC Homeland Security Intelligence and Information Fusion Report
April 28, 2005

U.S. Department of Homeland Security
Homeland Security Advisory Council

Intelligence And Information Sharing
Initiative: Homeland Security Intelligence
& Information Fusion

Joseph J. Grano, Jr.
Chairman
Homeland Security Advisory Council

William H. Webster
Vice Chairman
Homeland Security Advisory Council

Daniel J. Ostergaard
Executive Director
Homeland Security Advisory Council

Mitt Romney
Chairman
Intelligence & information Sharing
    Working Group

John Cohen
Executive Director
Intelligence & information Sharing
    Working Group

Michael J. Miron
Director
Intelligence & information Sharing
    Working Group

Background

Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about who the enemies are,[61] where

---

61   Including their capabilities, intentions, strengths, weaknesses.

and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use. This information should serve as a guide for efforts to:

- Identify rapidly both immediate and long-term threats;

- Identify persons involved in terrorism-related activities; and

- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism–related information. It can come through the efforts of the intelligence community; Federal, State, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, healthcare, general government), and the private sector (e.g., transportation, healthcare, financial, Internet/information technology).

For the most part, terrorism-related information has traditionally been collected outside of the United States. Typically, the collection of this type of information was viewed as the responsibility of the intelligence community and, therefore, there was little to no involvement by most State and local law enforcement entities. The attacks of September 11, 2001, however, taught us that those wanting to commit acts of terrorism may live in our local communities and be engaged in

criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories. Important intelligence that may forewarn of a future attack may be derived from information collected by State, tribal, and local government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.

The President and the U.S. Congress have directed that an information sharing environment (ISE) be created in the next two years to facilitate information sharing and collaboration activities within the Federal Government (horizontally) and between Federal, State, tribal, local, and private-sector entities (vertically). The concept of intelligence/information fusion has emerged as the fundamental process (or processes) to facilitate the sharing of homeland security-related information and intelligence at a national level, and, therefore, has become a guiding principle in defining the ISE.

Homeland Security Intelligence/Information Fusion

Homeland security intelligence/information fusion is the overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private-sector authorities. It is more than the one-time collection of law enforcement and/or terrorism-related intelligence information and it goes beyond establishing an intelligence center or creating a computer network. Intelligence fusion is a clearly defined, ongoing process that involves the delineation of roles and responsibilities; the creation of requirements; and the collection, blending, analysis, timely dissemination, and reevaluation of critical data, information, and intelligence derived from the following:

- Autonomous intelligence and information management systems (technical and operational) established to support the core missions of individual Federal, State, local, tribal, and government entities;
- General public; and
- Private-sector entities.

The fusion process is a key part of our nation's homeland security efforts. This process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. Simultaneously, it supports efforts to address immediate and/or emerging, threat-related circumstances and events. Although the collection, analysis, and dissemination of terrorism-related intelligence is not the sole goal of the fusion process, one of the principal outcomes should be the identification of terrorism-related leads—that is, any nexus between crime-related and other information collected by State, local, tribal, and private entities and a terrorist organization and/or attack. The fusion process does not replace or replicate mission-specific intelligence and information management processes and systems. It does, however, leverage information and intelligence developed through these processes and systems to support the rapid identification of patterns

and trends that may be indicative of an emerging threat condition. 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 nonterrorism 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.
- Effective intelligence/information fusion requires the following:
- The use of common terminology, definitions, and lexicon by all stakeholders;
- Up-to-date awareness and understanding of the global and domestic threat environment;
- A clear understanding of the links between terrorism-related intelligence and nonterrorism-related information (e.g., flight school training, drug trafficking) so as to identify those activities that are precursors or indicators of an emerging threat;
- Clearly defined intelligence and information requirements with the Federal intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts;
- Identifying critical information repositories[62] and establishing the processes, protocols, procedures, and technical capabilities to extract information and/or intelligence from those repositories;
- Reliance on existing information pathways and analytic processes as ssible;

---

62 These repositories are not limited to those maintained by law enforcement entities. For example, critical information may be contained in systems supporting medical examiners (unattended death), public health entities, emergency rooms (information similar to the Drug Abuse Warning Network program), environmental regulatory inspectors, transportation entities, housing inspectors, health inspectors, building code inspectors, etc.

- All-hazards and all-crimes approach to defining information collection, analysis, and dissemination;
- Clear delineation of roles, responsibilities, and requirements of each level and sector of government involved in the fusion process;
- Understanding and elimination of impediments to information collection and sharing (i.e., it should be a priority for the Federal Government to provide State, local, and tribal entities unclassified terrorism-related information/intelligence so that it can be integrated into statewide and/or local fusion efforts);
- Capacity to convert information into operational intelligence;
- Extensive and continuous interaction with the private sector and with the public at large;
- Connectivity (technical and/or procedural) with critical intelligence streams, analysis centers, communication centers, and information repositories at all levels of classification as necessary;
- Extensive participation of subject-matter experts (SMEs) in the analytical process; and
- Capacity and commitment to ensure aggressive oversight and accountability so as to protect against the infringement of constitutional protections and civil liberties.

Participants in the Fusion Process

To some degree, the fusion process involves every level and sector (discipline) of government, the private-sector, and the public. The level of involvement from these participants will vary based on specific circumstances. Some disciplines, such as law enforcement, represent a core component of the fusion process because of the relationship between crime and because, in many cases, law enforcement authorities are best-suited to coordinate statewide and local fusion efforts. Minimally, the fusion process should be organized and coordinated on a statewide level and each State should establish and maintain an analytic center to facilitate the fusion process. Each major urban area (as defined by the Urban Area Security Initiative [UASI] program) may want to establish a similar capacity ensuring it is interlinked with the

fusion process established by the State. Other localities, tribal governments, and even private-sector entities should develop a process to interlink and participate in these statewide (or UASI) fusion efforts. The public should be engaged through public education programs that describe what they should look for and what to do if they observe suspicious activities or circumstances.

Efforts should be organized and managed on a geographic basis and scalable so adjustments can be made based on changes in the operating and/or threat environment. While national standards and guidelines should guide the institutionalization of the process, the actual technological infrastructure and operational protocols used by individual jurisdictions should be based on the management structure, specific needs, and capabilities of each individual jurisdiction.

Stages of the Fusion Process

Fusion is cyclical process that includes the following stages and activities:

- **Management/Governance**
  - ✓ Define a management structure (e.g., who is in charge, what entity will manage and coordinate daily activities).
  - ✓ Identify core (permanent) and ad hoc stakeholders.
  - ✓ Design a governance structure advisory committee (multidisciplinary and multilevel of government).
  - ✓ Define goals and objectives.
  - ✓ Develop a process to define information and intelligence collection requirements.
  - ✓ Develop the process and necessary memorandums of understanding to communicate requirements.

- **Planning and Requirements Development**
  - ✓ Conduct (and update frequently) a comprehensive and compatible risk assessment (threat, vulnerability, and consequence).
  - ✓ Identify patterns and trends reflective of emerging threats.

- ✓ Define collection requirements based on results of risk assessments.
- ✓ Identify the circumstances or events (e.g., crime, public health) that represent indicators and/or precursors of threats.
- ✓ Identify the sources and/or repositories of data and information regarding indicators and precursors.
- ✓ Identify the existing capacity to collect key information from existing sources.
- ✓ Identify collection gaps and mitigate.
- ✓ Define public education, and other activities necessary to enhance situational awareness by the public.
- ✓ Develop training for front line law enforcement and other personnel so that they can better identify suspicious activities that may represent planning and/or operational activity by terrorist group.
- ✓ Ensure a mechanism exists to support reporting of collected information (e.g., 9-1-1, tipline, Internet, connectivity to key information systems).
- ✓ Identify regulatory, statutory, privacy, and/or other issues that impede collection and sharing of information.
- ✓ Develop (in partnership with private-sector officials) detailed knowledge of vulnerabilities and consequence in the private sector to possible terrorist attacks to assess the likelihood of attack, the likely methods of attack, the likely equipment and substances used to carry out such an attack, and identify planning activities.

- **Collection**
  - ✓ Communicate collection requirements to relevant State, tribal, local, and private-sector entities.
  - ✓ Implement situational awareness activities (e.g., training, public education).
  - ✓ Mitigate impediments to collection.
  - ✓ Compile classified and unclassified data, information and

intelligence generated by people and organizations.

- ✓ Serve as the 24/7/365 initial point of contact for information provided by the U.S. Department of Homeland Security, Department of Defense, Department of Justice, Federal Bureau of Investigation, and other Federal entities (via telephone calls, Homeland Security Information Network/Joint Regional Information Exchange System, LEO, e-mail bulletins, VTC, fax) for the receipt of the following:

- **Immediate threat-specific information (classified and unclassified)**
- **Long-term threat information (classified and unclassified)**
- **Tactics and methods used by terrorists (classified and unclassified)**

  - ✓ Integrate with other reporting systems (e.g., 9-1-1, 3-1-1), and establish and maintain further, easy-to-use capability for the public reporting of suspicious activity in conjunction with the Joint Terrorism Task Force (e.g., internet, toll-free tipline).
  - ✓ Establish a process to identify and track reports of suspicious circumstances (e.g., pre-operational surveillance, acquisition of items used in an attack).

- **Analysis**
  - ✓ Blend data, information, and intelligence received from multiple sources.
  - ✓ Reconcile, deconflict data, and validate as to credibility of data, information and intelligence received from collection sources.
  - ✓ Evaluate and analyze data and information using SMEs.
  - ✓ Identify and prioritize the risks faced by the jurisdiction (e.g., State, local).
  - ✓ Produce value-added intelligence products that can support the development of performance-driven, risk-based prevention, response, and consequence management programs.
  - ✓ Identify specific protective measures to identify and disrupt

potential terrorist attacks during the planning and early operational stages.

- **Dissemination, Tasking, and Archiving**
  - ✓ Identify those entities and people (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management (public and private) efforts.
  - ✓ Provide relevant and actionable intelligence in a timely manner to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sector).
  - ✓ Archive all data, information, and intelligence to support future efforts.
  - ✓ Support the development of performance-based prevention, response, and consequence management measures.
  - ✓ Establish the capacity to track performance metrics associated with prevention, response, and consequence management efforts.
  - ✓ Provide feedback to information collectors.

- **Reevaluation**
  - ✓ Track the achievement of prevention, response, and consequence management program performance metrics so as to evaluate impact on the risk environment.
  - ✓ Update threat, vulnerability, and consequence assessments so as to update the risk environment.

- ✓ Assess effectiveness of national (i.e., Federal, State, tribal, and local) intelligence and information collection requirements process.

- **Modification of Requirements**
  - ✓ Modify collection requirements as necessary.
  - ✓ Communicate modifications in a timely manner.

Intelligence and Information Sharing Working Group Members

Chair, Governor Mitt Romney (Homeland Security Advisory Council [HSAC])
Chuck Canterbury (HSAC)
Frank Cilluffo (HSAC)
Major General Bruce Lawlor (Retired) (HSAC)
Mayor Patrick McCrory (HSAC)
Lydia Thomas (HSAC)
Mayor Karen Anderson (State and Local Senior Advisory Committee [SLSAC])
James Dunlap (SLSAC)
Don Knabe (SLSAC)
Peggy Merriss (SLSAC)
Karen Miller (SLSAC)
Mayor Donald Plusquellic (SLSAC)
Michael Carona (Emergency Response Senior Advisory Committee [ERSAC])
Frank Cruthers (ERSAC)
Ellen Gordon (ERSAC)
Phillip Keith (ERSAC)
Paul Maniscalco (ERSAC)
Dr. Allan Zenowitz (Academe, Policy and Research Senior Advisory Committee)
George Vradenburg (Private Sector Senior Advisory Committee)
John Cohen (Office of the Governor, Massachusetts)
Cindy Gillespie (Office of the Governor, Massachusetts)

Fusion Group Subject-Matter Experts

Kenneth Bouche, Colonel, State Police, Illinois
Dan Cooney, Captain, State Police, New York
George Foresman, Homeland Security Advisor, Virginia
Bart Johnson, Lieutenant Colonel, State Police, New York
Fred LaMontagne, Fire Chief, Maine
Pete Modafferi, Chief of Detectives, Rockland County, New York
Steve McGraw, Homeland Security Advisor, Texas
Jim McMahon, Homeland Security Advisor, New York
Tom O'Reilly, Office of the Attorney General, New Jersey
Russ Porter, Assistant Director, Department of Public Safety, Iowa
Mark Zadra, Chief of Investigations, Office of Statewide Intelligence, Florida Department of Law Enforcement

Homeland Security Advisory Council Staff

Dan Ostergaard, Executive Director, Homeland Security Advisory Council
Rich Davis, Director, Academe and Policy Research Senior Advisory Committee
Jeff Gaynor, Director, Emergency Response Senior Advisory Committee
Katie Knapp, Special Assistant to the Homeland Security Advisory Council
Mike Miron, Director, State and Local Officials Senior Advisory Committee
Candace Stoltz, Director, Private Sector Senior Advisory Committee

Appendix E
Information Exchange Analysis and Design Report

Information Exchange Analysis and Design

Analyze information exchange among law enforcement and homeland security partners and build models for successful information sharing.

Justification

Law enforcement and homeland security partners operate myriad systems for collecting, maintaining, analyzing, and sharing data and information critical to carrying out their respective missions. Creating the capacity to share information among and between agencies, levels of government, and a variety of disciplines—indeed, creating an enterprise approach—means overcoming established barriers to data exchange. It involves understanding cross-jurisdictional information needs and the data exchanges that cross sometimes radically different lines of business.

Information exchange in any environment is triggered by internal or external events. In the justice system and homeland security environments, these triggering events are the key decision points in our routine business processes, such as an arrest, a traffic accident involving hazardous materials, a release from prison, or a terrorist incident. In order to share intelligence electronically, it is essential to understand the nature of these business processes, decision points, and triggering events.

Most organizations do an adequate job of applying technology in their internal environments. On the other hand,

most information exchange between organizations is not developed with similar rigor, following the "anarchy model." In the anarchy model, each interface is a custom interface, and decisions about information sharing are made without regard for other data that may pass between the same two organizations and without regard for other agencies that may need the same information.

As interfaces are constructed with this anarchy model, architectural decisions are made that may constrain future efforts to share data by organizations that may have no interest in these original exchanges. For example, a decision by courts and prosecutors to establish a data warehouse as a central location for sharing documents electronically will make it more difficult and expensive for law enforcement agencies to develop a middleware approach for sharing traffic accident information. In a second example, law enforcement agencies and the courts may decide on an approach for sharing citation information electronically, without consulting the prosecutor, the state motor vehicle division, or the state criminal history repository, which also have an interest in electronic citation data.

There are two problems that result from application of the anarchy model: 1) the architecture that evolves is seldom optimal and often is inadequate for most other information exchange, and 2) efforts to expand information exchange generally end up collapsing beneath their own weight as the number of data trading partners increases. What is needed is an enterprise model for designing

information exchange for fusion centers. An enterprise approach considers all of the information exchange needs of all stakeholders when developing the integration architecture.

Whether interfaces between systems for sharing intelligence consist of simple queries and responses, or are more sophisticated transactional processes that build central index entries or populate data warehouses, it is important to document and analyze this information exchange at the planning stage of a project and to create a blueprint at the enterprise level for sharing data electronically that capitalizes on efficiency, accuracy, and timeliness. This design should be created by business experts from the participating organizations, under the direction of policy leaders and with the assistance of technologists. It should be based on a disciplined examination of current business practices, existing technology, and paper and electronic exchange of intelligence that already is occurring.

The Justice Information Exchange Model (JIEM)

The Justice Information Exchange Model (JIEM) is a tool that can assist fusion centers in performing these important tasks. JIEM documents the processes, triggering events, and conditions that govern information exchange at the enterprise level. It models the data that flows or should flow between organizations. It is a planning tool, a business modeling tool, an information exchange modeling tool, and a data modeling tool. It is linked

with the Global Justice XML Data Model (GJXDM), allowing easy importing of model components to design electronic documents. Soon it will be linked with the ability to import and export XML schema and other Information Exchange Package Documentation (IEPD) artifacts that are essential to implementing the GJXDM. This will eventually enable justice agencies to seamlessly generate (and, if need be, re-generate) GJXDM compliant information exchanges from the business rules encapsulated in JIEM, ensuring that they can be rapidly adapted to the needs of an increasingly dynamic environment. JIEM is also being enhanced to support the exchange of information not only within domains (as in the justice domain today) but between different domains, such as justice, emergency management, transportation, and intelligence, in support of emerging organizations such as Fusion Centers.

JIEM was developed to collect requirements from practitioners for justice information sharing initiatives; specifically to assist justice system leaders in analyzing and documenting existing information exchange at the enterprise level, in designing new electronic exchange processes as a part of an integrated justice initiative, and in adopting and implementing national business, data, and technology models to save time, effort, and money. It helps justice and public safety practitioners to articulate requirements that can be communicated to technologists who develop systems and interfaces. It is being expanded to support the needs of developers who will build the systems and interfaces needed to share intelligence in the law enforcement and homeland security community.

JIEM was created by SEARCH, the National Consortium for Justice Information and Statistics, with funding from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. It has been used in dozens of integrated justice initiatives in the United States and has been adopted by the Canadian government.

Creating a Blueprint for Information Sharing

Once practitioners understand the enterprise and how it conducts business, they can begin to build a blueprint for a more effective enterprise. Information sharing analysis will expose inefficiencies, redundancies, gaps, and opportunities in the current system. Once the system's current operations are obvious to decision makers, they can decide how they want to work together in the future and construct a blueprint or "to-be" plan. This will be a critical activity for the development of a nationwide system of intelligence fusion centers.

Common Exchanges Create a Reference Model for Others to Use

JIEM users have each created databases of their detailed justice information exchanges. JIEM was designed to allow administrators to review, analyze, compare, and contrast exchanges entered by all jurisdictions. That research has led to the development of the JIEM Reference Model, a set of common exchanges found in most locations. A similar process could be used to create a universal set of exchanges for intelligence sharing.

With a reference model, fusion centers that are just beginning their information sharing efforts could incorporate those common exchanges, rather than starting with nothing. They could import those exchanges into a new database that can then be tailored to the unique needs of their region or jurisdiction. The reference model enables centers to build exchanges that reflect their individual business practices but in a manner that is consistent with national activities and initiatives. This essential product of JIEM was developed by and for the practitioners who use the tool to model actual, operational exchanges in their jurisdictions.

The JIEM methodology and modeling tool can be used by any enterprise seeking to analyze its business processes, understand its information exchange, and reengineer its business processes by quickly leveraging best practices and capitalizing on the experience of other jurisdictions.

What Is Included in JIEM?

JIEM has five components:

- A **conceptual framework** for understanding justice information exchanges (today), as well as information exchanges in and between additional domains (such as emergency management, transportation, immigration, and intelligence) in the future.

- A **methodology** for analyzing current information exchange and for reengineering information exchange in an information sharing environment.

- The **JIEM Modeling Tool**©, a Web-based software package to assist justice system practitioners in applying JIEM.

- The **JIEM Reference Model**, a set of information exchange descriptions that are common to most jurisdictions.

- An interface with the **Global Justice XML Data Model** that allows users to import types and properties directly into their JIEM documents.

Who Uses JIEM?

JIEM is used by practitioners during the strategic planning phase of an information sharing initiative or later by developers during the design of specific interfaces between applications. Using JIEM, a site can accomplish the following:

- Document existing business processes and information flow between justice and justice-related organizations with text and graphical outputs.

- Analyze the effectiveness and economy of existing practices.

- Gather requirements for improved information exchange, creating a blueprint for the integration initiative.

- Analyze existing data transfers to determine which provide the most favorable cost/benefit ratios for automation.

- Use JIEM outputs as inputs to other developer tools to enhance justice applications and to develop interfaces between systems.

- Access, import, and extend national models, such as the JIEM Reference Model, the Global Justice XML Data Model, and Information Exchange Package Documentation (IEPD).
- Register locally developed IEPD artifacts in a national repository for use by others.
- Provide data to support national efforts to develop and improve models, methodologies, and tools to support integrated justice.

JIEM Benefits

The JIEM analysis requires the active input of stakeholders from all participating organizations. It delivers a number of benefits to local, state, and regional integrated justice efforts that go beyond the specific products provided by the system, including:

- An opportunity to bring staff from diverse but interdependent justice disciplines together with a common language and methodology to focus on business practices of mutual concern at the enterprise level.
- Access to best practices from around the nation to avoid reinventing the wheel.
- Free software and support to preserve scarce resources; a personal computer and Internet access are the only requirements to access JIEM.
- Participation in national efforts to improve the integration of justice information resources.

Issues for Consideration

When analyzing and designing methods for obtaining and disseminating intelligence electronically, consider:

- Identifying organizations that will contribute and consume information from the fusion center.
- Recognizing the political independence of these organizations that are operationally interdependent.
- Understanding the diversity in format and structure of information in all of these agencies.
- Analyzing the diversity of technology applications, communications protocols, and development environments that exist in justice-related organizations.
- Acknowledging the issues that relate to business processes that overlap organizational boundaries and the need to coordinate these practices between entities.
- Maintaining relationships with leaders of these organizations to ensure that internal changes in business processes do not disrupt information exchange.
- Recognizing the organizational, political, legal, and budgetary constraints that operate on justice organizations and drive efforts to improve operations while conserving resources.

Appendix F
Fusion Center Report Glossary

28 CFR Part 23—A guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems (Criminal Intelligence Glossary, November 2004).

Administrative Analysis—The provision of economic, geographic, or social information to administrators (Gottlieb, Singh, and Arenberg, 1995, p. 13). 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 (Criminal Intelligence Glossary, November 2004).

Advanced Authentication—Definitively identifying users before they access an organization's network is a key component in protecting information resources. Start by choosing an authentication system with encrypted password protocols. Before choosing an advanced authentication system, it is imperative that data owners evaluate user access, hardware, and other requirements (Criminal Intelligence Glossary, November 2004).

Analysis—The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. (Peterson, 1994, p. 269) 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 (Criminal Intelligence Glossary, November 2004).

Association/Link/Network Analysis—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 (*Law Enforcement Analytic Standards*, November 2004). 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 (Criminal Intelligence Glossary, November 2004).

Audit Trails—The use of audit procedures (e.g., tracking who is accessing the data or what data was accessed) combined with analysis of audit logs and follow-up for unauthorized or anomalous activity is essential for long-term system security and privacy (Criminal Intelligence Glossary, November 2004).99

Authentication—The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be but says nothing about the access rights of the individual (www.webopedia.com).

Authorization—The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures

that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity (www.webopedia.com).

Classified Information/Intelligence—A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure certain information be maintained in confidence in order to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities (Criminal Intelligence Glossary, November 2004).

> **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 (Executive Order 12958, March 25, 2003).

> **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 (Executive Order 12958, March 25, 2003).

> **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 (Executive Order 12958, March 25, 2003).

Collation (of Information)—The process whereby information is assembled together and compared critically (*Law Enforcement Analytic Standards*, November 2004). 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 (Criminal Intelligence Glossary, November 2004).

Collection (of Information)—The directed, focused gathering of information from all available sources (INTERPOL, 1996, p. 9). 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 (Criminal Intelligence Glossary, November 2004).

Commodity Flow Analysis—Graphic depictions and descriptions of transactions, shipments, 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 (Criminal Intelligence Glossary, November 2004).

Concept of Operations (CONOPS)—A statement outlining how an operation or organization will achieve its mission and goals. The concept is designed to give an overall picture of the operation.

Continuity of Operations Plan (COOP)—A plan that specifies the activities of individual departments and agencies and their subcompartments to ensure that their essential functions are performed in the event of an emergency or disaster.

Coordination—The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment (Criminal Intelligence Glossary, November 2004).

Crime-Pattern Analysis—A process that looks for links between crimes and other incidents to reveal similarities and differences that can be used to help predict and prevent future criminal activity (*Law Enforcement Analytic Standards*, November 2004). 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 Intelligence Glossary, November 2004).

Criminal Investigative Analysis—The use of components of a crime and/or the physical and psychological attributes of a criminal to ascertain the identity of the criminal (Peterson, 1994, p. 42). An analytic process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s) (Criminal Intelligence Glossary, November 2004).

Critical Infrastructure Resiliency (CIR)—The ability of critical infrastructure systems to maintain or rapidly recover essential functions and structure in the face of internal and external change and to degrade gracefully if they must. (*Science Magazine* and the Report of the Critical Infrastructure Task Force, January 2006, by the U.S. Department of Homeland Security's Homeland Security Advisory Council.)

Database Integrity—It may be advisable, depending on the sensitivity of the data, to utilize multilevel, secure database products to ensure the safety of data. In addition, limiting data access via database engine passwords or digital certificates separate from the operating system password adds another layer of security (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

Dissemination (of Intelligence)—The release of information, usually under certain protocols (Peterson, 1994, p. 271). 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 (Criminal Intelligence Glossary, November 2004).

Encryption—The process of encoding information so that unauthorized individuals will be unable to read, understand, or use the information. A password or key is required to decode (decrypt) the information back into its original, useable form.

Evaluation (of Information)—An assessment of the reliability of the source and accuracy of the raw data (Morris and Frost, 1983, p. 4). All information collected for the intelligence cycle is reviewed for its quality, with an assessment of the validity and reliability of the information (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004). The compilation and analysis of data relating to events as they have occurred over time allow the analyst to draw conclusions and recommendations based on the analysis (Peterson, 1994).

Financial Analysis—A review and analyses 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 (*Law Enforcement Analytic Standards*, November 2004).

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; it may show missing actions or events that need

further investigation (*Law Enforcement Analytic Standards*, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

Fusion Center—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 terrorism activity (Recommended Fusion Center Law Enforcement Intelligence Standards, March 2005).

Inference Development—Drawing conclusions based on facts (Peterson, 1994, p. 48). 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 (Criminal Intelligence Glossary, November 2004).

Intelligence (Criminal)—The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature. Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity (NCISP, October 2003). The product of the analysis of raw information related to crimes or crime patterns with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible criminal activity (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

Intelligence Bulletins—A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically sensitive but unclassified and available for distribution to local, state, tribal, and federal law enforcement.

Intelligence Information Reports (IIR)—Raw, unevaluated intelligence concerning "perishable" or time-limited information concerning criminal or national security issues. While the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to sensitive but unclassified information in the report under the tear line (Criminal Intelligence Glossary, November 2004).

Intelligence-Led Policing—The collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels (NCISP, October 2003). 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 (Criminal Intelligence Glossary, November 2004).

Intelligence Process (Cycle)—Planning and direction, collection, processing and collating, analysis and productions, and dissemination (Morehouse, 2001, p. 8). An organized process by which information is gathered, assessed, and distributed in order to fulfill the goals of the intelligence function—it is a method of performing analytic activities and placing the analysis in a useable form (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

***National Criminal Intelligence Sharing Plan* (NCISP)**—A formal intelligence sharing initiative, supported by the U.S. Department of Justice that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence. 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 (Criminal Intelligence Glossary, November 2004).

Need to Know—As a result of jurisdictional, organizational, or operational necessities, intelligence or information is disseminated to further an investigation (Criminal Intelligence Glossary, November 2004).

Operational Analysis—Identifying the salient features, such as groups of or individual criminals' relevant premises, contact points, and methods of communication (Europol, 200, Insert 3). 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 (Criminal Intelligence Glossary, November 2004).

Perimeter Security—Routers, firewalls, and intrusion detection systems should be implemented to tightly control access to networks from outside sources. Routers and firewalls filter and restrict traffic based upon very specific access control decisions made by the network operators, thereby limiting the types of unauthorized activities on a network (Criminal Intelligence Glossary, November 2004).

Physical Security—System and network administrators should tightly control physical access to computer and network hardware. Only authorized members of the technical staff should be allowed access to systems (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

Privacy (of 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 where legal process permits use of the personally identifiable information (Criminal Intelligence Glossary, November 2004).

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 where legal process authorizes surveillance and investigation (Criminal Intelligence Glossary, November 2004).

Profile/Criminal Profile—An investigative technique by which to identify and define the major personality and behavioral characteristics of the criminal offender based upon an analysis of the crime(s) he or she has committed (Criminal Intelligence Glossary, November 2004).

Reliability—Asks the question, "Is the source of the information consistent and dependable?" (Criminal Intelligence Glossary, November 2004)

Requirement—A validated intelligence information need (IIN) submitted to address an intelligence gap. Requirements can be "standing" (normally valid for months or years) or "ad hoc" (processed as they are identified, normally outside of planned, periodic requirements development and prioritization cycles) (FBI Intelligence Requirements and Collection Management Process, August 2003, p. 9).

Right to Know—Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports (Criminal Intelligence Glossary, November 2004).

Risk Assessment—An analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

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 to only those persons necessary to further the investigation or to prevent a crime or terrorist act (Criminal Intelligence Glossary, November 2004).

Sensitive Compartmented Information (SCI)—Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the director of the Central Intelligence Agency (Criminal Intelligence Glossary, November 2004).

Sensitive Compartmented Information Facility (SCIF)—An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed (Criminal Intelligence Glossary, November 2004).

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 (Criminal Intelligence Glossary, November 2004).

Strategic Intelligence—Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, criminal trend projections, or projective planning (*Law Enforcement Analytic Standards*, November 2004). 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 (Criminal Intelligence Glossary, November 2004).

Tactical Intelligence—Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety (*Law Enforcement Analytic Standards*, November 2004). Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case (Criminal Intelligence Glossary, November 2004).

Terrorism—Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational

groups or clandestine agents, usually intended to influence an audience (Title 22 of the United States Code, Section 2656f[d]).

Terrorism Information—All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other United States government activities, relating to 1) the existence, organization, capabilities, plans, intentions, vulnerability, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; 2) threats posed by such groups or individuals to the United States, U.S. citizens, or U.S. interests or to those of other nations; 3) communications of or by such groups or individuals; or 4) information relating to groups or individuals reasonably believed to be assisting or associated with such groups or individuals (Executive Order 13356).

Threat Assessment—A strategic document which looks at a group's propensity for violence or criminality or the possible occurrence of a criminal activity in a certain time or place (Peterson, 1994, pp. 56-57). 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 (Criminal Intelligence Glossary, November 2004).

Validity—Asks the question, "Does the information actually represent what we believe it represents?" (Criminal Intelligence Glossary, November 2004).

Vulnerability Assessment—A strategic document which views the weaknesses in a system that might be exploited by a criminal endeavor (NCISP, October 2003). 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 (Criminal Intelligence Glossary, November 2004).

Appendix G
Acronyms

ACTIC	Arizona Counter Terrorism Information Center		**GXSTF**	Global XML Structure Task Force
ATIX	Automated Trusted Information Exchange		**HIDTA**	High Intensity Drug Trafficking Areas
CAP	Common Alerting Protocol		**HIFCA**	High Intensity Financial Crime Areas
CDC	Centers for Disease Control and Prevention		**HSAC**	Homeland Security Advisory Council
CFR	Code of Federal Regulations		**HSIN**	Homeland Security Information Network
CICC	Criminal Intelligence Coordinating Council		**HSOC**	Homeland Security Operations Center
CII Act	Critical Infrastructure Information Act		**HSPD**	Homeland Security Presidential Directive
CITCS	Criminal Intelligence Training Coordination Strategy		**IACA**	International Association of Crime Analysts
			IACP	International Association of Chiefs of Police
CONOPS	Concept of Operations		**IADLEST**	International Association of Directors of Law Enforcement Standards and Training
COOP	Continuity of Operations Plan			
CTTWG	Counter-Terrorism Training Coordination Working Group		**IALEIA**	International Association of Law Enforcement Intelligence Analysts
DHS	U.S. Department of Homeland Security		**ICE**	U.S. Immigration and Customs Enforcement
DISA	Defense Information Systems Agency		**ICSIS**	Integrated Convergence Support Information System
DOJ	U.S. Department of Justice			
EPIC	El Paso Intelligence Center		**IJIS**	Integrated Justice Information System
FAQ	Frequently Asked Questions		**INTERPOL**	International Criminal Police Organization
FBI	Federal Bureau of Investigation		**JICC**	Justice Intelligence Coordinating Council
FEMA	Federal Emergency Management Agency		**LEIN**	Law Enforcement Intelligence Network
FinCEN	Financial Crimes Enforcement Network		**LEIU**	Law Enforcement Intelligence Unit
FOIA	Freedom of Information Act		**LEO**	Law Enforcement Online
FOUO	For Official Use Only		**LES**	Law Enforcement Sensitive
GISAC	Georgia Information Sharing and Analysis Center		**MOU**	Memorandum of Understanding
			NCISP	*National Criminal Intelligence Sharing Plan*
GISWG	Global Infrastructure/Standards Working Group		**NCJA**	National Criminal Justice Association
GIWG	Global Intelligence Working Group		**NCSD**	National Cyber Security Division
Global	Global Justice Information Sharing Initiative		**NDA**	Non-Disclosure Agreement
Global JXDM	Global Justice XML Data Model		**NDIC**	National Drug Information Center
GTRI	Georgia Tech Research Institute		**NIST**	National Institute of Standards and Technology

Nlets	The International Justice and Public Safety Information Sharing Network	**SME**	Subject-Matter Expert
NW3C	National White Collar Crime Center	**SOA**	Service-Oriented Architecture
OASIS	Organization for the Advancement of Structured Information Standards	**STTAC**	State Terrorism Threat Assessment Center (California)
OEP	Occupant Emergency Plan	**STIC**	Statewide Terrorism Intelligence Center (Illinois)
OJP	Office of Justice Programs	**TRS**	Terrorism Research Specialists
RCIC	Rockland County Intelligence Center	**UNYRIC**	Upstate New York Regional Intelligence Center
RISS	Regional Information Sharing Systems®	**US-CERT**	United States Computer Emergency Readiness Team
SARA	Superfund Amendments and Reauthorization Act	**USP3**	United States Public-Private Partnership (formerly DHS's HSIN-CI)
SBU	Sensitive But Unclassified	**VICAP**	Violent Criminal Apprehension Program
SCI	Sensitive Compartmented Information	**XML**	Extensible Markup Language
SCIF	Sensitive Compartmented Information Facility		