



THE OFFICE FOR DOMESTIC PREPAREDNESS GUIDELINES FOR HOMELAND SECURITY JUNE 2003

Prevention and Deterrence

U.S. Department of Homeland Security

U.S. Department of Homeland Security
Office for Domestic Preparedness

810 Seventh Street, NW
Washington, DC 20531

Tom Ridge
Secretary

Office for Domestic Preparedness
World Wide Web Homepage:
www.ojp.usdoj.gov/odp

ODP HelpLine
1-800-368-6498

The Office for Domestic Preparedness
Prevention Guidelines for Homeland Security
June 2003

Introduction

The preeminence of prevention as a component of Homeland Security is made clear in the opening statements of the Executive Summary, **The National Strategy for Homeland Security**:

The strategic objectives of homeland security in order of priority are to:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism, and;
- Minimize the damage and recover from attacks that may occur.¹

Within the text of that document, the meaning is unambiguous. Even the definition of homeland security makes prevention an imperative: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."²

Prevention is a broad term that is often contextually defined. In the context of terrorism employing weapons of mass destruction (WMD), the **National Strategy for Homeland Security** includes the following elements that comprise prevention:

- "...deter all potential terrorists from attacking America through our uncompromising commitment to defeating terrorism wherever it appears."
- "...detect terrorists before they strike."
- "...prevent them and their instruments of terror from entering our country."
- "...take decisive action to eliminate the threat they pose."³

In September 2002, the Office for Domestic Preparedness (ODP) began a "task analysis" process to identify, with the assistance of multi-disciplinary, multi-wave Subject Matter Experts (SMEs), some of the key elements of "Prevention" within the framework of WMD Terrorism and Homeland Security. The process began with a solicitation of open-ended responses to the following:

"At this stage, we are simply soliciting the insight and comments of the Subject Matter Experts (SMEs) regarding the objectives which are most appropriate to prevention of WMD attacks and threats of terrorism, of all varieties (Nuclear, Biological, Chemical, Incendiary, Explosive, Cyber/Technological)."

¹ Office of Homeland Security. (2002). **National Strategy for Homeland Security**. Washington, DC: Government Printing Office. P.vii.

² Ibid. P. 2.

³ Ibid..

The comments were lengthy and, once collated and organized, coalesced logically into categories. The next step in the process involved SMEs revising, elaborating upon, and rating the importance of the tasks identified in the first solicitation. The tasks were then screened and collapsed, where possible. As a result of this process, a list of the most critical tasks was developed. These tasks do not represent a comprehensive list because such a list would be impossible to develop in this time of emerging threats and innovative tactics. Rather, these tasks reflect a base of key actions or activities representing a “**framework for prevention**” that each jurisdiction should consider in adapting to the exigencies of terrorism.

Application of the Guidelines

These Guidelines represent, at this stage of development, a set of general activities, objectives, and elements that organizations as well as those in command positions within the organizations, should consider in the development of prevention plans. The Guidelines are divided into the functional categories of Collaboration, Information Sharing, Threat Recognition, Risk Management, and Intervention. Prevention, if it is to be effective, begins before a response is necessary. The tasks and activities in this booklet, however, make it clear that preventing further harm is a necessary aspect of prevention and one that makes prevention and response seamless.

Collaboration is critical for agencies, organizations and jurisdictions to develop a framework for prevention. Describing tasks as Law Enforcement, Fire, Emergency Management Agency, Public Health, etc. is often an impediment to collaboration by maintaining “stovepipes”. We propose that the tasks and activities suggested in the Guidelines be considered by **Jurisdictions**, as opposed by disciplines, and the responsibilities for action and implementation be determined collaboratively within those jurisdictions, based on resources, agencies, and personnel.

To establishing the “Jurisdiction” as the locus of activity, control, and responsibility, we recommend that policy makers and stakeholders collaboratively address each of the tasks listed below, defining each in the context of the organizations at the local, regional, state, and federal levels with which they have relationships, and establish a “framework for prevention” unique to the Jurisdiction’s capabilities, threats, vulnerabilities, and risks, as well as the available resources.

If the activities delineated below are considered, it is likely a “cultural shift” will occur among the public safety agencies, organizations and personnel. This “cultural shift” is more a product of the process than an intended consequence. The SMEs in a recent panel stated:

“As a consequence of the collaboration, information sharing, and coordinated activities inherent in adopting and executing a Risk Management Model, or some other analytical risk and vulnerability model, it is expected that there will be a “Cultural Shift” in the public safety community.”

The “Cultural Shift” will occur through a process including:

- Identify a prime mover (an organization, person, or event)
- Identify public and private Stakeholders
- Establish Meeting(s) of the Stakeholders to:

- Articulate the Mission, Goals, Objectives in Preventing terrorism
- Plan Joint/Integrated Training and Awareness Training
- Plan Joint Exercises
- Adopt a Risk Management Decision Model
- Develop MOUs and Policies to enable cooperation
- Centralize an Information Management System and Fusion Center
- Define agency or individual responsibility for all of the Prevention tasks and activities described in the Guidelines, appropriate to the jurisdiction.

The shared motivation of the Jurisdictions' which includes fiscal support, public safety, proactive steps to deter and prevent attacks should produce shared values in existing organizations and personnel. These values should become "organic" and perpetuated through pre-service training as well as in-service training and exercises.

We include the information on this "Cultural Shift" because it represents a significant element of the overarching process jurisdictions should consider when implementing a "framework for prevention" and applying these Guidelines.

The Glossary accompanying the Guidelines provides specific definitions and descriptions. While there are other definitions that could have been used, these selected definitions represent the reference points for the SMEs who considered the issues associated with Prevention and the development of the Guidelines. The Glossary was not intended to be comprehensive in addressing all terms and terminology related to WMD terrorism, but instead was developed to articulate and define the terms associated with this document. Additionally, a brief overview of the various analytic models as examples for assessing risk and vulnerability is contained in the appendix.

Note that this document, and its accompanying Glossary, are a living document. SMEs will continue to refine and append the materials to improve their comprehensiveness and specificity. The Guidelines are likely to always be "in progress" and subject to revision, but they are being released so that agencies, organizations, and jurisdictions can begin to benefit from the work of ODP and its SMEs.

Jurisdictions seeking to improve “Collaborations” between and among public and private sector agencies to prevent WMD terrorism should:

- 1. Recognize that there is a need for prevention activities and actions and that prevention is critical to a jurisdiction’s preparation for terrorism.**
 - Provide the political leadership with sufficient “awareness” and “process” training to develop an appreciation for the importance of prevention;
 - Acquaint policy makers with the role governmental administrators play in preventing attacks and reducing vulnerability;
 - Ensure that plans for WMD incorporate and begin with prevention activities;
 - Establish policies, budgets, and plans that reflect prevention priority;
 - Reinforce the priority of prevention through exercises and scenarios.

- 2. Establish a system, center, or task force to serve as a “clearing house” for all potentially relevant domestically generated terrorism data and information to ensure interpretation and assessment of the data and information.**
 - Follow provisions of 28 Code of Federal Regulations (CFR) pertaining to Criminal Intelligence Systems operating policies (Chapter 1, Part 23 in particular);
 - Establish an “all source intelligence fusion center”;
 - Prioritize the intelligence fusion center services in order to accommodate the task force as one of its principal accounts;
 - Conduct an information needs analysis as a component of the intelligence center or system;
 - Ensure that intelligence requirements are formulated in a clear and concise manner;
 - Ensure that the information gathering and sharing system includes all “owners” of key assets/critical infrastructure;
 - Establish a workable and reasonable “tier-line” approach for the sharing of information with other agencies, jurisdictions, and the private sector;
 - Ensure appropriate representation in the task force and in the Intelligence Center, including public and private representatives;
 - Establish the information system using plans and processes that reasonably assure that all terrorist-related activity is reported to the system, fusion center, or task force;
 - Identify “intelligence requirements” with sufficient specificity to alert observers to watch for certain things, and train them to forward the information to one central point;

- Establish coordination points with related agencies to share information, strategies, and tactics;
 - Establish a clear path of information from observers (e.g., police) to the fusion center;
 - Conduct education/training periodically to test observation of suspicious events and behaviors.
- 3. Prepare Memorandum of Understanding (MOUs) and formal coordination agreements between appropriate agencies (public and private) describing mechanisms to exchange information regarding vulnerabilities and risks, coordination of responses, and processes to facilitate information sharing and multi-jurisdictional preemption of terrorist acts or events.**
- Identify in the planning process and agreements the appropriate agencies, public and private, that need to participate (i.e., supply information and/or receive information and intelligence) in collaborative information sharing;
 - Identify in the agreements the types and parameters of information exchanged, including standard methods of defining data, information, vulnerabilities, and risks;
 - Establish formal agreements or MOUs that identify the agencies, the points of contact, and the parameters of exchanges of information;
 - Ensure that the process of exchanging information achieves collaboration among agencies and organizations;
 - Include in the exchange of information blueprints, schematics, and other information on infrastructure on a need-to-know basis.
- 4. Use Community-policing initiatives, strategies, and tactics as a basis to identify suspicious activities related to terrorism.**
- Train Law Enforcement in the jurisdiction to utilize community policing or other similar collaborative policing approaches;
 - Encourage prevention, proactive policing, and close working relationships between the police and the community;
 - Train police officers to accomplish the mission, goals, and objectives of the community policing philosophy while engaging in the prevention of terrorism and terrorist threats;
 - Provide examples, training, and materials (e.g., public service announcements, videos, fliers, other media materials) that may aid the recognition of terrorism to Community policing contacts in order to make members of the community aware of those actions, behaviors, and events that constitute “suspicious”;
 - Ensure that members of the community are aware of the means of and processes for relaying observed data to police officers and police

organizations, just as they are, or should be, aware of methods to relay information to Community Policing officers;

- Organize community meetings to emphasize prevention strategies, vigilance, and public awareness;
- Train police officers to understand the legally appropriate response to data relayed by members of the community;
- Train, prepare, and test police officers on the most appropriate and expedient methods for relaying the data to the intelligence center, fusion center, or task force for assessment, and analysis.

5. Explicitly develop “social capital” through collaboration between the private sector, law enforcement and other partners so that data, information, assistance, and “best practices” may be shared and collaborative processes developed.

- Examine all plans and processes to ensure that they reflect clear linkages between public and private sectors and stakeholders;
- Examine planning documents to ensure that fluid coordination is represented in the MOUs, task force organization, and other formal agreements;
- Reserve task force seats for key private sector representatives;
- Ensure that the planning documents and processes establish facility sharing and the sharing of resources as well as information;
- Structure the information sharing, with appropriate legal limitations, so that the private sector receives accurate, timely, and critical information on a need-to-know basis;
- Establish a relationship of trust, which will lead to social capital, with the private sector as a partner in the information sharing relationships;
- Include, private sector organizations that are representative groups such as the Chamber of Commerce in formal or informal relationships;
- Establish multi-disciplinary cooperation, including the private sector, in target hardening activities, which should include threat analysis and risk management, matched with protocol and treatment;
- Employ practical exercises and assessment centers to reinforce the “social capital;”
- Use After Action Reports to identify ways to strengthen and perpetuate collaboration;
- Construct conceptual, structural, and strategic exercises and scenarios to reinforce collaboration.

6. Coordinate Federal, state, and local information, plans and actions for assessments, prevention procedures, infrastructure protection, and funding priorities to address prevention.

- Establish all-hazards councils with special conditions identifying dimensions, including prevention for funding decisions with

demonstrated cooperation and demonstrated activities associated with prevention;

- Overtly develop an “inclusion strategy” as a measurable doctrine to influence the environment of stakeholder agencies;
- Include prevention in a planning process similar to the incident management system/incident command system (IMS/ICS) but in a continuing process as opposed to during an “incident” or event;
- Coordinate multi-disciplinary prevention training and exercises that go beyond existing response training and exercises;
- Conduct training and exercises with sufficient frequency to ensure coordination;
- Ascertain that every training curriculum includes an appropriate incident management system, such as the ICS model, to encourage an understanding of roles and to facilitate coordination and cooperation, both horizontally and vertically;
- Establish awareness training for all agencies and the public that includes protection measures and emphasizes collaboration;
- Achieve coordination of training among all constituent jurisdictions to ensure that consistent and coordinated models and approaches to risk identification and protection are used;
- Participate in exercises to test collaboration and awareness or vulnerabilities and coordination of prevention approaches based on a risk management model;
- Link coordination, training, and exercises on prevention to funding priorities.

7. Establish a regional prevention information command center and coordinate the flow of information (in and out) regarding infrastructure.

- Establish MOUs and plans to coalesce cooperation and collaboration with all appropriate agencies to create a Joint Information Center for prevention;
- Link fusion center activities to other-than-public safety organizations, including transportation, public health, health services, and all other appropriate organizations;
- Establish a formal liaison with second and third responder agencies and organizations, as well as support organizations, to emphasize those agencies’ roles in prevention;
- Integrate regional prevention information centers with task forces, using a model consistent with the IMS/ICS model;
- Establish “design, fabrication and construction monitoring” programs to provide consultation and advice regarding anti-terrorism measures.

8. Exercise prevention and collaboration measures.

- Include prevention elements in every exercise, including those testing response, to demonstrate to officials that, had those elements been recognized and acted upon, the event would have been altered or prevented;
- In exercises, embed prevention cues that are, or should be, visible to agencies other than law enforcement, thereby necessitating collaboration in order for the cues to be recognized and acted upon;
- Make collaboration essential to the success of every exercise;
- Adopt the proposition that “failures” in prevention exercises are “successes” in identifying gaps and areas for collaborative improvement, ultimately making the communities safer and more secure;
- Conduct “red team” exercises to test the collaboration dimension of prevention;
- Coordinate multi-disciplinary prevention training and exercises that go beyond existing response training and exercises;
- Conduct training and exercises with sufficient frequency to ensure coordination;
- Examine all training curriculum to ensure that an appropriate incident management system, such as the IMS/ICS model, is used, in order to encourage an understanding of roles and facilitate coordination and cooperation, both horizontally and vertically;
- Conduct awareness training for all agencies and the public, including prevention and protection measures, that emphasizes collaboration;
- Ensure coordination of training among all constituent jurisdictions so that consistent and coordinated models and approaches to risk identification, risk management, and protection are used;
- Participate in exercises to test collaboration and awareness of vulnerabilities and coordination of prevention approaches based on a risk management model;
- Link coordination, training, and exercises on prevention to funding priorities;
- Make funding conditional on degree of collaboration and exercise evaluations.

Jurisdictions seeking to develop “Information Sharing” linkages to prevent WMD terrorism should:

1. Enhance analytic capabilities for linking information on potential threats.

- Train analysts to perform analysis, linkage, and fusion of data;
- Identify the data categories most relevant to the threats defined;
- Identify the data sources from whom or from which the data can be received, extracted, or collected;
- Clearly define data gathering, analysis, and dissemination formats;
- Identify the technology and techniques most appropriate to the analysis;
- Disseminate information and intelligence on a need-to-know basis, defined *pre hoc* by a task force or other representative group;
- Integrate public order issues, crime analyses, antiterrorism and counterterrorism concerns with street level data and information.

2. Establish a framework for sharing information/intelligence and prevention strategies, particularly between Law Enforcement and other agencies.

- Use joint terrorism task forces and the state’s homeland security office to facilitate information sharing;
- Integrate information sharing into the “Intelligence Cycle;”
- Establish data and information gathering, analysis, interpretation, and dissemination processes within Law Enforcement, driven by WMD terrorism;
- Establish a “fusion center” for the accumulation of data, and clearly define the dissemination of data and information as well as intelligence.
- To the greatest extent possible, retain analytical dimensions in each organization where data and information can best be understood and linked after dissemination by fusion center;
- Clearly articulate categories of data, information, and intelligence to be shared, as well as conduct and behaviors defined by the data.
- Include in the information sharing framework private emergency medical services (EMS) and volunteer firefighters, with access based on a need-to-know basis, and with appropriate limitations;
- Establish a process for information sharing across all tiers of government and the private sector, which specifies dissemination to the lowest organizational level possible to ensure that line personnel will receive appropriate information, on a need-to-know basis;

- Review federal and state-level laws regulating gathering and acting upon information to ensure consistency with the framework for information gathering and sharing.

3. Establish an information exchange network and directory for information sharing.

- Utilize existing systems, such as the law enforcement organization (LEO), the Criminal Justice Information System, or other systems that are appropriately secure and capable of interfacing with other agencies;
- Continue the process of developing next generation information systems that can better serve the agencies, organizations, and jurisdictions;
- Include wireless and traditional Internet capabilities for voice and data, as well as alternate infrastructure, to promote rapid, secure, and accessible information sharing, such as the internet, intranet and email;
- Develop and maintain "call down" lists for each agency;
- Design the Intelligence Cycle to ensure that all appropriate agencies and organizations (Public Health, EMA, EMS, Fire, selected Private Sector, etc.) at all tiers (local, regional, and state) receive restricted information on a need-to-know basis, as defined in advance by the task force or central authority;
- Examine the information sharing framework periodically to determine that all agencies are sharing appropriate information systematically;
- Establish a system for disease surveillance, such as the Health Alert Network, to ensure data interoperability with the Emergency Management Agency, and which is also integrated into the information exchange network;
- Consider ease of use and familiarity in defining the information network to ensure that information is accessible and usable;
- Tie together the various analytic centers so that information and intelligence dissemination is comprehensive and consistent;
- Review the participant agencies and organizations to ensure that all appropriate representatives are linked to the information sharing system;
- Evaluate the collection, assessment, storage, access, and dissemination of information periodically;
- Establish basic standards by which the intelligence products are created and shared;
- Establish protocols to insure that information is being shared with agencies and organizations that are overtly or potentially impacted by an identified threat;

- Establish protocols to insure that information is being linked with the private sector, particularly that associated with critical infrastructure, on a need to know basis;
 - Disseminate valuable and usable information to agencies and organizations which are or implicitly are affected by the information.
- 4. Ensure a reliable capability to alert officials and emergency personnel of terrorism threats, with warnings initiated, received, and relayed to alert key decision makers and emergency personnel regardless of the threat or operational involvement, as well as a robust, redundant, timely system for sharing information with other agencies, organizations, and the public.**
- Use a Risk Management Model or some other appropriate analytical model to identify “hazards” and the appropriate information to be disseminated;
 - Test the process for implementing the model against a variety of threats and hazards;
 - Provide system redundancy to provide alternative communications using two-way communications, voice, and data;
 - Insure the system is compatible with internal and external communications systems of the parent organization.
- 5. Establish a multi-disciplinary approach to public information for education and awareness and protective action information.**
- Participate in public information campaigns to enhance awareness and public cooperation in information gathering;
 - Provide alert systems that can be implemented for hospitals, emergency rooms and private practice physicians;
 - Provide public health information to the public on vaccination risks and advantages.
- 6. Develop an adaptive, organic architecture to facilitate information sharing.**
- Identify key stakeholders, contributors, and consumers of information;
 - Include stakeholders in planning process for information sharing;
 - Agree upon the location, structure, and funding for a centralized intelligence center or fusion center;
 - Select and train criminal intelligence analysts;
 - Secure access to all sources of data, information, and intelligence revising and refining sources constantly;

- Adopt or develop an analytical model for assessing key assets, critical infrastructure, risk, vulnerability, and options for managing risk;
- Test new sources and methods of information gathering and sharing to enhance the complex adaptive nature of the analysis process;
- Establish clear methods for disseminating the intelligence products;
- Provide for competent legal advice on the operation of the intelligence center or fusion center, the dissemination of information and intelligence, and the actions taken based on the information and intelligence.

Jurisdictions considering “Risk Management”⁴ approaches to reduce vulnerability of targets and prevent WMD terrorism should:

- 1. Adopt or develop an appropriate analytic “risk management” model to assess risk or vulnerability and identify probable treatment methods to reduce risk.**
- 2. Provide training and technical assistance to local governments in developing, adopting, and implementing building codes, fire codes, and land-use ordinances consistent with crime prevention methods.**
- 3. Design the built environment to reduce vulnerability, being certain that Crime Prevention through Environmental Design (CPTED) principles and methods are available to agencies and organizations for target hardening" enhancement of appropriate locations in the built environment.**
- 4. Establish “anti-terrorism" CPTED "target hardening” activities.**
 - Assess threat, risk, and vulnerability;
 - Balance CPTED strategies against the threat, risk, and vulnerability;
 - Employ the appropriate CPTED measures, given the level of threat, risk, and vulnerability. Measures may include:
 - Install adequate security lighting;
 - Use planters and bollards as impediments or obstacles to prevent cars or trucks from driving into or parking close to potential targets;
 - Use security cameras in key locations;
 - Increase police presence at sensitive locations;
 - Use random inspection of trucks/vans entering target-rich environments;
 - Establish protocol for searches of people and their possessions when entering large gatherings;
 - Adopt biometric technology, where applicable, to enhance access control and identification.

⁴ “Risk Management” was previously labeled “Target Hardening”. The broader description was selected to reflect the decision-making processes inherent in determining which assets to secure, the methods and resources used to address the security, and the cost-benefit calculus associated with those decisions.

- 5. Develop incentives (such as ordinance, legislation, or insurance ratings) to encourage CPTED at critical or mass-gathering locations and to encourage mitigation activities sponsored by public/private partnerships:**
 - Establish state laws, local ordinances and/or regulations allowing incentives for CPTED anti-terrorism initiatives;
 - Extend sovereign immunity to cover advice and consultation for CPTED construction.

- 6. Assist and collaborate with the private sector to (1) identify the most serious vulnerabilities and risks, while suggesting the use of a common analytical model, (2) collaborate with the private sector to implement risk management (target hardening), and (3) inform the private sector of threats and efforts that could be taken to prevent incidents or minimize damage, in concert with the actions taken by public sector agencies;**
 - Facilitate meetings between private sector and the public sector representatives, to enable them to report back to the larger private sector group, on a need-to-know basis;
 - Establish mutual goals and objectives by geographic region/neighborhood as well as by industry sector;
 - Analyze and document protective measures for key assets/critical infrastructure as a result of assistance provided, to maintain accountability;
 - Review legal status of mass gathering ordinances requiring specified levels of participation by the private sector and incorporate preventive measures in the requirements.

- 7. Prioritize cyber infrastructure threats by considering vulnerability versus potential economic loss, as well as target hardening, alert, and response plans.**
 - Ensure that plans are consistent with the National Strategy to Secure Cyberspace (February 2003) infrastructure protection plans;
 - Apply risk management principles to public and private infrastructure assets.

- 8. As applicable and in concert with federal resources, establish perimeter and transportation security at borders and implement strict controls based on imminent threats.**

9. Employ innovative, visible, or advertised surveillance at vulnerable or key sites to increase the probability of recognition and capture.

- Utilize non-enforcement governmental personnel trained to use “watchout situations” to identify cues of terrorists and terrorism;
- Use law enforcement personnel to observe public and transportation movements (e.g., seat-belt checks, sobriety checkpoints, driver’s license checkpoints, traffic defiles, etc.) to better observe suspicious behavior and to serve as a deterrent;
- Compile lists of commonly available devices, equipment, and materials that can be used for criminal/terrorist purposes and train enforcement, compliance, and investigative personnel to be aware of the potential value in detecting and preventing terrorist events, using “watchout situation” training.

10. Identify and include in planning documents innovative approaches to disrupt potential actions of terrorists at strategic locations or during sensitive times.

- Conduct seat-belt checks, driver’s license checks, or sobriety checkpoints in high risk areas;
- Increase mobile patrols, walking patrols and mounted patrols in vulnerable areas;
- Alter traffic patterns to disrupt ingress and egress temporarily;
- Standardize notification procedures and reports of apartment rentals under suspicious circumstances;
- Develop public service announcements regarding health surveillance.

11. “Vaccinate” organizations against WMD attack to make them less vulnerable by:

- Using mock or “red team” attacks;
- Conducting “white level inspections” focused on prevention and risk reduction;
- Conducting exercises using private sector assets as well as public sector resources;
- Testing business continuity plans through exercises and tabletops;
- Conducting joint exercises to enhance relationships between public and private organizations.

12. Conduct threat analysis and site surveys training to provide assistance and recommendations to agencies, organizations and stakeholders on making assets less vulnerable.

- Employ CPTED experts to advise public and private organizations;
- Balance treatment with threat, using a risk management model;
- Publicize successes;
- Assist the private sector in recognizing the positive financial impact of WMD prevention through tax assistance for prevention and liability protection for advanced prevention development.

13. Conduct vaccinations, as appropriate, to reduce vulnerability to biological agents.

14. Establish or review quarantine authorities and include levels of isolation and quarantine in the risk management plan and model to prevent contamination or infection of unaffected persons or places.

15. Consistent with a “Risk Management Model,” conduct vulnerability assessments and institute procedures to secure facilities, property, equipment, and materials:

- Institute a culture of security-consciousness to avoid loss of uniforms or equipment that could be used to impersonate a fire, enforcement, security, or other public or safety official;
- Ensure security accountability consistent with the risk management model of key facilities, police stations, fire stations, health centers, and emergency facilities;
- Include terrorism prevention security issues in building inspections and premises inspections;
- Identify high risk and high consequence facilities, such as universities’ and private laboratories’ bio-storage facilities for extraordinary security awareness and accountability;
- Monitor and secure biological and radiological samples in college and university laboratories;
- Disperse stored resources to reduce vulnerability of sensitive materials;
- Engage in target hardening of facilities, based on threat assessments, to include fences, access control, traffic signaling devices, and biological and radiological sensors;
- Enhance facilities’ security to reduce the threat of theft of Public Works equipment, or other similar equipment, that could be used in an attack;
- Identify critical infrastructure, such a bridges and tunnels, for preventive observation and surveillance.

Jurisdictions seeking to improve “Threat Recognition” to halt the development of a WMD terrorism threat before it is executed should:

- 1. Create a secure system to collect, screen, and store relevant information with investigative value (including consequence management and medical surveillance, public health data, firefighters data, immigration and naturalization services (INS) information, etc.) in a database, hotline, or “data warehouse,” using nationally accepted definitions and protocols for “intelligence data” security and access, and that is controlled and protected at the federal level, available through a secure information portal and network, to be disseminated to those key decision-makers involved in terrorism prevention strategies and investigations, using the following processes or resources:**
 - Establish a rating and criteria system to reflect the quality and urgency of information, then distribute it widely to foster consistency and reliability of data, information, and intelligence;
 - Establish an intelligence database with the capacity to search existing police record management systems, identify associations among persons, organizations, locations, vehicles and incidents;
 - Establish a database, similar to secure national databases, with information shared on a need-to-know basis among those best equipped to collect and collate that information;
 - Establish definitions consistent with established protocols, such as Foreign Affairs Manual Volume 12 (Definitions of Diplomatic Security Terms) or other accepted and established definitions;
 - Conduct intelligence operations consistent with 28 CFR 23;
 - Conduct operations consistent with American National Standard for Information Technology – Role Based Access Control;
 - Conduct operations in conjunction with the Terrorist Threat Integration Center, DHS.

- 2. Train personnel to be familiar with standards for driver’s licenses and other forms of identification, consistent with the U.S. Identification Manual or other reference guides.**
 - Develop reference materials describing or providing information on, examples of, and criteria for:
 - driver's licenses;
 - commercial driver's licenses;
 - minor's licenses;
 - non-driver Identification cards;
 - identifying information on each form of documentation;

- types of laminations;
- security features including bar codes and magnetic strips;
- if license and signature are digitized for computer retrieval;
- telephone numbers for central authority of state issuance and enforcement to check validity of identification.

3. Map threats and capabilities for preemptive action:

- Establish geographic information system (GIS) and global positioning system (GPS) capabilities, if resources permit;
- Train personnel to access geocoded information;
- Provide technology and equipment for immediate retrieval of geocoded information.

4. Coordinate public safety communications to forewarn of threats:

- Integrate emergency warning systems for law enforcement;
- Integrate emergency warning systems for non-law enforcement agencies;
- Integrate public warning systems.

5. Train law enforcement personnel and others (e.g., fire, EMS, PW, HC, social services, etc.), using standard definitions, criteria, and terms to recognize as clearly as possible the behavioral, observable, and legal criteria for:

- What constitutes suspicious activity;
- An investigative lead;
- A suspect;
- An associate;
- An inventory of behaviors and/or activities that constitute "suspicious behavior" likely to forewarn of a pending terrorism conspiracy or plot;
- Establish protocol for identifying and responding to terrorists conducting reconnaissance/surveillance of potential targets and train personnel to recognize this behavior;
- Train personnel on the procedures and propriety for approaching persons posing possible threats, such as those taking unusual pictures/video of key sites and targets;
- Train law enforcement to recognize commonly available, dual-use equipment and materials in the context with high-risk locations;
- Conduct random inspection of buildings, facilities, and trucks/vans entering target rich environments;
- Search or screen people and their possessions when entering large gatherings;
- Establish extraordinary identification-verification requirements for activities linked with threats.

- 6. Train law enforcement personnel to link crime analysis queries from patrol officers directly into the database with replies and cues that classify subjects and clearly advise as to appropriate action (i.e., update address, interview and release, photo needed, prints needed, etc.).**
- 7. Establish awareness of general public and the private security sector regarding the identification of terrorists surveilling potential targets and insure that the public knows what constitutes such suspicious activity, as well as the notification processes to advise Public Safety of the information.**
- 8. Develop chemical, biological, and nuclear recognition and tracking systems in public and private sectors, consistent with threat and risk analysis models.**
- 9. Locate and position detection systems and closed circuit television (CCTV) systems in key transportation, energy and infrastructure sites, consistent with a risk management model.**
- 10. Establish analytical tools and linkages with non-governmental organizations to identify suspect groups via financial records, public records, and private records, with appropriate legal restrictions, and shared this information with task forces or fusion centers.**
- 11. Include the utilization of community resources to identify suspicious activities in Community Policing training**
- 12. Using an analytical model for risk management and vulnerability analysis, conduct threat analyses and critical site surveys to the level of training and needs, in order to identify those sites and facilities where threat recognition actions should be concentrated.**
- 13. Develop awareness and “watchout situation” training for other than first responders (public works, public health, health services, social services, public utilities, school officials, etc.) using appropriate behavioral signs, equipment, materials, dual-use potential.**
- 14. Establish an automatic-identification system for vessels, trucks, trains, and other transport vehicles, while maintaining security of information related to high-risk cargo.**
- 15. Enact mass gathering ordinances as protective measures, using models that have been validated, to describe equipment and personnel needs by type of gathering or event.**

- 16. Consistent with an analytical risk management model, facilitate the judicious public sector response and protection of assets, and the sharing of information to recognize threats, based on the vulnerability and threat levels.**
- 17. Institute a management information system to track, locate, and monitor public sector equipment and personnel (police, fire, EMS, HazMat, military, etc.), to immediately recognize losses that could represent terrorist threats.**
- 18. Maintain a current and complete inventory and an accountability system for hazardous materials and biological agents, even during transporting, that supplement procedures for reporting irregularities.**
- 19. Ensure the capability for early diagnosis of health hazards in the community, using epidemiological surveillance methods.**
- 20. Train appropriate personnel to be aware of the Select Agent Program for weaponized agents.**
- 21. Perform “white level” inspections, at a minimum, to discern patterns that can suggest vulnerability to terrorism, as well as safety issues.**
- 22. Recognize the threat potential for land, air, water, rail, mass transit, and other elements of the critical infrastructure, consistent with an analytical risk assessment model, and recommend appropriate prevention strategies**

Jurisdictions seeking to improve “Intervention” to stop terrorists before they can execute a threat should:

- 1. Train personnel to recognize threats and threatening cues and to respond appropriately to suspects preparing for attacks.**
- 2. Train law enforcement personnel in tactical capabilities with special teams of law enforcement, emergency response, and military resources to respond quickly and appropriately in a potential terrorism event with the objective of intervening in an impending attack.**
- 3. Articulate and disseminate the legal criteria for making cases, conducting wiretaps, and conducting surveillance on suspected WMD terrorists through general training and specific tactical training within Law Enforcement, to ensure familiarization with:**
 - Conspiracy statutes;
 - Search and seizure requirements;
 - Foreign Intelligence Surveillance Act (FISA) requirements;
 - Established legal criteria and procedures for intervention in suspicious circumstances and events;
 - Standard Operating Procedures (SOPs) for observing people and targets at high threat locations;
 - Laws that protect public safety information;
 - Contact lists and contact information for legal opinions and assistance.
- 4. Establish pre-service and in-service training in legal, tactical, and strategic aspects of policing in the WMD terrorism environment to enhance the ability to apprehend terrorists.**
- 5. If indicated in an analytical Risk Management Model, develop plans for pre-boarding searches for mass transit vehicles in the event of a credible threat.**
- 6. As indicated in an analytical Risk Management Model, establish plans and needs assessments for deployment of resources to meet known or anticipated threats to preempt or deter events.**
- 7. Facilitate a prosecutorial and judicial structure, process, collaboration, and expertise that enhances successful prosecution of WMD terrorism.**

- 8. Exercise processes for collecting and entering investigative intelligence and retrieving information, to result in the successful intervention and arrest of terrorists.**
- 9. Articulate the legal requisites for authorities to isolate and decontaminate to reduce spread of suspected diseases or agents.**
- 10. Include in Risk Management plan the collateral implications to the private sector in a WMD event intervention and have plans to coordinate mitigation.**

Broader WMD terrorism prevention strategies or approaches with national implications (described in National Strategy for Homeland Security):

- 1. Ensure that legal sanctions reflect the “certainty” of punishment for those engaging in WMD terrorism.**
- 2. Increase perceptions of the invulnerability of the nation, its sites and its populations.**
- 3. Establish the presence of strategic prevention capabilities within a national incident management system.**
- 4. Standardize military assistance protocols for prevention.**
- 5. Prepare, train, exercise, and equip responders to engage in prevention activities and surveillance.**
- 6. Establish coordinated standards for driver’s licenses.**
- 7. Establish a national laboratory for homeland security.**
- 8. Release results of successful resistance to cyber attacks.**
- 9. Develop chemical, biological, and nuclear countermeasures.**

APPENDIX: Glossary of Terms

AntiTerrorism - preventive in nature. It entails using "passive and defensive measures... such as education, foreign liaison training, surveillance, and countersurveillance, designed to deter terrorist activities." It is an "integrated, comprehensive approach ... to counter the terrorist threat The concept has two phases: proactive and reactive. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident."⁵

Community Policing – a "philosophy of policing, based on the concept that police officers and private citizens working together in creative ways can help solve contemporary community problems related to crime, fear of crime, social and physical disorder, and neighborhood decay."⁶

Counterintelligence - "... information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."⁷

Counterterrorism - is responsive or reactive to terrorist threats or attacks. It entails using "active measures... which incorporate the direct intervention of terrorists groups or the targeting... of terrorist personnel."⁸

CPTED — Crime Prevention Through Environmental Design - a method of reducing the perception of crime, the opportunity for crime, and crime itself by altering the physical environment. Employs territoriality (creates a sense of ownership), access control (increases the perceived risk of crime to potential offenders by restructuring or denying access to crime targets), and surveillance (keep potential intruders or attackers under threat of observation).

Design, Fabrication, and Construction Monitoring Programs – typically, codes and ordinances that provide for review of new construction, conditional rezoning petitions, development plans, and special exception petitions for the purpose of decreasing the opportunity for crime and increasing the perception of safety.⁹

⁵ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

⁶ Trojanowicz, Robert and Bonnie Bucqueroux. (1990). *Community Policing: A Contemporary Perspective*. Cincinnati: Anderson Publishing Co.

⁷ 50 USC 401a(3)

⁸ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

⁹ For example, see Plaster, Sherry and Stan Carter. (1993). *Planning for Prevention: Sarasota, Florida's Approach to Crime Prevention Through Environmental Design*. Tallahassee: Florida Criminal Justice Executive Institute.

Fusion Center – an organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence. A model process is likely to include:

- Extract unstructured data
- Extract structured data
- Fuse structured data

Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders. Types of analysis typically conducted in a fusion center include:

- Association Charting
- Temporal Charting
- Spatial Charting
- Link Analysis
- Financial Analysis
- Content Analysis
- Correlation Analysis

Data - unprocessed, unanalyzed, and raw observations, and facts

Force Protection – often used in the military sense to mean a security program designed to protect service members, civilian employees, family members, facilities, and equipment in all locations and situations.¹⁰

Information - processed fact; reporting with or without analysis. It is often prepared for publication or dissemination in some form and is intended to inform rather than warn or advise.

Intelligence - the product of adding value to information and data through analysis. Intelligence is created for a purpose. It is the process by which analysis is applied to information and data to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions. Intelligence serves many purposes among which are the identification and elimination of threat sources, the investigation and resolution of threats, the identification and treatment of security risk, the elimination of threat sources, the mitigation of harm associated with risk, preemption, response, preparation and operations related to threats and risks.

Intelligence cycle - the process by which information and data is collected, evaluated, stored, analyzed, and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, consumer.

¹⁰ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

Intelligence products - the intelligence deliverables.

They are the means by which intelligence is communicated to those who will use it. Intelligence products are not limited to written digests or summaries, reports or notes, and can also include oral warnings, alerts, advisories or notices given to the consumer when justified. It also includes oral briefings and other presentations made by the intelligence professional within the scope of his or her duties and responsibilities.

Need-to-Know - the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.¹¹

Reasonable Suspicion - when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.¹²

Red Team – a technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.

Risk Management Based Intelligence - an approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and counter-measures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations. (See David Schwendiman's *Risk Management Model*, described in appendix.)

¹¹ CIA Directive 1/7. (1998). Security Controls on the Dissemination of Intelligence Information.

¹² 28 CFR 23.20(c).

Social Capital - consists of the stock of active connections among people: the trust, mutual understanding, and shared values and behaviors that bind the members of human networks and communities and make cooperative action possible.¹³

Tear Line - the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized, less-classified version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need-to-know" principle and foreign disclosure guidelines, of the information below the tear line.

Watchout Situations – In fire management and fire service, watchout situations are indicators or trigger points that remind firefighters to reanalyze or to re-evaluate their suppression strategies and tactics. The “watchout situations” in the fire service are more specific and cautionary than the “Ten Standard Fire Orders.” In antiterrorism, the term is used as a metaphor for those observations that can alert trained personnel, not just firefighters but law enforcement, public works, private security, or anyone, to be more cautious, more observant, and more likely to report the unusual behavior or activity to the appropriate authorities.

White level inspections – Consistent with OSHA Construction Health and Safety Excellence (CHASE) partnership, private organizations at the “white level” (intermediate level) must implement a comprehensive written safety and health program based on the ANSI A10.38-1991 Guidelines or OSHA's 1989 Safety and Health Program Management Guidelines; meet a variety of training, management, and audit requirements, and have an acceptable safety record.

¹³ Cohen, D. and Prusak, L. (2001) *In Good Company. How social capital makes organizations work*, Boston, Ma.: Harvard Business School Press. P. 4.