U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

NEW REALITIES
Law Enforcement in the Post-9/11 Era

Assessing and Managing the Terrorism Threat

BJA Bureau of Justice Assistance

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

Domingo S. Herraiz
Director, Bureau of Justice Assistance

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

Bureau of Justice Assistance
www.ojp.usdoj.gov/BJA

NCJ 210680

Written by Col. Joel Leson

This document was prepared by the International Association of Chiefs of Police, under cooperative agreement number 2003–DD–BX–K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Bureau of Justice Assistance Information

BJA's mission is to provide leadership and services in grant administration and criminal justice policy to support local, state, and tribal justice strategies to achieve safer communities. For more indepth information about BJA, its programs, and its funding opportunities, contact:

Bureau of Justice Assistance
810 Seventh Street NW.
Washington, DC 20531
202–616–6500
Fax: 202–305–1367
www.ojp.usdoj.gov/BJA
E-mail: AskBJA@usdoj.gov

The BJA Clearinghouse, a component of the National Criminal Justice Reference Service, shares BJA program information with federal, state, local, and tribal agencies and community groups across the country. Information specialists provide reference and referral services, publication distribution, participation and support for conferences, and other networking and outreach activities. The clearinghouse can be contacted at:

Bureau of Justice Assistance Clearinghouse
P.O. Box 6000
Rockville, MD 20849–6000
1–800–851–3420
Fax: 301–519–5212
www.ncjrs.org
E-mail: askncjrs@ncjrs.org

Clearinghouse staff are available Monday through Friday, 10 a.m. to 6 p.m. eastern time. Ask to be placed on the BJA mailing list.

To subscribe to the electronic newsletter *JUSTINFO* and become a registered NCJRS user, visit *http://puborder.ncjrs.org/register*.

BJA

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

Washington, DC 20531

Official Business
Penalty for Private Use $300

Assessing and Managing the Terrorism Threat

September 2005

NCJ 210680

BJA *Bureau of Justice Assistance*

Contents

Acknowledgements

Post 9-11 Policing Project Staff

The Post 9-11 Policing Project is the work of the International Association of Chiefs of Police (IACP), National Sheriffs' Association (NSA), National Organization of Black Law Enforcement Executives (NOBLE), Major Cities Chiefs Association (MCCA), and Police Foundation. Jerry Needle, Director of Programs and Research, IACP, provided overall project direction.

- **International Association of Chiefs of Police**

  Phil Lynn served as IACP's Project Director, managed development and publication of the four Promising Practices Briefs, and authored *Mutual Aid: Multijurisdictional Partnerships for Meeting Regional Threats.* Andrew Morabito co-authored *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships* and analyzed Post 9-11 survey data. Col. Joel Leson, Director, IACP Center for Police Leadership, authored this monograph—*Assessing and Managing the Terrorism Threat.* Walter Tangel served as initial Project Director.

  Dr. Ellen Scrivner, Deputy Superintendent, Bureau of Administrative Services, Chicago Police Department, contributed to all phases of project design and co-facilitated the 9-11 Roundtables with Jerry Needle. Marilyn Peterson, Management Specialist-Intelligence, New Jersey Division of Criminal Justice, authored *Intelligence Led Policing: The New Intelligence Architecture.*

- **National Sheriffs' Association**

  Fred Wilson, Director of Training, directed NSA project activities, organized and managed Post 9-11 Roundtables, and worked closely with IACP staff throughout the course of the project. NSA project consultants included Chris Tutko, Director of NSA's Neighborhood Watch Project; John Matthews; and Dr. Jeff Walker, University of Arkansas, Little Rock.

- **National Organization of Black Law Enforcement Executives**

  Jessie Lee, Executive Director, served as NOBLE's Project Director and conducted most staff work.

- **The Police Foundation**

  Edwin Hamilton directed Foundation project activities and managed Post 9-11 survey formatting and analysis, assisted by Rob Davis. Foundation consultants included Inspector Garth den Heyer of the New Zealand Police and Steve Johnson of the Washington State Patrol.

- **Major Cities Chiefs Association**

  Dr. Phyllis McDonald, Division of Public Safety Leadership, Johns Hopkins University, directed the work of the Major Cities Chiefs Association. The MCCA team included Denis O'Keefe, Consultant; Corinne Martin, Program Coordinator; and Shannon Feldpush.

  Dr. Sheldon Greenberg, Director of the Division of Public Safety Leadership, co-authored *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships.*

Promising Practices Reviews

Promising Practices drafts were critiqued and enriched by a series of practitioners/content experts including: Richard Cashdollar, Executive Director of Public Safety, City of Mobile, AL; George Franscell, Attorney-at-Law, Franscell, Strickland, Roberts and Lawrence, Los Angeles, CA; Mary Beth Michos, State Mutual Aid Coordinator, Prince William County, VA; David Bostrom, Manager, Community Policing Consortium, IACP; John P. Chase, Chief of Staff, IAIP, Department of Homeland Security; John M. Clark, Assistant Vice President/Chief of Police, Burlington Northern Santa Fe Railroad; John A. LeCours, Director/Intelligence, Transport Canada;

Ronald W. Olin, Chief of Police, Lawrence, KS; Ed Jopeck, Analyst, Veridian; Jerry Marynik, Administrator, State Terrorism Threat Assessment Center, California Department of Justice; and Bart Johnson, Office of Counter Terrorism, New York State Police.

The Bureau of Justice Assistance, IACP, and each of the partner organizations in the Post 9-11 Policing Project wish to acknowledge and thank Ms. Melissa Smislova, Chief, Homeland Infrastructure Threat and Risk Analysis Center at the U.S. Department of Homeland Security for her review and input into *Assessing and Managing the Terrorism Threat* on behalf of the Department.

Executive Oversight

The Post 9-11 Policing Project was initially conceptualized by the Office of Justice Programs, U.S. Department of Justice. Since inception, the project was guided throughout by the chief executive officers of the partner associations:

- Daniel N. Rosenblatt, Executive Director, International Association of Chiefs of Police
- Thomas N. Faust, Executive Director, National Sheriffs' Association
- Jessie Lee, Executive Director, National Organization of Black Law Enforcement Executives
- Hubert Williams, President, The Police Foundation
- Thomas C. Frazier, Executive Director, Major Cities Chiefs Association

Bureau of Justice Assistance Guidance

We gratefully acknowledge the technical guidance and patient cooperation of executives and program managers who helped fashion project work: James H. Burch II, Deputy Director; Michelle Shaw, Policy Advisor; and Steven Edwards Ph.D., Senior Policy Advisor for Law Enforcement.

Executive Summary

The continuous threat of terrorism has thrust domestic preparedness obligations to the very top of the law enforcement agenda. For today's law enforcement executive, the capacity to assess and manage risk is imperative. In the post-September 11 era, this capacity must be considered as much a staple of law enforcement operations as crime analysis, criminal intelligence, and crime prevention. The consequences of failing to assess and manage terrorist threats and risk could be incalculable.

This document outlines the essential components of risk assessment and management, which entail the following sequential tasks:

- Critical infrastructure and key asset inventory.
- Criticality assessment.
- Threat assessment.
- Vulnerability assessment.
- Risk calculation.
- Countermeasure identification.

Risk assessment and management concepts and methodologies are evolving rapidly. Although models differ in the definition, labeling, and sequencing of steps, there is solid consensus on the essential components. In this monograph, each component is defined and briefly examined. Protocols are supplied to quantify/calculate criticality, threat, vulnerability, and risk.

Experience and skill with risk assessment and management are limited in many law enforcement agencies. To assist in reversing this situation, this report supplies capacity-building information that includes promising programs, software, and training references. Capacity "acquisition" through shared/regional arrangements is not only economically practical for many agencies, it promises to leverage effectiveness for all agencies by pooling and coordinating information and planning joint countermeasures.

Introduction

Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility but responsibility so poorly defined or so ambiguously delegated that action gets lost. It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to those who need it . . . . It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion—which is usually too late . . . . Finally, as at Pearl Harbor, surprise may include some measure of genuine novelty introduced by the enemy, and possibly some sheer bad luck.

—Thomas C. Schelling, as quoted in Pearl Harbor: Warning and Decision by Roberta Wohlstetter (1962)

The price of living in a free and open American society grew exponentially after the tragic events of September 11, 2001. The scale and method of the terrorist attacks on that day have significantly affected the way law enforcement and security operations must be conducted to protect critical infrastructure. High-profile incidents such as the World Trade Center bombing in 1993 and the bombing of the Murrah Building in Oklahoma City in 1995 should have served as a permanent wake-up call to all Americans. However, the relative speed with which these crimes were solved, and the perceived isolation in which they were conceived and executed, caused many to carry on with business as usual.

Statement of the Problem

Foremost among the demands that confront police in the post-September 11 environment is the ability to effectively and efficiently collect, assess, disseminate, and act on intelligence information regarding threats posed by transnational and domestic terrorists. In a country with nearly 17,000 law enforcement agencies staffed by 700,000 sworn police officers, deputy sheriffs, and criminal investigators, meeting these demands is particularly challenging and complex. Classified security and jurisdictional issues tend to blur lines of communication. The need for technological interoperability, standardization, and operational networking within and among all agencies has been amplified. These demands, coupled with the requirement that local jurisdictions conduct threat, vulnerability, and needs assessments to qualify for federal homeland security funding through the State Homeland Security Assessment and Strategy Program, present clear challenges to law enforcement executives.

Progress to Date

Results of a recent survey conducted by the International Association of Chiefs of Police (IACP) documents that the frequency of information sharing among federal, state, and local law enforcement agencies has improved since the September 11 terrorist attacks (Needle, 2004). The U.S Departments of Justice (DOJ) and Homeland Security (DHS) are promoting developments that are improving both the dissemination of intelligence and threat-related information and the ability to assess risk and reduce the vulnerability of potential targets within the public and private infrastructure. Guiding these improvements is the *National Criminal Intelligence Sharing Plan (NCISP)*, which was endorsed by both departments and the Federal Bureau of Investigation (FBI) in October 2003. The issuance of the NCISP has been followed by the development of the *Fusion Center Guidelines*, which will be issued jointly by DOJ and DHS, in coordination with DOJ's Global Justice Information Sharing Initiative (Global), which represents more than 30 independent organizations spanning the spectrum of law enforcement and other justice entities.

For example, DHS has expanded its computer-based counter-terrorism system to all 50 states, 5 territories, the District of Columbia, and 50 major urban areas to improve the flow of threat information. This relatively new communications system, called the Homeland

Security Information Network (HSIN), offers states and major cities real-time, interactive connectivity with the DHS Homeland Security Operations Center.

Another system, the Regional Information Sharing Systems (RISS), was initiated in 1980, and is administered by the U.S. Department of Justice, Office of Justice Programs' Bureau of Justice Assistance. It consists of six regional centers that share intelligence and coordinate efforts against criminal networks that cross jurisdictional lines. RISS serves more than 7,500 law enforcement agencies and their branches in 50 states, the District of Columbia, Canada, Australia, the United Kingdom, Guam, the U.S. Virgin Islands, and Puerto Rico. The FBI has created the National Joint Terrorism Task Force (NJTTF), and it supports FBI field office-based JTTFs to expedite the exchange of threat information. In July 2003, the DHS Office of Domestic Preparedness (ODP) announced a major refinement of the State Homeland Security Assessment and Strategy (SHSAS) Process, which was established in fiscal year 1999 to assess threats, vulnerabilities, capabilities, and preparedness related to weapons of mass destruction and terrorism incidents at the state and local levels. ODP continues to support state and local jurisdictions by providing technical assistance to ensure that SHSAS is fully implemented throughout the United States.

These major efforts to improve the flow of terrorist and criminal intelligence, coupled with the operation of newly formed regional law enforcement intelligence fusion centers in strategic locations throughout the country, hold great promise for law enforcement's collective ability to effectively acquire and exchange real-time intelligence and threat information. While federal and state law enforcement agencies have been actively pursuing improvements in intelligence and information flow and risk assessment, many county and municipal law enforcement agencies have been doing the same. They have been improving their information technology capabilities, organizing or expanding their criminal intelligence and critical incident management capabilities, and participating in regional intelligence consortiums.

The attacks of September 11 have brought, and continue to bring, changes in the way law enforcement conducts its operations. However, the critical and basic task of conducting timely, ongoing, and viable threat assessments has not changed.

Objectives

This monograph explains risk assessment, how it is conducted, and how it fits into the risk management process—a process that all law enforcement executives should master in the post-September 11 era. The monograph defines terms used in risk management, including *threat, vulnerability,* and *criticality assessment,* and provides a utilitarian risk management methodology. Finally, it discusses how promising local practices are being adapted to implement the DHS State Homeland Security Assessment and Strategy Program.

State of Practice

Professionals in the private sector and at all levels of government are unanimous in their opinions that it is not a question of if another devastating terrorist event will occur, but when and where it will occur. In an ongoing study, the Rutgers Center for the Study of Public Security is conducting a survey to discover how law enforcement officials in the United States assess their local terrorist threat. Eighty percent of the almost 1,400 respondents who were surveyed expect a terrorist event to occur in their jurisdiction within the next 5 years—most likely a cyberterrorism or conventional attack. Almost all respondents reported that at least one terrorist group is present in their jurisdiction.

To confront, minimize, and prevent terrorist acts, the law enforcement arsenal must include a sophisticated risk-management capability. Risk assessment and management must become an essential capacity of law enforcement agencies. Capacity can reside in-house, at the government level (e.g., a city office of homeland security), or be acquired from county, regional, or state law enforcement and homeland security collaborative groups or agencies. The risk assessment and management capacity of state and local law enforcement agencies has not been documented, though it is believed that many agencies, if not most, do not possess the required skills. Risk assessment is a relatively new activity for law enforcement agencies, and the art and its vocabulary

are constantly changing. The requirement that applications for select homeland security grants be accompanied by evidence that an agency is working with threat assessment also is leading to further conceptual and methodological development.

Identifying Critical Infrastructure: What To Protect

It is important to consider what can be threatened and what must be protected by state and local law enforcement agencies and their counterparts that provide security in the private sector. The scope and magnitude of critical infrastructure and assets are defined in *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (The White House, 2003). In initiating this strategy, President George W. Bush stated:

> *To address the threat posed by those who wish to harm the United States, critical infrastructure owners and operators are assessing their vulnerabilities and increasing their investment in security. State and municipal governments across the country continue to take important steps to identify and assess the protection of key assets and services within their jurisdictions. Federal departments and agencies are working closely with industry to take stock of key assets and facilitate protective actions, while improving the timely exchange of important security related information.*

Since implementation of this national strategy, the critical infrastructure sectors—those infrastructures and assets deemed most critical to national public health and safety, governance, economic and national security, and retaining public confidence—have been refined and expanded.

Critical infrastructure now includes:

- Agriculture.
- Banking and finance.
- Chemical and hazardous waste.
- Defense industrial base.
- Energy.
- Emergency services.
- Food.
- Government.
- Information and telecommunications.
- Transportation.
- Postal and shipping services.
- Public health.
- Water.

Key assets now include:

- National monuments and icons.
- Nuclear power plants.
- Dams.
- Government facilities.
- Commercial assets.

State and local law enforcement executives must ensure that their community's vulnerability to attack is properly analyzed by identifying critical facilities and functions, and must work to improve their security. It is understood that complete protection of every reservoir, parking garage, mass transit terminal, large building, and other potential targets within a jurisdiction is not possible. It is also understood, however, that the more difficult it is for terrorists to introduce weapons into a given area or facility, the less likely terrorists are to initiate an attack.

Evaluation of critical infrastructure and key assets in the community should be ongoing. Law enforcement leaders should constantly maintain and update a database of a jurisdiction's critical assets and vulnerable infrastructure points. Appendixes II and III provide tools that law enforcement executives can use to train personnel and establish a comprehensive database. Specifically, appendix II provides information on the Homeland Security Comprehensive Assessment Model (HLS–CAM), a software program that the State of Florida used to develop and maintain its database of critical assets and vulnerable

infrastructure locations. This appendix identifies what such a comprehensive database contains and describes the HLS–CAM software available to law enforcement and emergency service agencies. Although the evaluation and assessment processes may seem overwhelming, law enforcement agencies must make the risk analysis process an inherent part of their law enforcement operations and present an objective case for improved public safety. Assessments should be made not only on the basis of routine operation and testing, but also on how effective the procedures will be in an actual attempted attack.

A Risk Assessment and Management Approach

Risk assessment and management entails the following sequential steps:

- Critical infrastructure and key asset inventory.
- Criticality assessment.
- Threat assessment.
- Vulnerability assessment.
- Risk calculation.
- Countermeasure identification.

Literature and agencies differ in how they define, label, and arrange these steps.

Risk Assessment

Criticality Assessment: Evaluating Assets

DHS defines criticality assessment as follows:

> A systematic effort to identify and evaluate important or critical assets within a jurisdiction. Criticality assessments help planners determine the relative importance of assets, helping to prioritize the allocation of resources to the most critical assets.

An essential part of the risk equation is considering the consequence of the loss of or serious damage to important infrastructure, systems, and other assets. The measure of criticality, or asset value, determines the ultimate importance of the asset. Loss of life and damage to essential assets are of paramount concern to law enforcement executives. Loss of symbolic targets, which can result in the press coverage terrorists seek, is also important; it can destroy people's faith in the ability of law enforcement and government to protect the public.

Assessing criticality can at times involve some degree of subjectivity. Assessments may rely on the intimate knowledge of law enforcement agency professionals and their colleagues in other government agencies to gauge the importance of each potential target. However, clear objective thought must prevail when loss of human life is possible. Certain facilities are inherently vulnerable and should be addressed as critical infrastructure or key assets by law enforcement:

- Transportation facilities, terminals, and other areas with concentrations of persons.
- Public utilities—electricity, water, natural gas, waste treatment.
- Public and government facilities; symbolic sites; town halls; county buildings; police, fire, and school buildings; stadiums; museums; and monuments.
- Financial and banking institutions.
- Defense and defense-related industry and research centers.
- Transportation support systems—radar, bridges, tunnels, piers, and aids to navigation.
- Health care facilities—public and private.
- Cyber/information technology service facilities and sites.

Calculating Criticality

A five-point scale can be used to estimate the impact of loss of life and property, interruption of facility or other asset use, or gain to be realized by an adversary:

- **Extreme (5):** Substantial loss of life or irreparable, permanent, or prohibitive costly repair to a facility. Lack of, or loss of, a system or capability would provide invaluable advantage to the adversary (press coverage, the political advantage or tactical advantage to carry out further plans).
- **High (4):** Serious and costly damage to a facility or a positive effect for the adversary. No loss of life.
- **Medium (3):** Disruptive to facility operations for a moderate period of time; repairs—although costly—would not result in significant loss of facility capability. No loss of life.
- **Low (2):** Some minor disruption to facility operations or lack of capability, does not materially advantage the enemy. No loss of life.
- **Negligible (1):** Insignificant loss or damage to operations or budget. No loss of life (Proteus Security Group, 1997).

Extreme and high criticality are of greatest concern. When coupled with high threat and high vulnerability, counteraction is required.

Threat Assessment

DHS defines threat assessment as follows:

> A systematic effort to identify and evaluate existing or potential terrorist threats to a jurisdiction and its target assets. Due to the difficulty in accurately assessing terrorist capabilities, intentions, and tactics, threat assessments may yield only general information about potential risks.

These assessments consider the full spectrum of threats, such as natural disasters, criminal activity, and major accidents, as well as terrorist activity.

Fused Intelligence

The intelligence process is the foundation of threat assessment. Systematic exploitation of crime-related information can lead to and support evaluation and analysis of terrorism and terrorist groups. The who, what, where, when, and how of terrorist groups are closely related. Intelligence efforts help produce reliable, informed responses to these questions. Without such a process, threat assessments can be unpredictable and unreliable.

Threat assessments must be compiled from comprehensive and rigorous research and analysis. Law enforcement cannot function unilaterally. Threat assessments that do not incorporate the knowledge, assessments, and understanding of state, local, and private organizations and agencies with the potential threats being assessed are inherently incomplete. For example, a threat assessment of water-district facilities should include the most comprehensive data available from local police, sheriff, and fire departments; health services; emergency management organizations; and other applicable local, state, and federal agencies that may be affected by an attack on the water district's infrastructure. The threat assessment should also assimilate germane, open-source, or nonproprietary threat assessments, as well as intelligence information. Lastly, the assessment must provide a high level of awareness and understanding regarding the changing threat and threat environment faced by a government entity.

Essential data to collect for analysis prior to conducting a threat assessment include:

- **Type of adversary:** Terrorist, activist, employee, other.
- **Category of adversary:** Foreign or domestic, terrorist or criminal, insider and/or outsider of the organization.
- **Objective of each type of adversary:** Theft, sabotage, mass destruction (maximum casualties), sociopolitical statement, other.
- **Number of adversaries expected for each category:** Individual suicide bomber, grouping or "cells" of operatives/terrorists, gangs, other.
- **Target selected by adversaries:** Critical infrastructure, governmental buildings, national monuments, other.
- **Type of planning activities required to accomplish the objective:** Long-term "casing," photography, monitoring police and security patrol patterns, other.
- **Most likely or "worst case" time an adversary could attack:** When facility/location is fully staffed, at rush hour, at night, other.
- **Range of adversary tactics:** Stealth, force, deceit, combination, other.
- **Capabilities of adversary:** Knowledge, motivation, skills, weapons and tools (National Emergency Response and Rescue Training Center, n.d.).

To accomplish the intelligence mission of processing a threat assessment, a law enforcement executive must ensure that an officer or unit is trained and assigned to identify potential targets and can recommend enhancements for security at those targets. Action must be taken by all departments, including those with limited resources. Ideally, the entire patrol force should be trained to conduct intelligence gathering and reporting.

Calculating Threat

Threat levels are based on the degree to which combinations of these factors are present:

- **Existence:** A terrorist group is present, or is able to gain access to a given locality.
- **Capability:** The capability of a terrorist group to carry out an attack has been assessed or demonstrated.
- **Intent:** Evidence of terrorist group activity, including stated or assessed intent to conduct terrorist activity.
- **History:** Demonstrated terrorist activity in the past.
- **Targeting:** Current credible information or activity exists that indicates preparations for specific terrorist operations—intelligence collection by a suspect group, preparation of destructive devices, other actions.
- **Security environment:** Indicates if and how the political and security posture of the threatened jurisdiction affects the capability of terrorist elements to carry out their intentions. Addresses whether the jurisdiction is concerned with terrorism and whether it has taken strong proactive countermeasures to deal with such a threat.

To gauge the seriousness of a terrorist threat, the criticality, threat, and vulnerability can be quantified in the following way:

- **Critical (5):** Existence, capability, and targeting are present. History and intentions may not be.
- **High (4):** Existence, capability, history, and intentions are present.
- **Medium (3):** Existence, capability, and history are present. Intention may not be.
- **Low (2):** Existence and capability are present. History may not be present.
- **Negligible (1):** Existence or capability may not be present (Proteus Security Group, 1997).

Identifying a threat is a complex process that is too often overlooked because the process of threat assessment is not well understood and is often seen as technically unreachable. Many resources are present within and outside of the law enforcement community to help law enforcement agencies complete this task, and it is important that they be used.

Vulnerability Assessment

DHS defines vulnerability assessment as follows:

> The identification of weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists. The vulnerability assessment also may suggest options to eliminate or mitigate those weaknesses.

Vulnerability is difficult to measure objectively. Progress is being made by agencies such as the National Institute of Justice in partnership with the U.S. Department of Energy's Sandia National Laboratories, as well as by studies conducted by the National Infrastructure Protection Center of DHS, to assist with these assessments. (See the list of Promising Practices/Resources in appendix I.)

Factors to consider when determining vulnerability include:

- **Location:** Geographic location of potential targets or facilities, and routes of ingress and egress; location of facility or target relative to public areas, transportation routes, or easily breached areas.
- **Accessibility:** How accessible a facility or other target is to the adversary (i.e., disruptive, terrorist, or subversive elements); how easy is it for someone to enter, operate, collect information, and evade response forces?
- **Adequacy:** Adequacy of storage facilities, protection, and denial of access to valuable or sensitive assets such as hazardous materials, weapons, vehicles or heavy equipment, and explosives or other materials that some person or organization could use deliberately or in an opportunistic manner to cause harm.
- **Availability:** Availability of equipment, adequacy of response forces and of general physical security measures.

Calculating Vulnerability

The vulnerability level is determined on a five-point scale using estimates of the sufficiency of protection or accessibility listed in the above factors.

- **Highly vulnerable (5):** A combination of two or more of the following with due consideration of the threat level:
  - Direct access to asset or facility is possible via one or more major highway systems. Waterside access is open or adjacent land areas are unoccupied, unguarded, or allow free access.
  - Asset or facility is open, uncontrolled or unlighted, or security is such that threat elements may have unimpeded access with which to collect intelligence, operate, and evade response forces. Patrols, electronic monitoring, or alarm systems are easily defeated or provide incomplete coverage.
  - Individual systems within the facility, such as hazardous materials, weapons, explosives, or vehicles, are accessible with minimum force or possibility of detection.
  - Response units provide minimum effective force to counter the experienced threat level. In-place physical security measures do not provide protection commensurate with the anticipated threat level.
- **Moderately vulnerable (3):** A combination of two of the following:
  - Direct access to asset or facility is possible via one or more major highway systems, but road system is restricted or patrolled. Waterside access may be open or adjacent land areas unoccupied, but mitigating geographic conditions may be present (e.g., lengthy channel access).
  - Asset or facility is open, uncontrolled or unlighted, or security is such that threat elements may meet some resistance, be detected, or activate a remotely monitored alarm. Access to collect intelligence, operate, and evade response forces is at least partially hampered. Patrols, electronic monitoring, or alarm systems may be easily defeated or provide incomplete coverage.
  - Individual items within the facility, such as hazardous materials, weapons, explosives, or vehicles, are accessible with moderate force, or tampering may result in detection.
  - Response units provide effective force to counter the experienced threat level. Physical security measures do not provide protection commensurate with the anticipated threat level.
- **Low vulnerability (1):** A combination of two or more of the following, provided continual awareness of the anticipated threat level is maintained:
  - Asset or facility is difficult to access from major highway or road network, or outside access is limited by geography.
  - Asset or facility has adequate, positive access control. Patrols, cameras, remote sensors, and other reporting systems are sufficient to preclude unauthorized entry, loitering, photography, or access to restricted areas.
  - Appropriate and reasonable safeguards are taken to prevent or hinder access to sensitive materials. Protection is commensurate with degree of material sensitivity and level of threat.
  - Response force is able to answer an infrastructure or facility breach with appropriate personnel, equipment, and timeliness (Proteus Security Group, 1997).

Risk Assessment Calculation

Risk assessment combines all earlier assessments—criticality, threat, and vulnerability—to complete the portrait of risk to an asset or group of assets. Numerous techniques are available for calculating risk, ranging from simple qualitative systems to those based on complex quantitative formulas. A common feature of most methodologies is the input on which they are based. Almost every technique addresses the following three questions to aggregate the information obtained in each of the assessment steps:

- **Criticality:** Asks what is the likely impact if an identified asset is lost or harmed by one of the identified unwanted events.

- **Threat:** Asks how likely is it that an adversary will attack those identified assets.

- **Vulnerability:** Asks what are the most likely vulnerabilities that the adversary or adversaries will use to target the identified assets.

The law enforcement executive or individual assigned to undertake these analyses can use the methods described above to determine the risk of unwanted attack on each asset.

Calculating Risk

The comprehensive results of each of the assessments can be summarized into a risk statement with an adjectival or numerical rating. The risk equation used in most systems is expressed in this basic formula:

Risk = Threat x Vulnerability x Criticality

In this equation, risk is defined as the extent to which an asset is exposed to a hazard or danger. Threat times vulnerability represents the probability of an unwanted event occurring, and criticality equals the consequence of loss or damage to the critical infrastructure or key asset.

Using this methodology in conjunction with a numerical scale or adjectival rating will produce an objective conclusion regarding the risk to an asset. Consistency in conducting the evaluations will result in a more accurate decisionmaking process.

Risk Management

Identifying Countermeasures: Where "The Risk" Competes with "The Budget"

Countermeasures are actions, devices, or systems employed to eliminate, reduce, or mitigate risk and vulnerability. To assist in making studied decisions that can be supported over time, multiple countermeasure packages that recommend appropriate actions should be provided. Options are often characterized as follows:

- **Risk averse package:** The preferred option, unconstrained by financial or political considerations. This package provides a point of reference for the expenditure necessary to minimize risk most effectively. This option is designed to reduce risk to the greatest degree possible.
- **Risk tolerant package:** The option that strikes a balance between the needs of security and protection and the financial and political constraints of a state or municipality.
- **Risk acceptance package:** The least desired option, which typically reflects the highest acceptable amount of risk, but represents the least possible cost. (Jopeck, n.d.)

Countermeasures, such as expansion of agency staffing, installation of equipment and new technology, or target hardening, must be evaluated or tested periodically to ensure that improvements are actually working as intended. These evaluations and tests should verify that policies and procedures are in place to guide how the countermeasures will be used. Countermeasures include physical security (fencing, camera surveillance, seismic monitoring devices, barricades), cyber security (firewalls, antivirus software, secure computer networks), personnel security, and other proactive methods that industry uses to secure critical infrastructure. The California State Agency Guidance is an outstanding example of specific proactive countermeasures that the state is taking as the Homeland Security Advisory System is implemented in California.

Building Capacity

As automation technology advances, the process of conducting risk assessment and management is becoming more sophisticated, as noted in appendixes II and III. Law enforcement executives should avail themselves of the progress being made to ensure they have the ability to conduct these critical analyses.

Case Study: A Tale of One City

Imagine that you are the chief of police of a community of 75,000, located not far from a large metropolitan area. Your mayor has recently returned from a conference for municipal executives where he received a briefing on risk management and how to apply it to assets and infrastructure in towns and cities. He asks you to explain the method you use to assess risk in your community. He tasks you with conducting a risk assessment and documenting the rationale for how it was done. He wants it completed within 2 weeks.

Fortunately, you previously assigned a team of your officers to attend risk management training. They are already working with the fire chief, director of public health, city engineer, and other key public and private owners and operators of city infrastructure to prioritize risk in your jurisdiction. As in most cities, a number of key public facilities are of concern. A large electric plant supplies power to half of your state as well as a large portion of three contiguous states. A chemical plant producing hazardous materials, some of which may cause illness or death, is the main employer in your city. It receives and ships materials by rail, and the railroad's right-of-way traverses through a major portion of your city. There is a reservoir, constructed from a dam on the river that runs through the city, and a pier that receives military ordnance from a naval weapons station in an adjoining county. A regional

high school and a number of middle and elementary schools are located throughout the city. A large hospital that supports the four surrounding counties is within the city limits. The city has the normal range of commercial and public facilities.

Your special team of trained police officers has been developing a threat assessment in coordination with the region's Joint Terrorism Task Force (JTTF) and Regional Intelligence Center. They have acquired the latest information regarding domestic criminal extremist groups that are active in the area, and have current intelligence on two international terrorist groups that leads them to determine that these groups are targeting sites within your region. Based on this intelligence, your region has been operating under an elevated threat level of condition "Yellow," as defined by the Homeland Security Advisory System. Using all intelligence data available, in conjunction with the risk assessment steps provided earlier in this monograph, you determine that your community and its surrounding areas are at a medium threat level.

Your assessment team has been working closely with the critical infrastructure owners and operators within your area. Since September 11, security has become of greater concern to private firms. Each has conducted a risk management assessment and has worked diligently to implement the neccessary countermeasures. Using the vulnerability assessment techniques delineated above and verified by your team, you conclude that the vulnerability level at the chemical plant is low, in part because the owners have applied a full array of the safeguards listed in your vulnerability assessment methodology. In an objective series of assessments, you find that the weapons and ammunition pier is moderately vulnerable. Compared to other assessed facilities, this poses a major concern.

A criticality assessment determines that ordnance is being transferred through the pier and stored aboard moored vessels. With a war underway, this creates a level of extreme criticality. You apply the data previously gathered and rate each of the assets and critical infrastructures in your community against the rating system provided above, and find that the ordnance pier is a major risk to your community.

You present your findings to the mayor, who raises questions regarding your risk assessment. Your risk analysis provides you with the appropriate data to make an objective case and to delineate requirements. You provide countermeasure proposals, including coordination with state and federal authorities, to ensure that security improvements are prioritized within the currently identified necessary countermeasures.

With few modifications, the above scenario is one that actually confronted a chief of police. Without conducting a risk analysis, it would have been easy but incorrect to conclude that the chemical plant, in this case, was most at risk. Objective assessment revealed that the exposed ammunition pier was the primary risk to the city and required attention. Actions were taken, accordingly, to improve the security of the pier.

Summary

On September 11, 2001, the country realized the magnitude of the terrorist threat to the homeland. It took this cataclysmic event for the country to direct resources to law enforcement agencies so they could begin to build the capacity they need to deal with terrorism. The emergency services community is positioned to become better prepared to deal with threat. Law enforcement executives must realize, however, that resources remain limited at all levels of government. They must also realize that to become proficient in the entire gamut of risk management, and to ensure that staff can accomplish these analyses or gain access to those who can, is an operational imperative.

Appendix I: Promising Practices/Resources

Numerous resources, some more detailed and involved than others, are available to help law enforcement executives and their agencies conduct and gain mastery of risk assessments. The *Vulnerability Assessment Methodologies Report*, a comprehensive study sponsored by DHS, Office for Domestic Preparedness, provides ". . . an analysis of various commercial and government vulnerability assessment methodologies which can be used by state and local governments to assess risk associated with their area of responsibility." The report lists the following government methodologies for consideration:

Draft National Infrastructure Protection Plan (NIPP): The draft NIPP will be published in final form in fall 2005 by DHS, and will serve as the foundation of risk assessments for the nation's critical infrastructure. It will provide specific guidance and direction to interested parties to produce comprehensive risk assessments for terrorist attacks in a consistent format and will provide the framework for integrating critical infrastructure protection initiatives into a single national effort.

DHS Assessment and Strategy Development Tool Kit: This is the program guideline used by DHS, Office for State and Local Government Coordination and Preparedness. It applies to all missions and sectors and helps identify potential targets. It is also helpful in conducting vulnerability assessments to use in applying for baseline grant funding for state domestic preparedness equipment and other federally funded requirements. The guideline is available at www.shsasresources.com/documents/state_handbook.pdf.

Business Continuity Management (BCM) Methodology: This methodology was created specifically for financial institutions. It addresses identifying and determining the value of an asset; identifying threats to disclosure; calculating the consequences of loss or disruption; assessing technical and nontechnical weaknesses or vulnerabilities; and calculating risk by integrating the threat and vulnerability assessments.

California Highway Patrol Crime Prevention Plan: This plan provides guidelines for awareness, risk assessment, and mitigation actions. It includes questions for self-assessment and is directed primarily toward the physical security of law enforcement facilities.

State of Colorado Critical Infrastructure and Key Asset (CIKA) Assessment Methodology: This software package is designed for critical infrastructure and key assets. It allows the user to self-assess with a numerical 0–5 rating scale based on the following CIKA factors: visibility, value, accessibility, hazard, population, mass casualties, criticality, service disruption, primary function, and geographic impact. The total score represents the criticality/vulnerability rating for the identified critical infrastructure and key asset.

Method to Assess the Vulnerability of U.S. Chemical Facilities: This is a prototype vulnerability assessment methodology (VAM) developed especially for chemical facilities by Sandia National Laboratories and the National Institute of Justice. It compares relative security risks and allows for development of recommended measures to reduce risks.

North Carolina Terrorism Vulnerability Self-Assessment: This general guidelines worksheet for state agencies can be used for all sectors, but is particularly appropriate for assessing the bioterrorism response capability of local health departments and hospitals. It enables users to rate vulnerability on a scale of 1–20 (low to high) in the following areas: potential terrorist intentions, specific targeting, visibility, onsite hazards, population, mass casualty potential, security environment, criticality, high-risk personnel (critical to continuity of business and government), communications, security, and emergency response preparedness. This worksheet is available at www.nccrimecontrol.org/forms/terrorismselfassessment.htm.

Sandia National Lab Community Vulnerability Assessment Methodology (VAM): This plan applies to all mission and sector categories, in addition to education; recreation venues such as parks, museums, and tourist attractions; emergency facilities; foreign-represented governments (such as embassies, residences, businesses); and special divisions such as abortion clinics and religious facilities. This methodology was developed as a prototype for the Chemical Facility Vulnerability Assessment Project and lays the foundation for a computer-based vulnerability assessment tool. Sandia National Laboratories uses Dams Security Assessment Methodology, Water Supply and Treatment VAM, Vulnerability Analyses and Security Design Reviews for Correctional Facilities, and VAM for Community Vulnerability (VAM–CF).

- ***Risk Management: An Essential Guide to Protecting Critical Assets:*** www.nipc.gov/publications/nipcpub/P-RiskManagement.pdf.

The California State Agency Guide: In this document, published in March 2003, the California Governor's Office of Emergency Services integrates the federal Homeland Security Advisory System (HSAS) into the California HSAS. The 95 protective measures described for implementing the five color-coded federal threat conditions are comprehensive and useful for all levels of governmental and law enforcement jurisdictions.

Orange County Sheriff's Office, Santa Ana, California: Sheriff Mike Corona has developed a formal Threat Assessment Team for Major Counties and is part of the Integrated Multi-Agency Intelligence Gathering Group. Together, these two groups coordinate all homeland security activities by gathering and sharing intelligence, assessing possible threats, and planning and conducting all homeland security operations.

"The Red, Gray, and Blue Model: A New Tool to Help Law Enforcement Executives Address the Transformed Security Environment": This article, published in the February 2002 issue of *Police Chief Magazine*, provides insights and practical recommendations for assessing the threat, the environment, and the ability of law enforcement executives to operate in the arena of weapons of mass effect.

Appendix II: Homeland Security Comprehensive Assessment Model (HLS–CAM): Up and Running

Even though methods for performing threat, risk, and vulnerability assessments; security analyses; and security surveys existed previously, few related to one another and the definitions they provided often overlapped or were unclear. HLS–CAM is the first model to integrate assessments and indicate the order of priority in which critical facilities and infrastructure are assessed.

The HLS–CAM methodology was created by the National Domestic Preparedness Coalition, Inc. (NDPCI), a nonprofit, public and private partnership led by the Orange County (Florida) Sheriff's Office, the West Virginia University School of Medicine, and the West Virginia National Guard. HLS–CAM is a grassroots effort developed by emergency responders for emergency responders.

NDPCI created HLS–CAM after recognizing the need for a uniform, comprehensive, and holistic method of performing assessments by federal, state, county, local, and private organizations charged with protecting citizens, facilities, and infrastructure from terrorism and other hostile criminal activity. HLS–CAM complies with all four objectives of Homeland Security Presidential Directive 7, the National Critical Infrastructure Protection Plan, and the National Incident Management System (NIMS).

The States of Florida and West Virginia have adopted the HLS–CAM methodology as their assessment models. Plans and accomplishments include the following:

- Florida Regional Domestic Security Task Force to assess all seven regions of the state. Individuals from all 67 counties have been trained, and the second round of training has been completed.
- I-Florida Grant Project to assess state-owned bridges.
- Florida Department of Transportation to assess all FDOT facilities and infrastructure.
- The State of Florida to assess all state-owned facilities and infrastructure as mandated by state statute.
- Florida Department of Emergency Management to assess all emergency operations centers. This department must use HLS–CAM methodology to receive grant money for improvements.
- Various local jurisdictions throughout Florida have been trained and are in the process of completing HLS–CAM for their areas of responsibility.
- Alltel Stadium in Jacksonville, Florida, to be assessed for Super Bowl XXXIX using the HLS–CAM methodology.
- The State of West Virginia to use HLS–CAM to assess critical facilities, infrastructure, and events throughout the state.
- The National Guard Bureau has adopted the HLS–CAM methodology as the baseline assessment for the Full Spectrum Vulnerability Assessment in all 50 states.
- The National Park Service to use HLS–CAM, in conjunction with the Pennsylvania State Police, to assess Independence National Historical Park, located in downtown Center City, Philadelphia.

Methodology

HLS–CAM is a 5-part continuous process consisting of the following:

- **Threat assessment:** Examines and defines a community; identifies critical facilities, infrastructures, and events; identifies threat groups; determines the likelihood that, given the current intelligence or designated federal, state, or local threat levels, a specific target will be subject to terrorist or hostile criminal attack.

- **Criticality assessment:** Determines the overall impact of a terrorist attack on a given target and the adverse effect it has within a community.

- **M/D–SHARPP Matrix:** Used to analyze criminal and/or terrorist targets that have been identified through the community threat assessment and criticality assessment. M/D–SHARPP further analyzes potential targets using information obtained in the threat assessment, and looks at the target through the threat group's perspective.

- **Community priority assessment plan:** Derived from the criticality assessment and the M/D–SHARPP Matrix, used to determine the order of priority for the vulnerability assessment of critical facilities, infrastructure, and events as identified by the community threat assessment.

- **Vulnerability assessment:** A critical onsite physical examination and thorough inspection of an asset's perimeter, property within its perimeter, and exterior and interior building spaces, to include all operational systems and procedures along with the security of a facility.

Automated HLS–CAM™

Because of HLS–CAM's broad scope of implementation, NDPCI partnered with Intelliorg, Inc., to automate HLS–CAM, optimize its application, and enable efficient and accurate training of law enforcement personnel. The end product, Automated HLS–CAM™, is now available.

In June 2004, NDPCI received a grant from ODP to demonstrate the HLS–CAM methodology and Automated HLS–CAM™ in the States of Florida and Mississippi.

Training

NDPCI provides classroom training sessions that cover all aspects of the HLS–CAM methodology. Students representing many disciplines and backgrounds, including all emergency response providers, attend these 3-day courses offered at a variety of locations throughout the nation. The HLS–CAM training course provides students with a working knowledge of the HLS–CAM process as well as tools for using the HLS–CAM model in their particular community, in conjunction with their jurisdictional expertise.

Appendix III: A Promising Program

Operation Archangel: A Major Step in the Right Direction

Operation Archangel is an initiative being developed by the city and County of Los Angeles, the California State Office of Homeland Security, and DHS. Its primary focus is to prevent terrorist acts and critical incidents. It will eventually become applicable and exportable to all levels and sizes of government law enforcement agencies.

Operation Archangel is divided into four distinct, yet integrated initiatives:

- **Identification and Prioritization of Critical Assets:** Archangel has established a criterion, or standard, for identifying assets that are deemed critical. The Archangel definition of a critical asset is the product of an indepth, nationwide study of working models and publications that involved subject matter experts and stakeholders. The Archangel Critical Asset Definition will be used during a comprehensive reinventory of the city of Los Angeles, and is currently being considered for use by the California State Office of Homeland Security as its statewide standard. This definition will be used to help determine resource allocation.

- **Critical Asset Assessments (CAAs):** Archangel features the following three-tiered template for conducting critical asset assessments from a multiagency perspective:

  - Conduct appropriate vulnerability assessments (VAs) to determine and reduce a location's degree of vulnerability.

  - Harvest detailed, location-specific information (e.g., names, phone numbers, floor plans, exterior signs/characteristics), in readiness information folders (RIFs) for use by preincident planners and onsite incident commanders during critical incidents.

  - Draft site-specific, preincident security enhancement plans and postoccurrence action plans to provide planners and incident commanders with tactical guidance and insight in the field.

- **Archangel Critical Asset Management System (ACAMS):** Archangel is working with DHS to develop an interoperable database to manage the wealth of information associated with critical assets. The ACAMS development process has been broken down into three specific information collection and planning phases:

  - Critical asset information, including site-specific preincident security enhancement plans, for use by strategists to prevent and deter incidents from occurring.

  - Response information folders containing site-specific facility information.

  - Site-specific postoccurrence action plans for the incident command staff to use should an event occur to the asset despite efforts to the contrary.

- **Archangel Security Augmentation Teams (SATs):** SATs are plainclothes low-profile teams of personnel specifically trained and uniquely equipped to provide a comprehensive cloak of security to a threatened asset. Primarily, a SAT would be deployed when intelligence indicates that a reasonable threat may be directed at a critical asset or event. However, in the absence of clear intelligence, the SAT would deploy to critical assets throughout its area of responsibility, providing a low-key, but nonetheless visible and viable, enhancement to the resident security measures.

Appendix IV: Risk Assessment Training

The courses listed below are available to the law enforcement community and should be considered for integration into the training of personnel who are tasked with conducting risk and threat assessments:

- **Weapons of Mass Destruction: Threat and Risk Assessment (Local Jurisdiction):** DHS, Border and Transportation Security, ODP offers this course, which is delivered by the National Emergency Response and Rescue Training Center, Texas Engineering Extension Services, a member of NDCPI. The objective of the course is to teach attendees how to conduct comprehensive risk assessments and identify necessary countermeasures. The course is free to eligible jurisdictions, as determined by ODP. To enroll in this course, phone 1–800–368–6498, or go to www.fema.gov/compendium/course.

- **Homeland Security Comprehensive Assessment Model (HLS–CAM):** HLS–CAM is a 5-part continuous program that consists of threat assessment, criticality assessment, an analytical target matrix, a community priority assessment plan, and vulnerability assessment. NDCPI provides training that teaches students how to use the HLS–CAM model in their particular communities in conjunction with their jurisdictional expertise and gives students a working knowledge of the HLS–CAM process. For information regarding this course, contact NDCPI at 407–254–7100 or e-mail ed.dorce@ocfl.net.

- **State Strategy Technical Assistance:** Under the State and Local Domestic Preparedness Technical Assistance Program, ODP has implemented a State Strategy Technical Assistance component to help states meet the needs assessment and comprehensive planning required under ODP's Fiscal Year 1999 State Domestic Preparedness Equipment Support Program. More specifically, State Strategy Technical Assistance assists states in developing and implementing a 3-year state strategy to enhance a jurisdiction's preparedness for a terrorist incident involving weapons of mass destruction. The goals of the program are to enhance the state's and local jurisdictions' understanding of the assessment process; their ability to conduct assessments; and their ability to develop a 3-year state strategy. ODP is providing three distinct training sessions to better prepare state and local jurisdictions to meet each program goal. For further information on the Homeland Security Preparedness Technical Assistance Program, call ODP's Help Line at 1–800–368–6498 or e-mail askcsid@dhs.gov.

- **Assessing Terrorism Related Risk Workshop:** This workshop, provided by the S2 Safety and Intelligence Institute, aids security and public safety planners in developing an effective methodology for evaluating terrorism-related risk. It introduces the various types of terrorism-related risks and walks the students through the process of conducting a qualitative risk assessment. It uses exercises to help students understand the process of risk assessment and to teach them how to apply risk management principles to anti-terrorism and security planning.

In addition to exploring risk management principles, this workshop introduces students to unique challenges and solutions for evaluating vulnerability in specific types of terrorist attack scenarios. Some of the vulnerability assessment methods explored during the program include quantitative performance-based physical security assessment, qualitative blast vulnerability assessment, and analysis of vehicle barrier design and performance.

The workshop is intended for security managers, facility managers, military force protection officers, emergency planners, and city and government planning officials, and is restricted to verified security, law enforcement, and government employees only. CHS-certified practitioners are eligible for 16 hours of CEU/inservice training credit through the American College of Forensic Examiners. Assessing Terrorism Related Risk is presented in two 8-hour days. For more information, call 727–461–0066 or go to http://222.s2institute.com.

References

Jopeck, Ed. n.d. Continuous Risk Management—A Next Generation Approach to Security Management. Draft monograph prepared for Veridian-Trident Systems, Alexandria, VA.

National Emergency Response and Rescue Training Center. n.d. Assessment and Strategy Development: Introduction to the Assessment Process. Briefing. College Station, TX: Texas Engineering Extension Service.

Needle, Jerome A. 2004. *Post September 11 Policing: Best Practices for Managing New Realities.* Survey. Alexandria, VA: International Association of Chiefs of Police.

Proteus Security Group. 1997. Risk: *A Risk Model.* Monograph. The Proteus Security Group, Inc. Available online at http://members.aol.com/proteus101/risk.html.

The White House. 2003. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* Washington, DC.

Wohlstetter, Roberta. 1962. Foreword to *Pearl Harbor: Warning and Decision.* Palo Alto, CA: Stanford University Press.

Bibliography

Association of American Railroads. 2002. *Terrorism, Risk Analysis and Security Management Plan.* Washington, DC.

Flynt, Bill, and Ron Olin. 2002. The Red, Gray and Blue Model. *The Police Chief Magazine.* 69(2) (February).

Jopeck, Ed, and Geoff French. 2003. *Risk Analysis and Risk Management: Considerations for Homeland Security.* Alexandria, VA: Veridian.

Kempfer, Hal. 2002. Threat Assessment Process Supporting Risk and Vulnerability Assessments. Long Beach, CA: Knowledge & Intelligence Program Professionals.

Marynik, Jerry. 1998. *Threat Assessment Guide Evaluating and Civilianizing Criminal Extremist Groups.* Sacramento, CA.: California Department of Justice.

National Insitute of Justice. 2002. *Chemical Facility Vulnerability Assessment Methodology.* Special Report. NCJ 195171. U.S. Department of Justice.

New York State Office of Public Security. n.d. *The New York State Homeland Security System Definition.* Albany, NY.

North Carolina Department of Agriculture and Consumer Services. n.d. *Terrorism Threat Vulnerability Self Assessment Tool.*

Parachini, John. 2000. Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities. Testimony before the House Subcommittee on National Security, Veterans Affairs, and International Relations.

Major Cities Chiefs Association. 2004. Terrorist Alert Policy: Local Law Enforcement Threat Guidelines. Prepared for the Office of Domestic Preparedness. Washington, DC: U.S. Department of Homeland Security.

Office for Domestic Preparedness. 2003. *Vulnerability Assessment Methodologies Report.* Phase I final report. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. 2003. *Assessment and Strategy Development Tool Kit.* Original edition, U.S. Department of Justice, 1999. Washington, DC.

U.S. Department of Homeland Security. n.d. Homeland Security Advisory System. Available online at www.dhs.gov/dhspublic/display?content=3927.

U.S. General Accounting Office. 1998. *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Initiatives.* Washington, DC.

The White House. 2001. *National Strategy for Combating Terrorism.* Washington, DC.