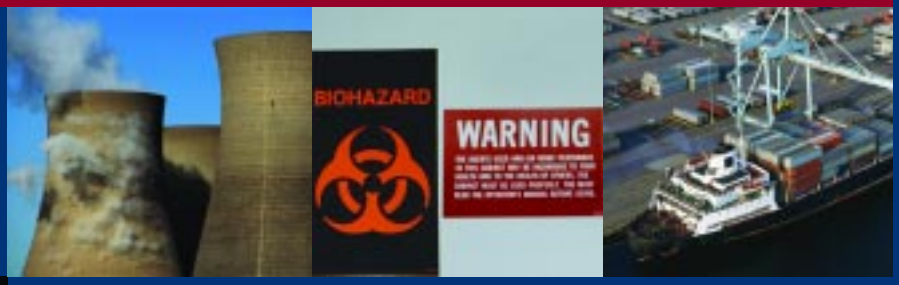

Volume Two: Homeland Security

A GOVERNOR'S GUIDE TO EMERGENCY MANAGEMENT

NGA Center for BEST PRACTICES

Volume Two: Homeland Security

A GOVERNOR'S GUIDE TO EMERGENCY MANAGEMENT

Since their initial meeting in 1908 to discuss interstate water problems, the governors have worked through the National Governors Association (NGA) to deal collectively with issues of public policy and governance. The association's ongoing mission is to support the work of the governors by providing a bipartisan forum to help shape and implement national policy and to solve state problems.

The members of NGA are the governors of the fifty states; the territories of American Samoa, Guam, and the Virgin Islands; and the commonwealths of the Northern Mariana Islands and Puerto Rico. The association has a nine-member Executive Committee and three standing committees: on Economic Development and Commerce, Human Resources, and Natural Resources. Through NGA's committees, governors examine and develop policy and address key state and national issues. Special task forces often are created to focus gubernatorial attention on federal legislation or on state-level issues.

The association works closely with the Administration and Congress on state-federal policy issues through its offices in the Hall of the States in Washington, D.C. The association serves as a vehicle for sharing knowledge of innovative programs among the states and provides technical assistance and consultant services to governors on a wide range of management and policy issues.

NGA's Center for Best Practices is a vehicle for sharing knowledge about innovative state activities, exploring the impact of federal initiatives on state government, and providing technical assistance to states. The Center works in a number of policy fields, including economic development and technology, education, natural resources, energy and environment, health, social services, trade, workforce development, and homeland security.

ISBN 1-55877-360-6

444 North Capitol Street, Washington, D.C. 20001-1512.

Design by zilart! creative. Printed in the United States of America.

Cover photograph of George Washington Bridge courtesy of the Port Authority of New York and New Jersey.

Contents

Acknowledgements

The National Governors Association Center for Best Practices acknowledges the generous financial support of the United States Department of Justice Office of Domestic Preparedness in the preparation and publication of this report. Specifically, we would like to thank Andy Mitchell for his commitment and support in the completion of this project.

This guide is a result of the efforts of a number of dedicated individuals. Sincere appreciation is extended to the governors' homeland security directors and state emergency management directors who expended significant energy in reviewing and commenting on the guide.

The Center for Best Practices would also like to thank the State Chief Information Officers and Chief Information Security Officers for their insightful comments on the cybersecurity chapter. Additionally, appreciation is extended to the Conference of Radiation Control Program Directors, Inc., for their contributions in reviewing the nuclear and radiological chapter.

Ann M. Beauchesne, program director for homeland security in the Center for Best Practices, directed the production and coauthored the report, along with coauthors Kevin Shanley, Chris McIlroy, and Erin Lee.

Preface

The September 11, 2001, terrorist attacks against the World Trade Center and the Pentagon quickly propelled terrorism to the top of the nation's agenda. Even before the events of September 11, governors had identified terrorism as a domestic security concern and, since 1996, the issue has been part of the National Governors Association's efforts in emergency preparedness. However, the magnitude and nature of the September 11 terrorist attacks, the subsequent anthrax releases, and ongoing national alerts have led governors to initiate unprecedented efforts to develop comprehensive state plans to prevent, respond to, and recover from terrorist attacks.

Homeland security is a complex challenge that demands significant investment; collaboration among local, state, and federal governments; and integration with the private sector. The purpose of *A Governor's Guide to Emergency Management Volume Two: Homeland Security* is to provide governors and their staff with policies, procedures, and general information regarding homeland security. It is not intended to be an all-encompassing document regarding various directives and information about homeland security; rather, it should be used as a reference document that addresses the major issues a governor and his or her staff need to know and prepare for.

NGA often addresses homeland security and emergency management at the governors' meetings and during seminars for chiefs of staff, policy advisors, and press secretaries. During these sessions, governors and staff who have handled emergencies describe their experiences and mistakes and candidly explain how they could have done things differently. NGA will continue to make homeland security and emergency management a key part of its services to the nation's governors.

Overview of the Guide

With lives, infrastructure, and resources at stake, governors must become instant experts in homeland security when their states are affected by a terrorist incident. *A Governor's Guide to Emergency Management Volume Two: Homeland Security* addresses the major homeland security issues a governor and his or her staff need to understand and prepare for. Sources of more detailed information, such as Web sites and phone numbers, are listed throughout the document.

As with natural disasters, acts of terrorism demand that a new governor be ready to respond as soon as he or she assumes office. Before a terrorist attack occurs, a governor needs to designate a homeland security director; establish a homeland security team; compile essential emergency management information; and assess the state's resources and capabilities for dealing with a terrorist incident involving weapons of mass destruction. Chapter 1 outlines basic steps a governor—particularly a newly elected one—should take to be prepared for a terrorist attack even during the early days of his or her administration. It also describes the authority and powers a governor has during a terrorist attack and outlines the interaction needed among the governor's office, the homeland security director, the state emergency management office, other state agencies, local governments, the private sector, volunteer organizations, and the federal government.

Homeland security presents a challenge to governors because of the need to educate the public without engendering unnecessary fear. Additionally, after an attack occurs, survivors, victims' families, and local citizens will look to the governor for leadership. Chapter 2 details important considerations in implementing an effective communications strategy for managing the public's emotions and expectations as well as ensuring that state government speaks with one voice.

In the response stages of a terrorist incident, the ability to save lives is directly proportional to the first responders' capability to communicate. Chapter 3 describes the challenges many states face as they develop state-of-the-art radio communications networks for emergency first responders, including law enforcement and fire personnel, emergency medical services (EMS) workers, and other public health professionals.

Immediately after September 11, governors throughout the country called upon state agency directors to identify vulnerabilities and enhance security in and around public buildings, dams, borders, water supplies, nuclear power plants, airports, education centers, and other critical infrastructures. Chapter 4 recommends that governors and state homeland security officials begin a comprehensive and proactive process to identify the state's critical infrastructures, assess their risk of and vulnerabilities to terrorist attack, and establish plans to protect the state's critical infrastructure.

To address a bioterrorist attack involving mass casualties, governors must make improving public heath and medical capabilities—and the ability to deploy these resources—exceedingly high priorities. The deliberate release of anthrax against civilians in October 2001 increased America's awareness and concern about bioterrorism and highlighted the responsibility of state and local health departments. Chapter 5 describes actions states should take to prepare for and respond to a bioterrorist attack, including improving the network of infectious disease surveillance, upgrading laboratory facilities, advancing diagnostic techniques, and expanding training of health-care personnel.

Chapter 6 describes the serious threat agroterrorism represents to human life, our economy, and the nation's food supply. The chapter lays out actions governors should consider in preparing to respond to the threat of agroterrorism, including incorporating agroterrorism response in state emergency plans; clarifying roles of actors in an agroterrorism response; removing redundancies and providing outlets for reporting outbreaks; establishing relationships with appropriate federal agencies, local authorities, producers, and veterinarians; and educating producers, veterinarians, and other members of the state agricultural network regarding reporting mechanisms, procedures, and state points-of-contact.

Chapter 7 highlights the potential that exists for terrorists to build chemical weapons. Additionally, chemical facilities located in high-population areas that use and store hazardous chemicals are attractive targets for terrorists. These facilities provide relatively easy access to chemicals at locations from which a significant intentional chemical release could harm large numbers of people.

Nuclear terrorism and radiological terrorism represent two of the most devastating and feared forms of terrorism that a governor will need to address. Should a detonation or the release of other radiological materials occur, the effects could be catastrophic in loss of human life and in the contamination of buildings, the environment, food, and water. Chapter 8 discusses the nature of the threats posed by nuclear and radiological terrorism (including fission devices, radiological dispersion devices, and nuclear reactors), preventive approaches to securing sources of radioactive materials, the nature of the response, and major federal assets available to governors in the event of an attack.

Today there is a heightened awareness of the potential for cyberterrorism to shut down public and private information systems, keeping them from performing essential functions, such as delivering electricity or water to homes and businesses. In the current environment, where many of these information systems are integrated and there is widespread use of the Internet and e-mail, there are many opportunities for cyberterrorists to disrupt our lives. Chapter 9 describes the robust cyberprotection, detection, warning, response, and recovery capabilities states must have to meet these potential threats.

Chapter 10 summarizes the federal government's response to a terrorist incident and outlines the Federal Response Plan as well as other available federal resources.

The Appendixes contain listings of sources for further information.

CHAPTER 1

The Basics: What Every Governor Should Know

As is expected during natural disasters, a new governor must be ready to respond to an act of terrorism as soon as he or she assumes office. This begins with establishing a homeland security team as soon as possible and ensuring that the team can effectively implement the emergency plans of the state should an incident occur.

To complete a homeland security infrastructure, new governors will need to oversee the development of new domestic security plans, make decisions on the investments of new federal and state dollars to improve public health and first responder capabilities, and coordinate the functions of numerous state agencies and resources. For this reason, a new governor immediately upon assuming office should:

- ★ establish a state homeland security structure;
- ★ review state homeland security plans;
- ★ review the role of the National Guard in response plans;
- ★ review the governor's emergency powers;
- ★ review, revise, or establish a continuity of operations plan;
- ★ review or establish an alert system; and
- ★ review long-term state homeland security plans and goals.

In preparing to assume office, new governors and their senior staff also should consult volume one of this series (*A Governor's Guide to Emergency Management, Volume One: Natural Disasters*), which describes the basic elements of emergency management.

ESTABLISH A STATE HOMELAND SECURITY STRUCTURE

One of the first acts of a new governor should be to establish a homeland security structure. In the absence of a crisis, governors should rely on these homeland security officials to make informed, coordinated decisions on all emergency and preparedness planning and investments. During a crisis, governors should rely on their homeland security and emergency management officials to solve problems concerning response and recovery.

The homeland security structure should be composed of the governor's chief of staff or governor's other senior staff and leadership from key state functions or agencies, including the National Guard, law enforcement, emergency management, public health, fire and rescue, transportation, agriculture, environment, public administration (facilities management), and information technology. In addition, it may be helpful to include a state budget officer to advise the team on funding matters. Finally, each team member should identify and maintain federal points of contact for assistance in such key issues as intelligence sharing, availability of federal assets, and the federal disaster funding process.

Indiana Counter-Terrorism and Security Council (C-TASC)

★ **Mission**

Develop and implement a comprehensive state strategy to address terrorism and serve as Indiana's liaison to the federal Office of Homeland Security.

★ **Functions**

- Determine the state strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats or attacks.
- Periodically review and coordinate strategy revisions.
- Serve as a central contact point for information regarding terrorist threats or activities within the state.
- Ensure, to the extent permitted by law, all appropriate and necessary intelligence and enforcement information relating to Indiana security is disseminated to and exchanged by appropriate departments and agencies responsible for security.

★ **Members**

Lieutenant Governor, C-TASC Director, Indiana House Speaker, Indiana Senate President Pro Tempore, State Police Superintendent, Adjutant General, State Health Commissioner, Executive Director of the Indiana Criminal Justice Institute, State Transportation Commissioner, Assistant Commissioner of Agriculture, Executive Director of the State Emergency Management Agency, State Fire Marshal, Utility Regulatory Commission Chair, FBI Special Agent in Charge, Grant County Sheriff, and the U.S. Attorney for the Southern District of Indiana.

Governors also should review the role of their state homeland security director and determine whether they are satisfied with the authority provided to that position and its relationship to emergency management, law enforcement, National Guard, and public health functions of the state. Since September 11, every governor designated an individual to serve as their state homeland security director. In a number of states, the homeland security director serves as an advisor to the governor and overall coordinator of emergency management, law enforcement, and related functions. In more hierarchical structures, the state homeland security director oversees some or all of these same agencies.

It is not clear what structure serves governors best. In all likelihood, a homeland security director's effectiveness is determined by his or her relationship with the governor rather than by formal authority. However, in choosing a director of homeland security, governors should consider the following.

- ★ During the next several years, significant new federal dollars may be available to the states to upgrade communications, public health infrastructure, and first responder capabilities. A homeland security director can serve as the focal point for all federal funding related to state homeland security. In this role, homeland security directors would oversee the process of obtaining and allocating federal homeland security funds for all state agencies. They also would coordinate investment decisions among agencies and across levels of government to avoid conflicts, redundancies, and misallocation of resources.

- ★ A homeland security director can fulfill the important function of coordinating plans, resources, and response activities among agencies and different levels of government.

- ★ Finally, a homeland security director can serve as a key point of contact for operational decisions during an emergency.

Most governors have chosen homeland security directors who are familiar with—if not proficient in—military, law enforcement, emergency management, or emergency response disciplines. In fact, most directors have come from the agencies that carry out these functions. In addition to this valuable experience, a homeland security director's job involves equal parts planning, coordinating, investing for the future, and responding to the present. For these reasons, a homeland security director should have strong managerial skills and be able to direct a multidisciplinary team, coordinate budgets, make sound investment decisions, and facilitate group discussion to solve problems. In short, the position requires a strategist more than a tactician.

REVIEW STATE HOMELAND SECURITY PLANS

State emergency management plans are essential blueprints that identify and assess state hazards and vulnerabilities, assign lead state agencies by function, and clarify these agencies' primary responsibilities. Most states have built upon their basic, all-hazard emergency management plans to develop terrorism-specific documents that fully describe potential biological, chemical, nuclear, and radioactive threats and how the state should prepare for, respond to, recover from, and mitigate such incidents. Some states have posted their terrorism plans on the Web sites (see box, "State and Federal Emergency Plans"). Governors should review their state's emergency management plans during transition or shortly after taking office to determine whether the state has fully assessed and addressed the threat of terrorism.

Generally, a state homeland security plan should:

- ★ describe state agency operations and responsibilities to prepare for, respond to, and recover from a threat or act of terrorism;
- ★ identify a chain of command for operational decisions during an emergency involving a threat or act of terrorism, including the roles of the governor and of the homeland security director;
- ★ describe a communications plan for vital public information on evacuations and other related alerts;
- ★ identify lead state and federal support agencies by function, such as public health, public safety, and critical infrastructure protection;
- ★ describe continuity of operations provisions that establish how all levels of state government will function under disaster conditions caused by an act of terrorism;
- ★ identify agencies responsible for collecting, interpreting, and disseminating information and intelligence to decisionmakers;
- ★ describe the process, responsibility, and methodology for assessing damage and for providing assistance;
- ★ describe the process for declaring a disaster and for requesting federal and other external assistance;
- ★ describe the process for maintaining records that detail the state's response and recovery actions in assets and related costs; and
- ★ enumerate the governor's powers and authorities that may be exercised during a terrorism incident.

State emergency management plans are discussed in greater detail in the *Governor's Guide to Emergency Management, Volume One*.

FOR MORE INFORMATION: State and Federal Emergency Management Plans

Arizona:	**www.dem.state.az.us/serrp**
California:	**www.oes.ca.gov**
Florida:	**www.dca.state.fl.us/bpr/Preparedness**
Indiana:	**www.in.gov/sema/ema/cemp.html**
Missouri:	**www.sema.state.mo.us/seoppage.htm**
North Carolina:	**www.dem.dcc.state.nc.us/NCEOP/NCEOP2001.pdf**
Federal Contingency Plan (CONPLAN):	**www.fema.gov/pdf/rrr/conplan/conplan.pdf**

REVIEW THE ROLE OF THE NATIONAL GUARD IN RESPONSE PLANS

In reviewing homeland security procedures, a governor should integrate the National Guard into the overall emergency response structure. The National Guard is one of the most effective resources to address new threats of biological, chemical, and nuclear terrorism. In some states, the Guard may be the only entity with the ability to assess, respond to, or even prevent a major terrorism threat.

Throughout its history, the National Guard has participated in domestic disaster responses and recovery operations. In recent years, this mission has been called Military Assistance to Civil Authorities (MACA). Because of its preparation for the full spectrum of federal missions and its organization, the National Guard, while performing with either state or federal status, is prepared to accomplish many homeland security roles. Many states' Guard forces include infantry, aviation, engineer, and a variety of service support units.

With homeland security, the National Guard can assist governors in several ways. For instance, in some states, the National Guard is responsible for receiving, breaking down, and distributing the Centers for Disease Control and Prevention (CDC) Pharmaceutical Push Packages and for securing and deploying other critical prepositioned emergency response equipment. In other states, the National Guard has been vital in protecting airports, seaports, and other key components of critical infrastructure. For example, Washington State has effectively utilized the National Guard in a number of areas, including border patrol assistance, U.S. Customs, and Immigration and Naturalization Service (INS) operations. Governors should be aware that when the National Guard is deployed under state activation, the costs are borne by the state and can be expensive.

Civil Support Teams

Thirty-two states currently have a federally supported National Guard Civil Support Team (CST) capable of operating in a contaminated zone and of conducting an immediate on-site assessment of hundreds of chemical, biological, radiological, and nuclear threat agents. The CST can assess a suspected weapons of mass destruction (WMD) event in support of the local responders; advise civilian responders regarding appropriate emergency actions to take; and work both to facilitate and to expedite the arrival of additional military forces if needed. The unit is supplied, trained, and equipped by the federal government. It is manned by National Guard soldiers. Under a governor's directive, the state adjutant general deploys the CST to support the state response.

CSTs provide life-saving situational awareness and technical assistance to first responders who might otherwise be among the legions of casualties when arriving at the site of a terrorist attack. Every state, territory, and the District of Columbia should seek federal designation of a National Guard CST to safeguard its citizens and emergency responders.

As homeland security evolves and matures, there undoubtedly will be new and unanticipated homeland security roles for the National Guard in addition to its vitally important combat role. For homeland security purposes, the National Guard is America's forward deployed military force.

REVIEW THE GOVERNOR'S EMERGENCY POWERS

State emergency management statutes dictate the conditions that trigger emergency powers and specify the roles and responsibilities of the governor during disasters and emergencies. As the state's chief executive, a governor typically has the authority to declare a state of emergency, request or require the evacuation of citizens, direct and allocate state resources, and request federal assistance when state resources have been exhausted or when conditions warrant it. Governors and their chief advisors (i.e., chief of staff, homeland security director, and homeland security team) must know when and under what specific circumstances the emergency powers take effect and terminate.

Among the key powers a governor and state homeland security officials should review are:

- ★ powers to declare a state of emergency, order evacuations, and quarantine affected populations;
- ★ authority to issue drugs and require vaccinations or request voluntary vaccinations;
- ★ authority to suspend certain regulations, issue price controls on critical items (such as gasoline and water), and declare martial law; and
- ★ ability and authority to use public airwaves for emergency announcements.

FOR MORE INFORMATION on the Governor's Emergency Powers Statutes

Maine: **www.janus.state.me.us/legis/statutes/37-B/title37-Bsec741.html**

Missouri: **www.moga.state.mo.us/statutes/c000-099/0440100.html**

The checklist on the next page provides additional information on powers to review. If existing statutes do not adequately establish the necessary powers of a governor during a disaster as described in the checklist, it may be necessary to request that legislation be amended. A governor and state homeland security officials should review the emergency power statutes within the first 60 days of office and request necessary legislation changes as soon as possible. Typically, state statutes provide the majority of powers needed under a declared emergency, but they may not include the powers needed to protect the public in the event of a disease outbreak or other health threat. Because many states have not changed their public health laws for decades, these laws should be reviewed carefully to determine if changes may be needed to respond to threats of bioterrorism.

CHECKLIST: A GOVERNOR'S EMERGENCY POWERS

- ✔ Issue orders, proclamations, and regulations as required, including evacuation orders, quarantine of affected populations, reentry of evacuated populations, and establishment of recovery centers.
- ✔ Declare a disaster if one has occurred or is imminent or threatened, thereby providing the basis for future federal assistance.
- ✔ Determine the duration of all orders, proclamations, and regulations.
- ✔ Promptly disseminate declaration information to the general public.
- ✔ Identify routes, modes of transportation, and destinations in association with an evacuation.
- ✔ Restrict/control entrances and exits from disaster areas and the movement and occupancy of people in those areas.
- ✔ Suspend any regulatory statutes prescribing procedures for the operation of state business or state agency orders and regulations.
- ✔ Deploy all available resources of the state government and of each political subdivision as is reasonably necessary to cope with the disaster.
- ✔ Suspend or limit the sale, dispensing, or transportation of alcoholic beverages, firearms, explosives, and combustibles.
- ✔ Terminate declarations when appropriate.

In addition to reviewing executive powers, homeland security officials should consider entering into mutual aid agreements with adjoining states and participating in the Emergency Management Assistance Compact (EMAC). Nearly every state has established an agreement with neighboring states and regions that enable all parties to the agreements to mutually benefit from shared assets during a disaster as well as to participate in regional training and exercises.

REVIEW, REVISE, OR ESTABLISH A CONTINUITY OF OPERATIONS PLAN

A continuity of operations plan (COOP) provides organizational stability and maintains minimal essential state government functions across a broad scope of potential emergencies. An effective COOP should outline official lines of succession, predelegation of authorities, procedures for safekeeping essential records, provisions for creating a secure operations center and alternate command sites, and measures for protecting government personnel and resources (see box, "Elements of an Effective COOP"). Specifically, a COOP should:

- ★ detail essential government functions and activities and list appropriate personnel;
- ★ identify mission-critical data and systems that support essential functions;
- ★ describe the decisionmaking process for implementing COOPs and procedures;
- ★ provide instructions for relocation to predesignated facilities with and without warning during duty and nonduty hours;
- ★ ensure operational capability within a specified amount of time (e.g., 30 days);
- ★ address the potential role of the National Guard if military forces are required to provide services normally under civilian authority;
- ★ provide interoperable communications; and
- ★ establish procedures to acquire resources necessary to continue essential government services for several days.

Additionally, executive office and state agency personnel should participate in COOP training exercises at an emergency operations center (EOC) and alternate sites for testing and validation purposes.

Lines of Succession and Delegation of Emergency Authority

Lines of succession typically are established by statute to ensure that civil political leadership will function and, if necessary, effectively transition under disaster conditions. A governor should review the state's COOP to ensure that this important element identifies individuals in state government who are authorized to act on his or her behalf when the governor is temporarily absent or otherwise unavailable. For example, most statutes establish lines of succession that pass authority from the governor to state officials in the following order: lieutenant governor, secretary of state, attorney general, treasurer/comptroller, general assembly/legislature (senate president, speaker of the house), judicial system, commissioner of agriculture, and adjutant general. The COOP should establish rules that address the specific conditions under which succession will occur as well as notification procedures.

As evidenced by the magnitude of the September 11 events, a disaster may be so catastrophic in scope that it requires a governor to delegate duties and responsibilities to individuals in descending order of authority within an agency. In addition, governors should require their state homeland security directors and agency heads with primary and support responsibilities in the state's emergency management plan to provide for delegation of emergency authorities. Finally, a governor should ensure that the COOP describes the delegation process, identifies the limits of authority, provides for accountability, and dictates the circumstances under which the authority is to be exercised.

Other Essential Elements of an Effective COOP

A governor and state homeland security officials should review the COOP shortly after the governor takes office to ensure that it provides procedures for the protection, duplication, and movement of physical and electronic records. These include operating records, such as orders of succession and delegations of authority, as well as legal and financial records.

Since activities at an EOC may be disrupted or, as at the World Trade Center, be totally destroyed, the COOP should identify secure alternate emergency operations facilities. The governor's state homeland security director and officials should adopt provisions that include sharing facilities with other jurisdictions through cooperative agreements or memoranda of understanding (MOU). In all cases, facilities should be selected on the basis of survivability, level of redundancy, and the ability of government to perform its essential functions during an emergency response period. Each essential state agency must be prepared to carry out its essential functions from remote locations.

Each state agency should develop and maintain standard operating procedures that will maintain an adequate communications capability and ensure the continuation of essential state government operations. These procedures, which should be published, distributed, and exercised in a training environment, include identification of emergency assignments, responsibilities, and duty stations; alerting or notification procedures; and other actions and measures to be taken as prescribed under various readiness levels.

ELEMENTS OF AN EFFECTIVE COOP

- ✔ List of essential functions
- ✔ Roster of personnel familiar with essential functions
- ✔ Procedures that provide reliable, effective, and timely notification by state emergency coordinators to persons designated in the state emergency plans, including those in the lines of succession
- ✔ Determination of who is responsible for direction and control activities at the executive level
- ✔ Rules of succession by office
- ✔ Determination of the extent and limits of authority of the senior elected and appointed officials and their effective and termination dates
- ✔ References to the state emergency management plan to determine the administrative and operational authorities of the emergency service agencies
- ✔ References to standard operating procedures for each state agency that provide specific authorities of designated successors to direct their agencies
- ✔ Location of the primary and alternate EOCs, mobile EOCs, and command posts
- ✔ Identification and location of individuals responsible for ensuring communications capabilities of the primary, alternate, and mobile EOC/command post, including dispatching capabilities, NAWAS (National Alert System) points, and telephone lines
- ✔ Identification of agencies and personnel (including lines of succession) responsible for providing water, electricity, natural gas, sewer, and sanitation services to affected areas
- ✔ Identification and location of alternate methods of communication, including satellite phones and amateur radios
- ✔ Identification of operational warning devices (sirens, weather radio/tone-alerts, cable screen-crawl, etc.) and the individuals responsible for activation
- ✔ Procedures for the acquisition of resources necessary to sustain operations over a predetermined period of time
- ✔ Protection of all vital records
- ✔ Location of EMAC, MOU, and cooperative agreements and their contact points
- ✔ Procedures for ensuring security, including employee security clearances, facility security, and communications security
- ✔ Procedures for collecting/exchanging information among state, local, and federal response organizations
- ✔ Procedures to ensure that public information officials (PIOs) coordinate all emergency public information with the governor's office and other agencies
- ✔ Identification of special communications needs (i.e., various languages in population)
- ✔ Procedures for state officials to provide a consistent message when dealing with the media and the public
- ✔ Identification of interoperable communications to support essential functions

SECURITY AT STATE CAPITOLS AND OTHER ESSENTIAL GOVERNMENT BUILDINGS

As part of a review of the COOP procedures, governors should review security plans for the state capitol and other essential government buildings. Most governors immediately enhanced physical security plans and procedures for state buildings in response to the events of September 11. At that time, governors ordered the implementation of basic, short-term, yet effective security measures including:

- ★ deployment of additional security personnel;
- ★ employee identification badges;
- ★ metal detectors;
- ★ barricades; and
- ★ modified traffic patterns.

Although efforts focused on capitol buildings, governors also enhanced security to a lesser extent at other facilities that house essential state functions.

Governors and state homeland security officials should assess existing physical conditions and cybersecurity conditions at essential state buildings shortly after taking office and implement new or enhanced procedures as required. However, some citizens and the media have questioned whether installing barricades and deploying armed guards is an overreaction to the terrorism threat and jeopardize public access to government. Governors should address this issue by assessing the risks to and vulnerabilities associated with essential state buildings and communicating the reasons behind their choice of security measures.

Finally, a state emergency plan must establish clear procedures and responsibilities for evacuating public buildings. In the wake of September 11, many states discovered that different buildings were controlled by different state agencies and branches of government during an evacuation and that evacuation orders were inconsistent. Evacuation procedures should be coordinated and practiced, and communication plans should be developed to inform employees on the status of an emergency and what they should do during and after an evacuation.

FOR MORE INFORMATION

Crime Prevention through Environmental Design: **www.ncpc.org/3cpted.htm**

General Services Administration (GSA) Publication: *Making Federal Buildings Safe*. Available at: **www.gsa.gov/Portal/content/pubs_content.jsp?contentOID=119420&contentType=1008&P=1&5=1**

GSA Facilities Standards for Public Building Services: **hydra.gsa.gov/pbs/pc/facilitiesstandards**

National Capital Planning Commission: **www.ncpc.gov**

The American Institute of Architects: **www.aia.org/security**

REVIEW OR ESTABLISH AN ALERT SYSTEM

In 2002, the federal Office of Homeland Security (OHS) developed a color-coded national warning system to notify the public and officials of credible terrorist threats. Although states are not required to adopt this system, governors and homeland security teams may consider implementing a warning system that is modeled on the federal system or that complements an existing state or local all-hazards readiness system the public is familiar with. In all cases, the governor and the homeland security team must ensure that public outreach is conducted so citizens know the conditions under which the warning system will be activated and what they are expected to do during a given threat level.

Federal Alert Warning System

Red
(Highest)
A severe risk of attack that might require special positioning of specialty teams, closing public and government facilities, and monitoring transportation systems.

Orange
(High)
Signifies a high risk of attack requiring the government to coordinate necessary security efforts with the National Guard or law enforcement agencies and take additional precautionary measures at public events.

Yellow
(Significant)
An elevated risk condition means there is a significant risk of attack that may require increased surveillance of critical locations and implementation of emergency response procedures.

Blue
(Guarded)
A general risk level means agencies may be asked to review and update emergency response procedures.

Green
A low risk of attack.

REVIEW LONG-TERM HOMELAND SECURITY PLANS AND GOALS

As with any emergency, new measures are created and plans are revised to address the changing severity and threat of potential incidents. Now that governors across the country have successfully enacted plans and programs based upon the immediate threats of September 11 and fiscal resources currently available, governors and state homeland security officials must focus on long-term planning. Major federal homeland security funding will be available to states in the future, enabling governors to think beyond the terrorist attacks of September 11 and develop multiyear homeland security strategies and programs to further strengthen and protect public health and critical infrastructure (see box, "Long-Term Homeland Security Strategy Checklist").

LONG-TERM HOMELAND SECURITY STRATEGY CHECKLIST

- ✔ Determine whether the existing state homeland security team and membership is viable and effective and, if necessary, initiate adjustments.
- ✔ Expand the identification, assessment, and monitoring of existing and new public health, public safety, and critical infrastructure risks associated with emerging threats.
- ✔ Seek to build upon existing partnerships by identifying and including additional representatives from state, local, and federal agencies and from private industry.
- ✔ Strengthen state terrorism plans by clarifying personnel duties and responsibilities and ensure that training exercises are conducted regularly for public and private-sector personnel in high turnover positions.
- ✔ Identify and strengthen inadequate capabilities, including hospital capacity and first responder equipment, personnel, and training.
- ✔ Seek, identify, and obtain available homeland security funding to strengthen existing and future state homeland security programs and critical infrastructures.
- ✔ Actively partner with the public and private sectors to improve communication that will enable first responders from different public safety agencies to communicate with each other at multijurisdictional incidents.

CHAPTER 2

Crisis Communication

Homeland security presents a challenge to governors and other political leaders because of the need to educate the public concerning the potential threat of terrorism without arousing too much attention and engendering unnecessary fear. Domestic preparedness is subject to swings in public and media attention, so governors face the additional challenge of balancing and sustaining public awareness of homeland security over the long term as other issues and crises arise.

Media coverage of disasters has increased public expectations for government response. The press is eager to report what the government is doing—or is not doing—to deal with an emergency or incident. Terrorist attacks will provide the opportunity for dramatic live coverage by the media and evoke strong emotions from the public. A governor should have a strategy in place for managing the public's emotions and expectations. State government must speak with one voice and the governor ultimately is in charge of the message. If an incident occurs, a governor should provide public assurance that:

- ★ the seriousness of the situation is recognized;
- ★ someone is in charge; and
- ★ all reasonable steps are being taken.

Consequently, to be effective at crisis communications, a governor should:

- ★ develop a communications strategy;
- ★ prepare to answer questions from the public;
- ★ develop effective media relations;
- ★ define the role of the governor and key aides; and
- ★ establish a joint information center.

DEVELOP A COMMUNICATIONS STRATEGY

A communications strategy is an important component of state emergency management and should be developed well before the state is faced with a crisis. Concerned citizens turn to the media for information, reassurance, and critical advice. Without adequate preparation and coordination by the governor's chief of staff, press secretary, and agency public information officers, rumor may be taken as truth and facts may be misrepresented, resulting in distorted public perception of an incident.

If an emergency arises, a good communication strategy will prepare a governor to:

- ★ make a quick, initial statement;
- ★ clearly establish who speaks about what and when;
- ★ establish a regular schedule of statements;
- ★ monitor the media closely;
- ★ correct erroneous reports; and
- ★ prepare for "Who's to blame?" questions.

A major terrorist incident will present difficult challenges not covered by normal policies and procedures. Information will need to be shared quickly and a coordinated, unified image of control presented. Governors' staffs should identify the challenges they expect to encounter when a credible threat has been identified and, prior to a crisis, practice several steps (see box, "Checklist for a Communications Strategy").

CHECKLIST FOR A COMMUNICATIONS STRATEGY

- ✔ Identify tough questions to gauge the appropriate level of response.
- ✔ List five action steps to take in the most likely emergencies and evaluate them.
- ✔ List appropriate contact names for help (in order of importance and immediacy).
- ✔ List media partners and their role in communicating the state's message.
- ✔ List community or private-sector partners and how they can assist.
- ✔ Develop daily key messages to communicate to staff, the public, and the media.
- ✔ Identify media implications of event.
- ✔ Adapt a crisis plan for the specific situation to provide appropriate action to support.
- ✔ Develop background information and risk communication strategies on threat agents and related illnesses for the general public.
- ✔ Work with media on a regular basis to increase public awareness of terrorist risks, personal protective measures, and community response procedures.

PREPARE TO ANSWER QUESTIONS FROM THE PUBLIC

Lack of timely and accurate information raises the anxiety level of the public. It also feeds inaccurate impressions of an event and can exaggerate or underestimate the potential harm. If a terrorist attack occurred, the public would likely want answers to the following questions about magnitude, immediacy, duration, and control.

Magnitude:

- ★ How big is the risk area—have I been or will I be attacked?
- ★ How many people have been/will be affected?
- ★ How much damage has occurred or could occur?

Immediacy:

- ★ Am I already affected?
- ★ How soon will I be affected?
- ★ How soon will something be done about it?

Duration:

- ★ How long will it last?
- ★ When can people go back home?
- ★ When will things be back to normal?
- ★ Will it happen again?

Control:

- ★ Who is in charge?
- ★ Is the situation under control?
- ★ Can the situation be corrected?

DEVELOP EFFECTIVE MEDIA RELATIONS

Though the media can be a hindrance, it can also be a helpful conduit by getting the word out quickly and providing valuable information during an incident. The First Amendment is clear that the media should and will play an important role in our society, but during a terrorist incident that role can be complex. Some fear that the media will act irresponsibly and cause mass panic and there is some basis for concern. When the media speaks too quickly or draws their own conclusions from incomplete information and presents them as fact, they can create mistrust and cause panic and fear. However, fostering a good relationship with the media can help ensure they do their job well.

The media can play a central role in assisting local, state, and federal government prior to a terrorist attack by disseminating information about preparedness and response ahead of time. Governors' staff should build relationships with members of the media and encourage ongoing positive and constructive news coverage. While they may not be able to control the media, they can control the message—and that message is very important. The public's perceptions, attitudes, opinions, and values are shaped by what it reads, sees, and hears. The information it is given will determine how it thinks and feels about a particular incident. Therefore, governors can use their extraordinary media access to get the word out to the public through scheduled press briefings, televised appearances, and radio announcements.

The media is after news and will go wherever there is a story. Media representatives seek information that is timely and factual, and they will talk to anyone who can provide information. For that reason, the governor should ensure that communication lines with the press are open and that questions receive prompt responses to ensure that false rumors are quelled before they spread.

It is equally important for a governor or his or her representatives to communicate personally with the victims and victims' families. If victims do not know where to turn for help, they become frustrated. Telling people specifically where to get help is among the most important types of information a governor can provide.

The governor should meet with the management of the region's major print media outlets and enlist their commitment as a public service to become part of the communications "team" in the event of a disaster. The governor also should meet with the top executives or station managers of local television and radio stations and include them on the state's emergency response team. The governor's communications strategy should describe the role of each media sector—print, television, and radio—in helping communicate emergencies and response. Establishing these expectations among all parties before an emergency occurs can prevent a "race for news" situation during an event, when inaccuracies often occur.

A good communications strategy allows reporters to continue to dig for news but ensures that critical safety information is reported in the same way among all local media. Should an incident occur, the governor's office should meet immediately with the key media managers and implement a day-by-day strategy to get information out to the public.

A bioterrorism attack presents a unique communication challenge. It involves the unknown, and people will react differently to it than they would to the kinds or emergencies they have come to know—hurricanes, tornadoes, fires, and even bombings. Consequently, during a bioterrorism incident, the media will be perhaps the most crucial conduit for important announcements, including information about where and when vaccinations are available and where the public should go for medical care.

Governors can use the media to calm an anxious public with facts about the biological agent involved, its treatment, its communicability, and other important medical facts. However, to ensure that the media has the correct information and is not putting out false information to the public, media representatives should be involved in the planning process and educated about the challenges all levels of government face during a bioterrorist event. A state's homeland security office should conduct periodic briefings with the media on the state's bioterrorism response plan to educate them before an emergency occurs. Reporters need to understand the basic elements of a state's response actions to minimize the misinformation getting out. How media handles information in the early phases of an incident sets the tone for the duration of the crisis (see box, "Timeline for Communicating with the Media").

TIMELINE FOR COMMUNICATING WITH THE MEDIA

10–12 Hours after a Crisis:

- ✔ Offer what you know—don't speculate.
- ✔ Initial statement: location, type of incident, when it happened, why (if known), who is involved or affected, and what is being done to rectify the situation.
- ✔ Designate a media setup area—a "one-stop shop" for information.
- ✔ Do not say "no comment"—instead, say "we will be issuing a statement shortly" or "we are investigating the situation and doing everything possible to ensure the safety of those involved."

12–24 Hours after a Crisis:

- ✔ Develop a media briefing schedule.
- ✔ Leave time for questions—don't react to the media, use your messages.

24–36 Hours after a Crisis:

- ✔ Don't forget local media.
- ✔ Get bad news out yourself, focus on the positive.

DEFINING THE ROLE OF THE GOVERNOR AND KEY AIDES

State homeland security is a shared responsibility that involves several agencies, so teamwork is critical. The governor and his or her key aides (chief of staff, homeland security director, and press secretary) form the core executive management team for any state emergency. For this reason, each team member must establish and clearly understand the role he or she will play during an emergency. Moreover, the team must have a clear understanding about how decisions are made as well as how information is communicated to the media and the public and by whom.

Interaction among the governor's office, the state emergency management office, the state legislature, other state agencies, local governments, the private sector, volunteer organizations, and the federal government is the foundation for effective emergency management.

Resources of the entire state emergency organization should be tapped to ensure that an interagency perspective and approach is established early. Recent disaster experience has shown that disaster preparedness and response can be enhanced through close coordination with the private sector, so tapping into critical private-sector resources should also be considered.

Role of the Governor

Disasters evoke powerful emotions, and the governor's presence and leadership can go a long way toward calming and reassuring the community. Survivors, victims' families, and local citizens will look to the governor for leadership. The governor should be involved and visible. Nothing can erode public confidence more quickly than the impression that the governor is inattentive or slow to respond during an emergency.

As the state's chief executive, the governor is responsible for the safety and welfare of the people of his or her state. Governors can use the media to calm an anxious public with facts about the attack; whether a biological, chemical, or radiological agent is involved and its treatment and communicability; and other important medical facts.

When an act of terrorism occurs, a governor should resist the temptation to speed to the scene; rather the decision to go should be made only after careful consultation among the governor's emergency management team. Depending on the circumstances, governors may decide to avoid the emergency area when their presence could interfere with rescue efforts or attract unwanted attention, possibly slowing assistance to victims. For example, Oklahoma Governor Frank Keating decided not to go immediately to the site of the Oklahoma City bombing disaster. Instead, he stayed away as much as possible to avoid impeding the rescuers and politicizing the disaster. He directed much of his communication and aid to surviving family members and to caregivers who were helping victims.

A governor's presence can be reassuring, but it can also set unrealistic expectations that government programs or assistance may be forthcoming when, in fact, they may not be. The most important role for the governor is to set realistic expectations for terrorism victims and to provide comfort by words and actions. A governor who rushes to the disaster scene and hastily proposes specific response and recovery measures is more likely to set improbable and unachievable expectations among victims. In such instances, no promises are forgotten and public confidence can be damaged long after the actual event.

First Day. During the first day of an emergency, the governor should make an announcement, either in person or through a press release, that information is being collected and that the state is working with the affected local governments. The announcement should indicate that the governor is in charge of the situation, there is a unified plan in action, and information on further developments will be forthcoming. Compiling and disseminating consistent, accurate information can be an enormous challenge. The governor should not provide a detailed assessment until adequate data have been collected to avoid communicating misleading or incomplete information.

Second Day. After the first day, a governor's representative should be ready to describe the extent of damage as well as response and recovery operations. If possible, the second-day announcement should be made from the disaster site. The governor's representative should not make specific promises for recovery assistance. Statements should be framed carefully to indicate that state and federal aid, if appropriate, will be available to those who qualify. The governor's press secretary may wish to coordinate messages regarding federal aid with the Federal Emergency Management Agency's (FEMA's) regional office to ensure accurate release of information.

Third Day and Thereafter. The governor's involvement and presence should not end suddenly with his or her return to the capital. People affected by the terrorist incident need to know the attack is still a top priority and that the governor is doing everything possible to provide assistance. A daily press release should indicate that on-site personnel are keeping the governor apprised of the situation. These releases should be coordinated with the state emergency management agency's press officer so all offices will be speaking with one voice.

Governors and their staff should remember, however, that every a terrorist incident is unique. It is important for the governor to be flexible and determine what action to take on a case-by-case basis rather than strictly adhere to a prescribed response approach.

The state homeland security director should continually brief the governor on state response and recovery efforts. Long after the incident occurs, assistance will be a key concern of the media from the affected area. The governor also will be questioned about the status of federal law enforcement, criminal justice, and recovery efforts. However, a governor should avoid answering questions about specific cases and instead reinforce the federal, state, and local response partnership when communicating with the victims.

Role of the Homeland Security Director

Since September 11, 2001, most governors have designated a state homeland security director to prepare for and manage their states' response to terrorism. Their role is to coordinate with state department heads and the federal government prior to and during a terrorist incident. The governor's homeland security director also should oversee all operational decisions that are consistent with a general plan agreed to by the governor's core emergency management team.

State homeland security directors should facilitate communication and cooperation among local, state, and federal authorities and coordinate security responsibilities should a terrorist attack occur. They should communicate technical information to the public but not fill the role of the governor as overall communicator of impact, comfort, and response.

Role of the Chief of Staff

Historically, the chief of staff has been the principal contact in the governor's office for emergency management. However, with the advent of the state homeland security director position, this has come to be a shared responsibility or delegated entirely to the governor's homeland security director. However, throughout the crisis, the chief of staff should coordinate the actions of the governor's office and interact with the state's homeland security director, emergency management director, and other agencies. The chief also may work closely with the state's homeland security director to coordinate with federal, state, and local government officials and the business community.

Role of the Press Secretary

Press secretaries in governors' offices spend most of their time accentuating the positive and ensuring that reporters see the best in state government. When terrorists strike, many are stunned and caught unprepared for the challenges of communicating with the media. Press secretaries should take time to read the state's emergency plan, learn the established procedures, and be familiar with the roles assigned to state officials in responding to disasters.

During an emergency, the governor's press secretary should maintain critical lines of communication among the governor's office and emergency personnel, victims, the press, state and local officials, and the federal government. Victims, legislators, congressional delegations, federal agencies, political opponents, and the general citizenry all want current information. Press secretaries have the enormous challenge of compiling information and preparing general statements that address the needs of a wide-ranging audience. There are several things a press secretary should do before a disaster strikes (see box, "Checklist for Press Secretaries: Before the Crisis").

CHECKLIST FOR PRESS SECRETARIES: BEFORE THE CRISIS

- ✔ Read the state emergency management plan.
- ✔ Sit down with homeland security directors and other emergency management officials, learn their roles, and designate a contact person in each organization.
- ✔ Meet with the state emergency management office's public information officer (PIO) and other key state personnel involved in communications to establish a relationship and protocol for information release.
- ✔ Promote a system to collect disaster relief supplies and donations of goods and services and determine a procedure for getting this assistance to victims.
- ✔ Respect state-local relationships and authorities. The state should be wary of stepping on important relationships and taking over existing systems.
- ✔ Establish a system for collecting information and delegate staff to help compile a "situation report" that details casualties, economic impacts, weather predictions, and other pertinent information.
- ✔ Develop a system for disseminating information to agency PIOs and the press. Clarify that the governor's office must approve all communications from the field.
- ✔ Understand federal disaster aid programs—including their purposes and limitations—and manage the dissemination of information so that public expectations are realistic when the governor asks the President to declare a disaster.
- ✔ Ensure that members of the governor's staff have two-way pagers. When telephone lines are down and cell phones become jammed, alternate communication links are critical.
- ✔ Understand the roles of the Red Cross, Salvation Army, and other emergency assistance groups and identify an appropriate governor's staff liaison to those organizations.
- ✔ Understand the best practices and lessons learned by the state, so communications can reinforce the steps the governor and state have taken to prevent the impact of disasters and mitigate the risks to citizens, communities, and the economy.

A consistent flow of accurate information is crucial during a terrorist incident. It is not enough to swiftly and effectively respond to a crisis; the public must be fully informed of the governor's actions. Establishing a media center for the press to obtain information, hold news conferences, and post reports is helpful. Local media representatives have special needs and press secretaries should ensure they get the access they need and are not boxed out by the national press. To enhance media coordination, press secretaries should:

- ★ remember the governor is at the top of the information flow;
- ★ establish a steady flow of information, a consistent spokesperson for general media information, and a schedule for general media updates;
- ★ identify who is responsible for speaking to the press on what issues;
- ★ ensure that disseminated information is accurate and describes how local, state, federal, and nongovernment partners are working together;
- ★ establish a media center to coordinate media access to the disaster site and to help provide reporters with phones, fax machines, and copiers to help them file stories;
- ★ use the state Web page to disseminate information;
- ★ have someone from the governor's office, the state's homeland security office, or emergency management agency available at all times;
- ★ ensure the governor's staff answering the telephones are fully informed and can refer citizens to appropriate help; and
- ★ avoid catering only to the national media and maintain relationships with local media, which is generally the best source of information for local citizens.

ESTABLISH A JOINT INFORMATION CENTER

After the President has declared a disaster, a joint information center (JIC) should be established to disseminate information about all disaster response and recovery programs and long-term prevention and mitigation strategies. Public information officers representing all federal, state, and local agencies providing response or recovery services should be part of the JIC to ensure the government speaks with one voice. The state emergency management office's PIO plays an integral role in the JIC and is an invaluable resource to the governor's press secretary. Volunteer organizations also should be included in the JIC.

The objectives of a joint information center are to:

- ★ instill confidence within the affected community that the state is using all possible resources and is working with federal, state, local, and nongovernment organizations to restore essential services and help victims begin to put their lives back together;
- ★ promote a positive understanding of response, recovery, and mitigation programs;
- ★ provide everyone with equal access to timely and accurate information about response, recovery, and mitigation programs; and
- ★ manage expectations so victims have a clear understanding of the response, recovery, and mitigation services available to them and the limitations of these services.

A state-federal JIC will provide media relations, Internet operations, and news analysis.

EXAMPLE OF A MEDIA RELEASE

FOR IMMEDIATE RELEASE

Contact: Name, phone number

Date:

Headline: Primary Message to the Public

We have been notified that **(insert brief description of incident)** and have taken steps to **(insert actions being taken)**. We are working to gather all the facts. Our first concerns are for **(insert staff, clients, family, public, etc.)** and completing a thorough investigation. As soon as we have more comprehensive information, we will make another statement and respond to questions. We appreciate your patience and know that you share our concern to resolve this incident as quickly and effectively as possible.

TO SEE SAMPLE PRESS RELEASES

at the State of Missouri Emergency Management Agency Web site, go to:
www.sema.state.mo.us/empuin.htm

CHAPTER 3

Interoperability and Disaster Communications

In the response stages of a terrorist incident, the ability to save lives is directly proportional to the first responders' capability to communicate. Many states are now developing state-of-the-art radio communications networks for emergency first responders, including law enforcement and fire personnel, emergency medical services (EMS) workers, and other public health professionals. It is critical that this equipment support interoperability.

Interoperable equipment, procedures, and standards for emergency responders are key to improving the effectiveness of mutual aid agreements with other states and other jurisdictions. Responding agencies and jurisdictions must have equipment that is compatible with all other responders.

Governors and their state homeland security directors should:

- ★ develop a statewide vision for interoperable communications;
- ★ ensure adequate wireless spectrum to accommodate all users;
- ★ invest in new communications infrastructure;
- ★ develop standards for technology and equipment; and
- ★ partner with government and private industry.

DEFINING INTEROPERABILITY

Interoperability refers to the communications capability that enables public safety agencies—including law enforcement, fire, and emergency medical organizations—to talk with one another by radio on demand and in real time.

Although public safety agencies have used radio communications systems for many decades, most of these systems have been limited in reach and have only enabled communication within a particular group, agency, or jurisdiction. Public safety radio systems operate in different frequency bands, much like AM and FM bands on standard radios. Just as AM radios cannot receive transmissions from FM radio stations, public safety radios in one frequency band cannot receive transmissions from another channel. As a result, when public safety agencies from different or multiple jurisdictions respond to incidents, they may not be able to talk with each other on their assigned radios due to incompatible equipment.

How Interoperability Impacts Public Safety

Interoperability can impact the ability of public safety agencies to provide a rapid and coordinated response. This can mean the difference between life and death. Most first responders rely on communications systems that have not kept pace with emerging threats or operational requirements. Moreover, existing communications systems must support an expanding set of missions, including responses to domestic terrorism, that require coordinated participation from state, local and federal agencies. For example, police officers from one agency can talk to each other over their assigned channels, but may not be able to communicate with paramedics or firefighters from the same jurisdiction. Likewise, first responders from one agency may be unable to communicate with their counterparts from neighboring jurisdictions who have responded to the same disaster.

What States Must Do to Improve Interoperability

State officials have a vested interest in establishing and protecting statewide wireless infrastructure because public safety communications often cross jurisdictional boundaries. Efforts to achieve public safety interoperability will require states to resolve several key issues, including spectrum, funding, coordination and partnerships, and standards and technology.

DEVELOP A STATEWIDE VISION FOR INTEROPERABLE COMMUNICATIONS

Governors should develop a well-planned, coordinated statewide vision to promote interoperability through new spectrum and revision of existing resources. This vision can help create a public safety communications infrastructure that provides consistent, quality service throughout a state. A governor should encourage change through the implementation of systemic improvements that will allow governments at all levels to realize efficiencies in spectrum allocation, funding, and shared use of common infrastructure components. State leadership is essential to the development of a common approach to regional and statewide interoperability.

Many states are establishing a foundation for cooperation and statewide planning through memoranda of understanding (MOU) or similar agreements. The federal Public Safety Wireless Network (PSWN) Program is establishing an executive-level public safety interoperability presence in each state. PSWN has fostered the formation of state interoperability executive committees (SIECs) as centralized forums to address wireless interoperability issues and encourage the development or modification of a state's communications system.

For example, the Washington SIEC has made substantial progress under the specific guidelines provided by the Federal Communications Commission (FCC). In establishing the SEIC, Governor Gary Locke authorized the development of a MOU to reach across broad policy objectives common to all potential participating entities. As relationships evolve and formalize, and as responsibilities become clearly defined, participants can execute additional agreements or other documents as needed. Most importantly, the governor has committed to an ongoing role in providing oversight and policy support.

ENSURE ADEQUATE WIRELESS SPECTRUM TO ACCOMMODATE ALL USERS

Spectrum is the finite range of radio channels that FCC assigns to public safety agencies for communications transmissions. As the amount of available spectrum decreases for general public safety communications, there is less of the spectrum available for interoperable communications. In addition, scarce spectrum results in congested radio traffic and increased interference. This severely limits the ability of first responders to communicate with one another and jeopardizes their safety and the efficiency of on-scene operations.

Existing spectrum management rules and regulations do not favor the implementation of shared local, state, and federal communications. Governors will need to work with the federal government to resolve the issue of wireless spectrum and obtain adequate capacity. A commitment by governors and extensive coordination between FCC and the National Telecommunications and Information Administration (NTIA) will be required to ensure that spectrum rules and regulations accommodate shared systems and interoperability frequencies are developed and maintained.

INVEST IN NEW COMMUNICATIONS INFRASTRUCTURE

Many existing public safety communications systems cannot support the modern technologies needed to achieve interoperability. Efforts to replace outdated systems or expand current systems are expensive. In fact, the PSWN Program estimates the value of existing noninteroperable communications systems in the U.S. at $18 billion; new interoperable wireless systems could cost each state nearly $200 million.

Despite these costs, governors must invest in new communications equipment. Some funding for such improvements will be available from the federal government, but states will still need to find additional resources (see box, "Federal Funding Sources").

Some states have adopted creative approaches to fund interoperability projects. For example, Indiana passed a technology surcharge on driver's license fees. A percentage of the fee is applied to Indiana's Project Hoosier SAFE-T (Safety Acting for Everyone-Together) to fund equipment procurement and maintenance. Project Hoosier SAFE-T is an initiative of Indiana's local, state, and federal public safety agencies to implement a statewide 800 MHz voice and data communications system. The project will average $16.9 million a year over a 15-year period. Initial funding has been obtained from numerous sources, including congressional appropriations; grants from the U.S. Department of Justice and the U.S. Department of Transportation; and state funding sources. To date, the program has been implemented in three demonstration sites: Johnson County, Montgomery County, and Southeast Indiana.

Project Hoosier SAFE-T will allow law enforcement, fire, emergency medical, and other public safety agencies to:

- ★ communicate with each other on a shared radio system;
- ★ decrease channel congestion;
- ★ provide enhanced radio system coverage;
- ★ achieve significant cost savings through joint planning, development, and maintenance; and
- ★ increase the time officials spend in their communities by enabling them to file paperwork, retrieve information, communicate with other agencies, and write reports from their vehicles.

Federal Funding Sources

- ★ Local Law Enforcement Block Grants (LLEBGs) from the Bureau of Justice Assistance (BJA) can be used to procure equipment, technology, and other material directly related to basic law enforcement functions. Go to: **www.ojp.usdoj.gov/BJA/grant/llebg_app.html**
- ★ The Office for Domestic Preparedness (ODP) Equipment Grant Program can be utilized to enhance the capacity of state jurisdictions to respond to and mitigate the consequences of incidents of domestic terrorism involving the use of weapons of mass destruction (WMD). Communications equipment is part of the authorized equipment purchase list for these grants. Go to: **www.ojp.usdoj.gov/odp/grants/goals/htm**
- ★ The Web site for the Office of Justice Programs (OJP) Information Technology Initiatives offers guidance on both federal and private funding sources. Go to: **www.it.ojp.gov/index.jsp**
- ★ The Advanced Generation Interoperability Law Enforcement program from the National Institute of Justice (NIJ). Go to: **www.nletc.org/agile**

DEVELOP STANDARDS FOR TECHNOLOGY AND EQUIPMENT

Although new radio technologies provide unprecedented technical capabilities to first responders, the greatest hindrance to progress involves incompatibility among systems. Many areas have invested in single, homogeneous systems that can provide substantial interoperability features among users of that system. However, such systems used by a state or governmental jurisdiction in one area may still be largely incompatible with an existing system in a nearby jurisdiction.

The problem is further exacerbated by failing to purchase equipment that meets industry standards. Consequently, jurisdictions often purchase tailored, integrated systems for their needs that may not be compatible with another system next door. In the absence of clear standards for all public safety systems, competing vendors continue to manufacture—and public agencies continue to purchase—equipment that is incompatible.

Governors can help ensure interoperability now and as systems expand by requiring their state and local public safety agencies to purchase equipment that conforms to industry compatibility standards. For example, the Association of Public Safety Communications Officials (APCO) coordinates the APCO Project 25 (P25), a joint effort among U.S. federal, state, and local governments, with support from the U.S. Telecommunications Industry Association (TIA) to create compatibility standards. State agencies are represented in this project by the National Association of State Telecommunications Directors (NASTD).

The P25 standards process seeks to provide digital, narrowband radios with the best performance possible, meet all public safety user needs, and permit maximum interoperability. A secondary objective is achieving maximum radio spectrum efficiency. The P25 documents were developed by TIA based on user needs and approved by a project steering committee that included state government representation.

PARTNER WITH GOVERNMENT AND PRIVATE INDUSTRY

Governors should form strong partnerships with local and federal governments and private industries to resolve the interoperability issue. By using a statewide, coordinated, cooperative approach, solutions can be tailored to reflect regional differences while still building sufficient statewide cohesion.

For example, in early 2000, Montana Governor Marc Racicot issued an executive order to establish the Montana Public Safety Communications Council. The order authorized the council to establish a coordinated approach to solving interoperability problems and to serve as a strategic advisor to the governor on Montana's public safety communications. Chaired by the director of administration, the council includes executive membership from state and local government, public safety associations, public safety agencies, tribal nations, and private industry. New governors should establish such an entity to address interoperability and coordinate activities with the state homeland security director.

ACTIONS A GOVERNOR CAN TAKE TO IMPROVE INTEROPERABILITY

Coordination and Partnerships

- ✔ Form a committee or council that reports back to the governor and the legislature on regional and state interoperability issues.
- ✔ Participate in statewide, regional, and national outreach and education initiatives to improve interoperability.
- ✔ Establish memoranda of understanding (MOU) that define interoperability procedures.
- ✔ Include interoperability success as part of governor's state-of-the state address.

Funding

- ✔ Establish public safety interoperability as a fiscal priority.
- ✔ Develop funding strategies or incentives that encourage greater local, state, and federal participation.
- ✔ Identify current and sustained funding to develop a shared system within the state.
- ✔ Research best practices of successful funding in other states.

Spectrum

- ✔ Retain a professional spectrum manager to provide coordinated, high-level policy guidance and direction to all public safety spectrum users.
- ✔ Develop and implement strategies for the efficient use of radio frequency spectrum.
- ✔ Ensure full state participation in Federal Communications Commission (FCC) rulemaking activities that impact the allocation of public safety spectrum.

Standards and Technology

- ✔ Ensure all new communications systems acquisitions adhere to accepted standards.
- ✔ Fully explore and test viable new technologies.
- ✔ Use small modernization projects to test technology that could have broader impact across a state or region and enhance local functional and operational requirements.
- ✔ Remain committed to standards development activities that ensure that state requirements are accurately reflected in emerging standards.

ACTIONS A GOVERNOR CAN TAKE TO IMPROVE INTEROPERABILITY (cont.)

Security

- ✔ Understand the potential security threats and risks associated with public safety communications systems.
- ✔ Establish a statewide security policy that provides maximum coverage to all agencies that could participate in a statewide or regional shared system.
- ✔ Ensure adequate funding to secure existing systems and strive to fund only those systems with existing security policies and plans.
- ✔ Identify federal security requirements that allow secure joint participation on major communications systems.

Interoperable Systems Development

- ✔ Lead planning efforts to identify state requirements necessary for implementing interoperable system strategies.
- ✔ Research best practices of other states.
- ✔ Develop an interoperable communications infrastructure available to all public safety agencies.
- ✔ Offer incentives for local and federal participation in shared or highly interoperable communications.

Source: Public Safety Wireless Network Program, National Interoperability Forum Summary Report, November 2001

Key Challenges to Wireless Interoperability

Spectrum

- ★ Public safety spectrum is in short supply
- ★ There is direct competition with powerful commercial interests
- ★ Many policymakers and the public do not understand the spectrum issue
- ★ There is no leadership in the regulatory arena

Funding

- ★ It is difficult to "sell" to government executives
- ★ The public safety wireless infrastructure is estimated to cost $18 billion
- ★ Federal funding streams are fragmented
- ★ Agencies cannot leverage combined purchasing power
- ★ Competition exists with other important government projects

Standards and Technology

- ★ Neighboring areas have incompatible equipment provided by different vendors
- ★ Standards development lacks support and funding
- ★ The standards process is slow
- ★ There are no incentives for vendors to adhere to standards

Source:
Public Safety Wireless Network Program, National Interoperability Forum Summary Report, November 2001

FEDERAL ACTIONS TO IMPROVE INTEROPERABILITY

The Public Safety Wireless Network (PSWN) Program is a federally funded initiative operating on behalf of all state, local, tribal, and federal public safety agencies. The U.S. Department of Justice (DOJ) and the U.S. Department of the Treasury jointly coordinate the program's efforts to foster interoperability among public safety wireless entities nationwide so that lives are never lost because public safety personnel cannot communicate with each other. A key element in achieving this goal is ensuring that decisionmakers at all levels have the full support of and work closely with first responder agencies. Additionally, PSWN is developing technical standards for communications systems, promoting partnerships and coordination among agencies, and serving as a clearinghouse for information.

The National Institutes of Justice (NIJ), DOJ's science and technology arm, has addressed interoperability technology issues for several years. Additionally, the Advanced Generation of Interoperability for Law Enforcement (AGILE) is developing wireless telecommunications and information technology standards and guidelines for information sharing to facilitate interoperability at state, local, and federal levels.

Finally, The Federal Emergency Management Agency (FEMA) is responsible for coordinating all federal wireless communications projects to ensure interoperability and standards and avoid stovepiped systems. Project SAFECOM includes convening wireless project managers to counter previous unsuccessful independent efforts of each federal agency working on interoperability. This project will establish separate tracks for federal-to-federal interoperability and state and local interoperability; however, project officials will closely work with state and local project managers in a subgroup to ensure horizontal and "bottom-up" interoperability. Other project goals include the release of the SAFECOM blueprint in the fall of 2002, spectrum management, and coordination with private industry.

FOR MORE INFORMATION

National Telecommunications and Information Administration (NTIA): **www.ntia.gov**

Public Safety Wireless Network (PSWIN): **www.pswn.gov**

CHAPTER 4

Critical Infrastructure Protection

As part of an overall homeland security strategy, states must assess vulnerabilities and enhance security in and around public buildings, dams, borders, water supplies, nuclear power plants, airports, education centers, and other critical infrastructures. This process should:

- ★ identify critical infrastructures;
- ★ conduct risk assessments of identified vulnerabilities;
- ★ assess the impact of interdependencies; and
- ★ implement a critical infrastructure protection plan.

IDENTIFY CRITICAL INFRASTRUCTURES

Critical infrastructures are physical systems and cybersystems consisting of private industries, institutions, and networks that provide a continual flow of goods and services essential to the nation's defense, economic security, government functions, and the welfare of its citizens. Shortly after taking office, governors should coordinate with state risk management officials to begin a critical infrastructure examination to determine vulnerabilities and risk.

Functions that contain critical infrastructure include:

- ★ banking and finance,
- ★ electric power,
- ★ emergency services,
- ★ telecommunications,
- ★ oil and gas,
- ★ transportation, and
- ★ water.

Banking and Finance

A new governor should identify banks, financial service companies, and payment systems as statewide and regional critical infrastructures that are vulnerable to physical attacks and cyberattacks. The physical threats are primarily associated with natural disasters, including flooding, fires, and wind damage that could cause information technology disruptions. Cyberattacks can be perpetrated by hackers as well as by individuals who do not have authorized access to sensitive information.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the designated lead agencies and the state homeland security office develop and implement protection plans that eliminate or mitigate identified deficiencies;
- ★ coordinate with lead agencies to develop an information-sharing system that identifies and prevents terrorist attacks;
- ★ work with the financial industry to provide education and outreach programs to increase awareness of infrastructure protection plans; and
- ★ coordinate with the lead federal agencies for this category as required.

Electric Power

The electric power infrastructure includes generating stations, transmission lines and substations, distribution networks that supply electricity to consumers, and the transportation and storage of fuels essential to the operation of these systems. This complex system includes nearly 3,000 independent electrical utilities interconnected by coordinated controls, operations, and telecommunications networks. A governor should recognize that although these utilities are owned by public investors, government, cooperatives, and manufacturing industries, nearly 80 percent of the nation's power is generated by the approximately 270 investor-owned power facilities.

Transformers, transmission towers, and substations are attractive targets to physical attacks largely because they are located outdoors. In addition, transmission towers and cables are typically situated in various rural settings with little protection. Any resulting cascading failures could shut down switching stations that impact interdependent infrastructures, such as banking and finance, transportation, communications, emergency services, and water. The primary threats are physical attacks resulting from natural or manmade causes and cyberattacks against the information or communications components that control electrical systems including unauthorized intrusions.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the lead state agencies assess the energy sector's vulnerability to physical attack and cyberattack;
- ★ work closely with the lead agencies to develop and implement protection plans that eliminate or mitigate existing physical vulnerabilities and cybervulnerabilities;
- ★ ensure that government and industry develop warning systems for anticipated or actual incidents;
- ★ coordinate with lead agencies to develop warning notification systems and conduct public awareness campaigns to educate citizens about that system;
- ★ direct the lead agencies to partner with the private sector to develop and implement innovative infrastructure assurance strategies; and
- ★ coordinate with the lead federal agencies for this category as required.

Emergency Services

The emergency services infrastructure includes police, fire, medical, and rescue systems and personnel who are called upon to respond to emergencies of various degrees. This sector also includes fire and emergency medical services (EMS) stations, apparatus and communications, 9-1-1 communications centers, hospital emergency rooms, computer networks, and pumping stations and water reservoirs. Assets of these infrastructures, such as transmission lines, are vulnerable to physical attacks and cyberattacks, which could lead to cascading failures. For example, 9-1-1 systems may become overloaded through misuse or mischief that interferes with responses to life-and-death calls. Response coordination at the scene of a terrorist incident also may be impacted by the lack of interoperable communications among first responders. Finally, responders may be specifically targeted by terrorists.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ coordinate with the lead agencies to assess the vulnerabilities of state critical infrastructures;
- ★ work closely with the lead agencies and the state homeland security office to develop and implement protection plans that eliminate or mitigate identified vulnerabilities;
- ★ partner with federal, state, and local governments and private industry to develop and implement solutions for the lack of interoperability among first responders; and
- ★ coordinate with the lead federal agencies for this category as required.

Telecommunications

As with other critical infrastructures, telecommunications are primarily vulnerable to natural disasters, cascading and escalating systems failures, and common construction accidents. The sector also is vulnerable to deliberate physical attacks and cyberattacks. With cyberthreats, individuals may possess the mechanisms, expertise, capability, and opportunity to access, penetrate, deny, alter, and destroy communications and information systems. Information technology and vulnerabilities to cyberterror are discussed in greater detail in Chapter 9.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the lead state agencies assess their critical infrastructures and coordinate with the state homeland security office and private industry;
- ★ partner with these government agencies, state homeland security, and the private sector to develop and implement protection plans to eliminate or mitigate identified vulnerabilities;
- ★ coordinate with lead agencies and private industry to develop outreach programs that raise the public awareness about telecommunications protection plans; and
- ★ coordinate with the lead federal agencies for this category as required.

Oil and Gas

Oil and gas infrastructure includes the production and storage sites for natural gas, crude, and refined petroleum and petroleum-derived fuels; refining and processing facilities and pipelines; and the ships, trucks, and trains that transport these commodities. An increase in the oil transported via pipelines has created attractive targets for physical attacks. Additionally, vulnerability of this infrastructure to cyberattacks has been exacerbated by modern technology, such as supervisory control and data acquisition (SCADA) systems that centralize operations and remote maintenance systems for public networks.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the designated lead agencies assess the vulnerability of their assets;
- ★ coordinate with lead agencies and the state homeland security office to develop and implement protection plans that eliminate or mitigate identified vulnerabilities;
- ★ direct the lead agencies to coordinate with private industry to develop and implement citizen-warning notification systems;
- ★ partner with government agencies and private industry to conduct outreach to the community on oil and gas protection efforts; and
- ★ coordinate with lead federal agencies for this category as required.

Transportation

Transportation infrastructure includes all facilities and structures that move people and goods throughout the states by air, land, and sea. In addition to possessing inherent risks, including mechanical and human failure, transportation assets have historically been vulnerable to a host of natural and manmade disasters. The nation's overwhelming reliance on information systems has introduced new vulnerabilities via electronic penetrations and attack, which could disrupt or completely shut down state and regional transportation systems.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the designated lead agencies assess the vulnerabilities of the state's transportation assets;
- ★ coordinate with lead agencies, the state homeland security office, and private industry to develop and implement protection plans that eliminate or mitigate identified vulnerabilities; and
- ★ coordinate with the lead federal agencies for this category as required.

Water

Water infrastructure includes all surface and groundwater sources of untreated water for public and private-sector use; reservoirs and storage facilities; water aqueducts and transport systems; filtration and cleaning systems; pipelines; cooling systems; and wastewater collection and treatment facilities. The nation's extensive water systems cannot be entirely protected at any given time, so these systems are vulnerable to physical attack and cyberattack. Terrorists may attack water and wastewater systems by introducing contaminants or initiating other physical attacks and cyberattacks meant to deprive citizens of essential water and water-dependent functions, such as firefighting operations, sanitation, and manufacturing.

A governor should:

- ★ identify the lead state agencies for this category;
- ★ ensure that the designated lead agencies assess the vulnerability of state water assets;
- ★ coordinate with lead agencies and the state homeland security office to develop and implement protection plans that provide safe drinking water from alternate sources, such as neighboring or regional water plants;
- ★ work with the lead agencies to establish a communications protocol to notify appropriate state officials about an anticipated or actual terrorist threat;
- ★ ensure that the lead agencies develop public outreach programs to explain the actions that must be taken in a water emergency; and
- ★ coordinate with the lead federal agencies for this category as required.

CONDUCT RISK ASSESSMENTS OF IDENTIFIED VULNERABILITIES

Governors and their homeland security teams should initially collaborate with the appropriate risk managers to determine who will conduct the risk assessment process and the methodology to be used. Many states have developed and applied their own risk-and-vulnerability assessment tools; others have either designated agency risk managers or contracted with the private sector to conduct assessments.

Risk management officials will initially assess risk in the context of natural, manmade, terrorism, technological, cyber, and internal or external threats. They will ascertain whether the risk is controllable and whether any prior warning is likely. The risk managers will then assess the impact by determining event probability, assessing information credibility, and considering the duration of the event's impact on essential services. Threats are then prioritized based on probability of occurrence, likely severity, and the impact to state and regional interdependencies. Upon completion of the risk assessment process, the officials should coordinate with the governor, state lead agencies, and the state homeland security director to develop and implement a critical infrastructure protection plan that will identify measures to prevent, eliminate, or mitigate the threat.

ASSESS THE IMPACT OF INTERDEPENDENCIES

Each critical infrastructure possesses unique risks; however, the ultimate impact and magnitude of these risks may be determined by interdependencies. Interdependencies are defined here as two or more infrastructures with operations dependent on each other. They produce a higher risk environment for critical infrastructure if they allow a minor local incident to cascade into an unanticipated regional, statewide, or multistate event impacting several systems. Since a significant number of these interdependent infrastructures are owned and operated by private industry, a new governor and homeland security office should partner with the private sector to conduct complete and timely critical infrastructure protection activities.

IMPLEMENT A CRITICAL INFRASTRUCTURE PROTECTION PLAN

Each state agency should identify and assess risks that could disrupt or destroy essential services, evaluate the capability of its response and recovery mechanisms, and eliminate or mitigate vulnerabilities. If governors and state homeland security officials determine that existing resources are inadequate to counter identified threats, they will need to develop and execute critical infrastructure protection plans that prioritize the required protection efforts and authorize participation in memoranda of understanding (MOU) with neighboring states (see box, "Checklist for the Development of a Critical Infrastructure Protection Plan").

Lead agencies should develop long-term protection plans that identify risks that can be addressed on a priority basis and use intelligence resources to monitor emerging threats. Any plan should include education and outreach programs to increase public awareness of infrastructure vulnerabilities. For example, the state's lead energy agency should develop warning notification systems, plan for response actions, and review strategies to ensure restoration of essential services.

A majority of states may have a ready resource in Year 2000 (Y2K) critical infrastructure assessments. The arrival of 2000 was uneventful largely due to the extensive risk and vulnerability assessments that were conducted by state officials. Y2K provided the impetus for states to proactively develop and implement risk assessment and continuity of government programs. Preparing for the date change, states established comprehensive critical infrastructure protection programs that can now be a foundation for the assessment of terror-related infrastructure vulnerabilities. Governors also should consider the Y2K "lessons learned" that states can build upon in assessing their critical infrastructure vulnerabilities.

CHECKLIST FOR THE DEVELOPMENT OF A CRITICAL INFRASTRUCTURE PROTECTION PLAN

- ✔ Ensure that infrastructure stakeholders coordinate with each other to assess vulnerabilities.
- ✔ Emphasize that critical infrastructure information must be shared among affected state agencies.
- ✔ Review state plans and statutes and assess state capabilities.
- ✔ Evaluate the state's preparedness against conventional and unconventional threats.
- ✔ Identify legal liabilities and consequential damages in cascading events.
- ✔ Develop infrastructure assurance awareness, education, and exercise programs.
- ✔ Assess the availability of technical assistance to protect infrastructure.
- ✔ Develop and implement exercise and training programs that determine how and when warnings will be disseminated to agencies and the general public.

The Iowa Homeland Security Critical Asset Assessment Model

The Iowa Homeland Security Critical Asset Assessment Model (CAAM) ensures systematic identification, assessment, and prioritization of critical assets and offers recommendations based on assumptions of future credible terrorism threats or actual identification of a target. This assessment tool:

- ★ enables elected and appointed officials to set priorities that reflect the degree of risk;
- ★ provides descriptors for each potential target in the state;
- ★ establishes a methodology for comparison of different assets;
- ★ justifies management decisions for altering customary programming, budgeting, and staffing assignments;
- ★ encourages identification of technical and research needs in asset protection and emergency management;
- ★ enables the establishment of a viable geographic information system (GIS) database of asset criticality and vulnerability;
- ★ remains flexible to accommodate past and future asset analyses; and
- ★ evaluates the prioritized assets in greater detail to address their vulnerabilities.

FOR MORE INFORMATION

American Water Works Association (AWWA). Go to: **www.awwa.org**

Critical Infrastructure Assurance Office (CIAO). This agency, housed in the U.S. Department of Commerce, was created by Presidential Decision Directive 63 (PDD-63) to develop a national plan for critical infrastructure protection on the basis of plans developed by the private sector and federal agencies. Go to: **www.ciao.gov**

Critical Infrastructure Protection Process (U.S. Fire Administration Job Aid). Go to: **www.usfa.fema.gov/dhtml/fire-service/cipc.cfm**

Energy Information Sharing and Analysis Center (ISAC) for oil and gas infrastructures. Go to: **www.energyisac.com**

Federal Computer Incident Response Center (FEDCirc). This agency is operated by the General Services Administration (GSA) as the central coordinating point on security vulnerabilities and lower level security incident data. Go to: **www.fedcirc.gov**

Infragard. A nationwide information-sharing and analysis initiative that includes the U.S. government and an association of businesses, academic institutions, state and local law enforcement agencies, and others. Go to: **www.infragard.net**

The Infrastructure Security Partnership (TISP). Go to: **www.tisp.org**

National Infrastructure Protection Center (NIPC). An organization within the FBI that has expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response. Go to: **www.nipc.gov**

National Telecommunications and Information Administration (NTIA). This agency's responsibilities include raising information- and communications-sector awareness of vulnerabilities and risks; assisting the sector to eliminate/mitigate its vulnerabilities; facilitating establishment and operation of sector information sharing and analysis centers; developing cooperative efforts with other countries and international organizations; and providing industry with information on results from U.S. government research and development. Go to: **www.ntia.doc.gov**

Presidential Decision Directive 63 (PDD-63). The Clinton Administration's policy on critical infrastructure protection. Go to: **www.nipc.gov/about/pdd63.htm**

U.S. Department of Energy Office of Critical Infrastructure Protection. The mission of this program includes working with state and local governments and industry to develop and implement infrastructure assurance plans; fulfilling responsibilities as the lead federal agency for assuring the continuity and viability of the nation's critical electric, oil, and gas infrastructures; providing technologies, tools, and expertise to promote infrastructure assurance; working with infrastructure stakeholders to assess physical vulnerabilities and cybervulnerabilities; assisting with the development of plans to mitigate significant vulnerabilities; and working with state and local governments and industry to develop/enhance plans for response and reconstitution of essential capabilities and services. Go to: **www.ocip.dis.anl.gov**

U.S. Department of Transportation, Office of Pipeline Safety (OPS). Go to: **www.ops.dot.gov**

U.S. Environmental Protection Agency (EPA) counterterrorism Web site. Go to: **www.epa.gov/swercepp/cntr-ter.html**

U.S. Environmental Protection Agency (EPA) drinking water security Web site. Go to: **www.epa.gov/safewater/security/index.html**

Water Information Sharing and Analysis Center (ISAC). The Water ISAC was created to provide information about potential and imminent threats to utilities, reports of incidents on a nationwide basis, incident trends, possible responses to threats and attacks, and research on infrastructure protection. Go to: **www.amwa.net/isac/watercip.html**

CHAPTER 5

The Challenge of Bioterrorism

The United States has little experience with the deliberate release of a biological agent to cause a major disease outbreak. Unlike explosives or chemical releases, an attack involving biological agents could go undetected for days. No early warning satellites will alert us to an attack, no fire trucks and ambulances will rush to the scene. Only when individuals go to a doctor, clinic, or hospital, will any evidence of attack appear. Even then, the initial symptoms might not be recognized and accurately diagnosed. Furthermore, those individuals could be at great distances from the original site of exposure by the time symptoms occur.

In a bioterrorist attack, the medical personnel will be the front-line responders. The deliberate release of anthrax against civilians in October 2001 increased national awareness and concern about bioterrorism and highlighted the responsibility and importance of state and local health departments. Across the nation, local, state, and federal authorities are continuing to improve the ability to more rapidly detect abnormal public health problems. However, the public health and medical care fields still face shortages in capabilities and resources to respond and react to weapons of mass destruction (WMD) events. To prepare for and respond to a bioterrorist attack, the United States needs an improved network of infectious disease surveillance, enhanced communications, upgraded laboratory facilities, advanced diagnostic techniques, and expanded training of health-care personnel.

To deal with actual or potential mass casualty events, governors must make the increase in public heath and medical capabilities—and the ability to deploy these resources—very high priorities. Governors and their homeland security directors can prepare their states to respond to a bioterrorism attack by:

- ★ building strong public health systems;
- ★ ensuring public health is integrated into emergency management systems; and
- ★ reviewing the governor's emergency powers.

BACKGROUND: THE HISTORY OF BIOTERRORISM

The use of biological weapons in warfare has been recorded throughout history. One of the first cases of biological warfare occurred in the 14th century. In 1346, after a three-year unsuccessful siege of the Crimean seaport of Kaffa, the Tartars placed plague-infected cadavers on their catapults and flung them into the walled city. The plague quickly spread throughout the city and the fleeing population brought the plague to Europe via the Mediterranean trade routes.

Smallpox also became a biological weapon on several occasions. The Spanish conquistador Francisco Pizarro presented South American natives with variola-contaminated clothing in the

15th century. During the French and Indian War of 1754 to 1767, England's Sir Jeffrey Amherst gave smallpox-laden blankets to Indians loyal to the French and the Native Americans sustained epidemic casualties.[1]

In 1943, the U.S. began research into the use of biological agents for offensive purposes. This work began as a response to a perceived biological warfare threat from Germany. The U.S. conducted this research at Camp Detrick (now Fort Detrick) and produced agents at other sites until 1969, when President Richard Nixon stopped all offensive biological and toxin weapon research and production by executive order. Between May 1971 and May 1972, all stockpiles of biological agents and munitions from the now-defunct U.S. program were destroyed.

In 1972, the U.S., the United Kingdom, and the former Soviet Union signed the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and their Destruction (commonly called the Biological Weapons Convention). More than 140 countries have signed on since. Despite this agreement, biological warfare research continues to flourish in many countries hostile to the United States.

Proliferation and Current Threat of Bioweapons

At least 25 countries possess—or are in the process of acquiring and developing—the ability to inflict mass casualties and destruction through biological agents. Among these are "rogue nations" with histories of sponsoring terrorism. In addition to the nations pursuing these weapons, subnational groups and other nonstate actors also have shown interest in acquiring bioweapons.

Several contributing factors have led to the proliferation of biological weapons. First, creating biological weaponry often requires fewer infrastructures (i.e., laboratory space, chemical reagents, specialized equipment, etc.) compared to nuclear or chemical weapons. Second, the global diffusion of knowledge and the spread of "dual-use" technologies into the commercial market have increased accessibility to those individuals, groups, or states who seek to create or acquire biological weapons.[2] It also is difficult to prove the existence of bioweapons programs. Detection of bioagents is far more difficult than detecting the presence of materials needed to construct a nuclear weapon. Vast amounts of money have been invested in environmental sensors to detect biothreats, but with minimal success.

Long-Term Threat

Many experts believe the rudimentary anthrax attacks of the fall of 2001 were just a prologue to the more ambitious use of bioweapons in the future. The technology to create bioweapons is becoming more powerful, more available, and less expensive. What used to take a highly skilled team of scientists months to accomplish can now be done by a motivated and skilled individual in days. We are entering an era in which the threat of bioterrorism will involve far more than the common agents or delivery systems we know today.

---

[1] *Bioterrorism in the United States: Threat, Preparedness, and Response, Chemical and Biological Institute*, CBACI Project Team, Michael Moodie, Project Director.

[2] *Proliferation: Threat and Response*, Office of the Secretary of Defense, January 2000.

The Impact of Bioweapons

The impact of a biological weapon will depend on the characteristics of the pathogen or toxin, the design of the weapon or delivery system, the environment in which it is used, and the speed and effectiveness of the medical and public health response. A successful bioterror attack could cause high human morbidity, serious economic impact, and damage the effectiveness of government.

Biological Agents. Biological agents are organisms or viruses that can cause deadly diseases in people, livestock, and crops. The agents kill by spreading a disease that is normally fatal or by tricking the body's or plant's cells into producing a toxin that overwhelms its defenses. Only a small number of the hundreds of bacteria and viruses are viable as terrorist weapons because most cannot survive outside narrow temperature ranges or are too rare and hard to grow.

Many biological agents are colorless, odorless, and difficult to detect. They are usually dry in form, although liquid forms also can be used. Though liquid agents are easier to prepare, they are more difficult to disperse. Dried agents, on the other hand, are difficult to produce. They require sophisticated production equipment, but the agent often can be dispersed in highly effective aerosol form.

Facts about Smallpox

Smallpox is a disease caused by a virus, which has not been seen outside two secure laboratories since 1980. The disease can spread from person to person. Transmission usually occurs only after the patient develops a fever and rash. Although there is no treatment for the disease, a vaccine against smallpox provides excellent protection and will stop the spread of the disease. While many vaccines must be given weeks or months before a person is exposed to infection, smallpox vaccine is different. It protects a person even when given two to three days after exposure to the disease and may prevent a fatal outcome even when given as late as four to five days after exposure. Smallpox was eradicated globally by 1980 and vaccinations stopped everywhere in the world.

The Smallpox Vaccine

The federal government, which has pledged to secure enough smallpox vaccine to inoculate the entire U.S. population, is now developing a policy on who should receive the vaccine. Increased risk of dying from the vaccine's side effects could have a major impact on the government's final vaccination policy. A Centers for Disease Control and Prevention (CDC) advisory panel recently suggested that 10,000 or 20,000 health-care workers likely to come into contact with the disease in the event of a bioterrorist attack be inoculated, but the U.S. Department of Health and Human Services (HHS) is considering a wider vaccination scheme that could see several hundred thousand health-care workers vaccinated. The private sector is working to produce treatments to mitigate the vaccine's side effects and to produce a safer vaccine for use if a mass vaccination was ordered by the federal government. Currently, the government employs a ring vaccination strategy under which the infected person and his contacts are vaccinated, but officials have said that could be quickly revised if a large-scale smallpox attack were to occur.

Bioterror agents can be categorized as lethal or incapacitating and as contagious or noncontagious. Anthrax is not contagious. People do not spread it among themselves and individuals cannot catch anthrax from someone who is dying of it. On the other hand, smallpox is contagious. It spreads rapidly, magnifying itself, causing mortality and chaos on a large scale.

Whether a delivered agent causes sickness or death depends on the health of those attacked, their immune status, the characteristics of the agent, and the route of entry in humans. Most biological agents take time to infect a body, so persons infected by an attack may disperse over wide areas, making it extremely difficult to determine where or when the original attack occurred. Ominously, individuals may not display symptoms for days while they may infect others.

Facts about Anthrax

- ★ Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus Anthracis*. Anthrax most commonly occurs in hoofed mammals and can also infect humans.
- ★ Symptoms of the disease vary depending on how the disease was contracted, but usually occur within seven days after exposure. The serious forms of human anthrax are inhalation anthrax, cutaneous anthrax, and intestinal anthrax.
- ★ Initial symptoms of inhalation anthrax infection may resemble a common cold. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is often fatal.
- ★ The intestinal form of anthrax may follow the consumption of contaminated food and is characterized by an acute inflammation of the intestinal tract. Initial signs of nausea, loss of appetite, vomiting, and fever are followed by abdominal pain, vomiting of blood, and severe diarrhea.
- ★ Direct person-to-person spread of anthrax is extremely unlikely, if it occurs at all. Therefore, there is no need to immunize or treat contacts of persons ill with anthrax unless they also were exposed to the same source of infection.
- ★ In persons exposed to anthrax, infection can be prevented with antibiotic treatment. In the event of a bioterrorist attack, health authorities would conduct a rapid investigation, determine the place and time of the release, and identify individuals who need antibiotics. The federal government has stockpiled antibiotics for large-scale distribution in the event of a bioterrorist attack of anthrax.
- ★ Early antibiotic treatment of anthrax is essential—delay lessens chances for survival. Anthrax usually is susceptible to penicillin, doxycycline, and fluoroquinolones. An anthrax vaccine also can prevent infection. Vaccination against anthrax is not recommended for the general public and is not available.

BUILDING A STRONG PUBLIC HEALTH SYSTEM

Building a strong public health system is the first step in developing a plan to combat bioterrorism. A strong public health system will not only counter the threat of terrorism, but protect citizens from the health dangers present in the 21st century, such as West Nile Virus and Mad Cow Disease. In addition to enhancing basic capabilities, governors must integrate public health into emergency plans and ensure their emergency powers are current and adequate.

The nation's public health system is a complex network of people, systems, and organizations working at local, state, and national levels. The public health system is unique because it focuses on the health of entire populations, rather than on the health of the individual.

HHS has dedicated $1.1 billion in 2002 to help states strengthen their capacity to respond to acts of bioterrorism and other public health emergencies for both human and animal populations. However, during the past 20 years, our public health system has been neglected. Many public health programs are underfunded and in various states of neglect. The nation's public health system faces an unprecedented opportunity to rebuild its infrastructure while facing new and emerging threats. Notable among these are the spread of HIV infections here and abroad, Hantavirus in the Southwest; a growing West Nile epidemic; and most recently the bioterrorism (anthrax) events of October 2001 in Connecticut, Florida, Maryland, New York, Virginia, and Washington, D.C.

The anthrax mailings of last October proved that even a relatively minor scale of attacks could severely test the public health infrastructure. Though the current system was stretched to its limit, states were able to mobilize to address these public health threats. However, these events were an eye-opener, and the nation discovered that much needed to be done to increase the capacity and capability of the public health system.

To meet the threats facing us today, governors must oversee an unprecedented buildup of state and local public health infrastructure, which will be aided by a large infusion of federal dollars. For the buildup to be successful, governors and state homeland security officials should focus on:

- ★ enhancing public health leadership;
- ★ upgrading surveillance capabilities;
- ★ enhancing biological laboratory capacity
- ★ improving epidemiology capabilities; and
- ★ enhancing health alert networks.

Enhancing Public Health Leadership

The state health director is a key player on a governor's homeland security team. A new governor should ensure that state health department directors, particularly if they also are new to government, understand the importance of integrating public health into the state's overall emergency management structure. The governor should meet with his or her chief of staff, homeland security director, and state health director to define their roles and responsibilities prior to and during a bioterror attack. Moreover, the governor should meet with all state agency officials who would respond to a bioterror attack to ensure they understand how to interact with the governor's office and state public health department during an emergency.

As the nation's experience with anthrax last fall demonstrated, public health leadership, expertise, and resources are essential when an act of bioterrorism is suspected or threatened. During the anthrax investigations in October, state public health laboratories throughout the nation tested thousands of samples of suspicious powder every day. Labs in Maryland, for example, tested over 2,000 powders, nasal swabs, and clinical specimens.

Upgrading Surveillance Capabilities

Surveillance is the single most important tool to identify infectious diseases and the possible release of a bioterrorism agent. Effective surveillance requires establishing good reporting procedures by the health-care community and ensuring that robust laboratory and other diagnostic capabilities are available. An effective surveillance system should:

- ★ detect minor changes in the health status of the monitored population;
- ★ monitor as many data types as possible;
- ★ establish systems of exchanging this information on an ongoing basis; and
- ★ rapidly analyze information.

The best surveillance detects suspicious illnesses before diseases are confirmed by diagnosis. The appearance of an unusual disease or increased incidence of an ordinary disease in a normally healthy population would probably first be recognized through basic public health surveillance at the state and local level. However, the challenge of stemming infectious diseases has fallen to agencies that often lack the experience and the money to spot a budding outbreak.

Effective preparation for emerging infectious diseases requires strong foundations in professional expertise, laboratory support, and research capacity. These foundations support the infrastructure to address the ongoing but often changing threats from emerging infections. Such a system requires trained personnel in states and local communities and timely communications among state and local health departments, public and private laboratories, health-care providers, and CDC.

Investigative capabilities of state health departments vary widely. Bigger health departments tend to have two or three specialists who investigate the source and scope of infectious diseases and who work with hospitals and other agencies. They track down contacts and histories of infected people, identify the routes of transmission, and help determine who is at risk. Departments with less funding and smaller staffs may rely entirely on restaurant inspectors or nurses for investigative and epidemiology work.

Whether departments are big or small, any number of staffers may be pulled from their regular jobs and dispatched into the field during an outbreak. Health directors cannot sustain manpower demands of large outbreaks for long. Infectious-disease teams must have the staff and funding to be effective.

Enhancing Biological Laboratory Capacity

The laboratory component of public health and medical response to bioterrorism is largely an assessment tool. Laboratories must have a minimum capability to confirm or refute preliminary test results on bacteria and viruses. Physicians will depend on laboratories to distinguish the agents used in a bioterror attack. Laboratories also must be able to test for antimicrobial sensitivity and determine whether a particular antibiotic or vaccine will be effective against the given agent. Laboratories also will be important in determining how many biological agents are involved and must support law enforcement efforts through microbial forensics to determine where the agent may have originated.

All state health departments can obtain test results on suspected infectious agents. Laboratories are usually classified as Level A, B, C, or D. Level A laboratories are those typically found in community hospitals, and these laboratories can perform initial testing on all clinical specimens (usually blood or some other body fluid). Public health laboratories are usually Level B. These can confirm or refute preliminary test results and usually perform antimicrobial susceptibility tests on bacteria and viruses. Level C laboratories, which are reference facilities and can be public health laboratories, perform more rapid identification tests. Level D laboratories perform the most sophisticated tests and are located in federal facilities such as CDC.

Every state has a laboratory response network (LRN) contact. The LRN links state and local public health laboratories with advanced-capacity laboratories, including clinical, military, veterinary, agricultural, water, and food-testing. Laboratory technicians should contact their state public health laboratory to identify their local LRN representative.

Improving Epidemiology Capabilities

Epidemiology can assess the exact nature of a bioterrorist event. Epidemiologists interpret raw data gathered through surveillance and investigations to determine the source of an outbreak, mode of transmission, extent of exposure, and pattern of progress. Based on this information, they make recommendations for the appropriate public health and treatment measures to contain the outbreak.

There are acute shortages of epidemiologists, nursing staff, pharmacists, and other critical health personnel across the nation. Moreover, there is insufficient state and local capacity for conducting rapid and widespread epidemiology during suspected bioterrorist attacks. There are only a small number of epidemiologists available at even the largest public health departments, and much of their time is consumed by investigating natural disease outbreaks or engaging in pubic health campaigns.

A robust epidemiological investigation capability must include:[3]

- ★ adequate personnel to analyze surveillance data and investigate unusual outbreaks;
- ★ real-time access to surveillance data, including archived historical disease data for comparison;
- ★ electronic systems to compile and analyze patient data gathered manually during epidemiological interviews;
- ★ open lines of communication and shared information with laboratories, hospitals, physicians, and federal-level entities; and
- ★ a broad understanding of a variety of disease patterns—endemic or nonendemic, food borne or water borne—produced by both traditional bioterrorism agents and unexpected or nontraditional agents.

It is unlikely that any state can employ enough full-time epidemiologists to address a widespread disease outbreak or bioterrorism event. For this reason, state health departments should identify epidemiological resources that can be tapped in an emergency. The source of such expertise may be found in the consulting industry, private and state colleges and universities, federal facilities (including military bases and labs), and private labs.

Enhancing Health Alert Networks

Information and communication play central roles in counterterrorism activities. Several initiatives have been designed and are being implemented to improve sharing of key data. Foremost among these is the Health Alert Network (HAN), which improves the basic information technology infrastructure of state and local public health departments.

[3] *Bioterrorism in the United States: Threat, Preparedness, and Response, Chemical and Biological Institute*, CBACI Project Team, Michael Moodie, Project Director.

HAN provides a secure Internet connection that links states' health resources and provides information and warnings about bioterrorism and other issues. It gives state health-care communities a powerful diagnostic tool. For example, if an emergency room in one city treats a patient with unusual symptoms, doctors can immediately contact local or state health authorities who can identify similar reported cases and issue an alert. This system helps state health-care authorities react quickly and effectively in the situation—whether it's the intentional release of a biological agent or the spread of West Nile.

ENSURING PUBLIC HEALTH IS INTEGRATED INTO EMERGENCY MANAGEMENT SYSTEMS

Bioterrorism has two dimensions: the biological, where public health expertise is necessary to detect and respond; and terrorism, which is a criminal act requiring law enforcement prevention and response. The challenge—and potentially the great strength—of bioterrorism preparedness is combining the state's resources and skills of public health with those of other public safety and emergency preparedness disciplines. Each of these disciplines should have a robust system in place.

The public health system must be properly integrated with the state's overall emergency management functions. In particular, a governor must ensure that:

- ★ disease surveillance networks have procedures to alert homeland security officials of possible events that suggest a bioterror attack;
- ★ key public health personnel have procedures for dealing with and processing classified information; and
- ★ public health officials participate in drills with law enforcement and other agencies to practice responding to a bioterrorism incident.

State public health directors, homeland security directors, law enforcement officials, and emergency management officials should meet regularly and keep each other apprised of each other's activities. Relationships can be key to the success of a response. State officials also should develop a rapport with federal agencies and the private sector through forums, training exercises, and site visits. Likewise, governors and their senior staff should participate in training events, drills, and exercises. These activities provide an excellent opportunity to build these relationships and integrate public health into the state's emergency management system.

Governors must assess the state's emergency preparedness and response capabilities for bioterrorism, other outbreaks of infectious disease, and other public health emergencies. They should then review the statewide plan for preparedness and response and set priorities to fill any gaps in readiness. Governors also should review their state's plans and protocols to receive and distribute the national pharmaceutical stockpile (NPS) to make sure they are adequate. For more information on the NPS, go to page 70.

Governors also may want to establish a bioterrorism preparedness advisory committee.[4] This committee should work closely with the governor's homeland security director. The committee should include representatives from:

- ★ state and local health departments and government;
- ★ state homeland security office;
- ★ emergency management agencies;
- ★ emergency medical services;
- ★ office of rural health;
- ★ police, fire department, and emergency rescue workers;
- ★ occupational health workers;
- ★ other health care providers, including university, academic, medical, and public health;
- ★ community health centers;
- ★ Red Cross and other voluntary organizations; and
- ★ the hospital community (to include veterans and military hospitals).

Governors also may want to establish a hospital biopreparedness planning committee (affiliated with the statewide bioterrorism advisory committee). Its composition may include representation from:

- ★ emergency medical services;
- ★ emergency management agencies;
- ★ rural health office;
- ★ state hospital associations;
- ★ veterans affairs and military hospitals; and
- ★ primary care associations.

Most of the reserve capacity in the hospital system has been eliminated. Moreover, there is no "surge capacity" in the hospital system to handle a bioterror attack that would cause extensive casualties. Lack of decontamination capabilities for medical facilities would further exacerbate this situation. Governors should assess and strengthen hospital surge capacity and urge their emergency management, medical, and public health professions to work on all levels to ensure they have a certain minimum surge capacity to deal with mass casualty events. Governors also should consider nontraditional ways to buttress medical surge capacity, including using alternate sites, such as veterans' hospitals; in addition, they should utilize gymnasiums, armories, and other facilities, such as mobile hospitals, for mass casualty incidents.

[4] CDC's "Guidance for Fiscal Year 2002 Supplemental Funds for Public Health Preparedness and Response for Bioterrorism." Available at: www.cdc.gov

Top Ten Suggestions from State Health Officials Who've Been There

Pre-event:

1 **Establish strong relationships with top state officials in law enforcement.**

- ★ Establish these relationships among the highest levels to avoid complex chains of communications.
- ★ Recognize that disaster sites that are also crime scenes have special chain-of-evidence issues that should be discussed with law enforcement.

2 **Prepare for the possibility that various levels of law enforcement may have poor communications among themselves (FBI, U.S. Department of Justice, state and local authorities).**

- ★ Recognize that public health may sometimes serve as a communications bridge between different law enforcement agencies.

3 **Prepare procedures to address classified information issues.**

- ★ Build protocols with law enforcement to determine what information is classified and what can be made public.
- ★ Create a team of law enforcement and public health personnel that can assess each new piece of information. Give this team the authority to make on-the-spot decisions about what can be made public.

4 **Address, in advance of an emergency, who will need FBI security clearance.**

- ★ Ensure that senior public health staff have sufficient security clearance to be involved in law enforcement activities and briefings.
- ★ Determine which local authorities require clearance to attend meetings and participate in decisionmaking.

5 **Plan in advance for multijurisdiction issues with regional input.**

- ★ Deal now with issues like interstate needs, public/private capacity sharing, out-of-state volunteer credentialing, etc.
- ★ Develop, whenever possible, written agreements and contact protocols for these regional issues.

6 **Review personal information restrictions and emergency powers.**

- ★ Examine the ability of hospitals to share patient status information in an emergency and the authority of the health department to lift privacy restrictions.
- ★ Plan for concerns of vital records, including death certificates and identity theft.

(continued on next page)

Top Ten Suggestions from State Health Officials Who've Been There (cont.)

Post-event:

7 Arrange for the availability of an immediate 1-800 phone number.

- ★ Recognize that more than one number may be needed so providers, law enforcement, and others can reach the department 24-hours-a-day. Announce availability of the numbers immediately to avoid confusion and frustrations.
- ★ Establish a separate number for general inquiries and public information.

8 Capitalize on strong relationships between public health and the provider community.

- ★ Work with local public health authorities to reach out to providers.
- ★ Distribute fact sheets, diagnostic guides, procedural protocols, and contact information to the provider community.

9 Recognize the emotional and mental health needs of first responders, health department personnel, and the public.

- ★ Mitigate post-traumatic stress concerns by having on-site teams available for first responders, including mental health counselors and other therapists.
- ★ Provide opportunities for health department staff not directly involved to make contributions in longer term situations. Address their safety concerns and attempt rumor control through information sharing.

10 Address long-term outcomes of the current events.

- ★ Recognize and prepare for long-term mental health needs of and possible substance abuse by the general public following such events.
- ★ Strengthen occupational health-monitoring systems.
- ★ Build up surveillance systems for syndromes for future events.
- ★ Establish support services for survivors.
- ★ Revisit your emergency response plan. Update, discuss, and revise as needed, and ensure all personnel are prepared to implement.

Source: Association of State and Territorial Health Officials

Governors should consider developing mutual aid agreements across multiple jurisdictions and a regional bioterrorism response capability with neighboring states. Governors also should participate in state (and multistate) drills and exercises to prepare for bioterror attacks. Exercises are a vital component of bioterrorism preparedness efforts at all levels of public health.

REVIEWING THE GOVERNOR'S EMERGENCY POWERS

In addition to the state homeland security director, governors should consult regularly with their appointed state commission charged with developing the state's bioterrorism preparedness plan to ensure they understand the state's plan and have the necessary legal authority to carry it out.

Governors may want to designate a senior public health official within the state health department to serve as executive director of the state bioterrorism preparedness and response program and another as a coordinator for hospital preparedness planning. It is imperative that the bioterrorism coordinator maintain regular communication with the governor's homeland security advisor, who has lead responsibility for the state's overall response to terrorism.

Communications Strategy

A governor should have a strategy for communicating with the public during a bioterrorism attack (Chapter 2 discusses crisis communication in detail). The importance of the governor communicating comprehensive, current information to the public in the aftermath of such an attack cannot be overemphasized, even if it is disturbing information. It is important also for the governor to have medical and scientific leaders who will lead such efforts that are trained well in the difficult skill of media communication. The potential for positive or negative impact is so great that governors must make this a priority.

Emergency Powers

The governor's legal counsel should review the governor's emergency powers early in the administration to ensure the governor has the power to declare an emergency if there is a public health threat caused by acts of terrorism (chemical, biological, radiological, or mass trauma) or a communicable disease. A clear understanding of the governor's powers saves time during critical situations and enables the governor to proceed confidently. During a bioterrorism attack, the governor needs to:

- ★ use all available state government resources;
- ★ suspend laws that hinder a response;
- ★ direct actions of state personnel (including militia);
- ★ work with other states to coordinate aid;
- ★ enforce quarantines;
- ★ see that people are vaccinated;
- ★ seize and destroy property without compensation; and
- ★ ration medical supplies, food, water, and fuel.

GOVERNOR'S BIOTERRORISM PREPAREDNESS CHECKLIST

- ✔ Assess state's preparedness and response capabilities.
- ✔ Review statewide bioterrorism preparedness plan.
- ✔ Review and assess laws, statutes, regulations, and ordinances within the state that provide for credentialing, licensure, and delegation of authority for enforcing essential emergency public health measures, including quarantine.
- ✔ Designate a senior public health official to be executive director of the state bioterrorism preparedness and response program.
- ✔ Establish a bioterrorism advisory committee.
- ✔ Establish a hospital biopreparedness committee.
- ✔ Improve surveillance, detection, and communication capabilities based on symptomology and disease reporting at both local and regional levels (including alerts and notifications).
- ✔ Assess training needs and conduct bioterrorism-relevant training.
- ✔ Conduct drills and exercises to prepare for bioterror attacks.
- ✔ Assess and strengthen hospital surge capacity.
- ✔ Develop a crisis communications plan.

Update Public Health Laws

Most state health emergency laws haven't been updated since the polio outbreaks a half-century ago. Policymakers must ensure that their state's public health system and laws are current and will serve the public well in a terrorist attack. These are the same public health laws that help states guard against natural threats, such as influenza, measles, West Nile virus, and Hantavirus; toxic substance spills; and natural disasters, such as hurricanes, fires and floods.

A model law developed for CDC and provided to states in 2001 is a tool states can use to measure their state laws and ensure that proposed emergency response measures include broad powers to control both people and property in extraordinary emergency situations. For example, it allows compulsory medical examinations and vaccinations and it requires people to be quarantined or face a penalty. The public health agency also would control health-care facilities, materials, food, medicines, transportation, and other property and services as necessary to reasonably respond to the emergency.

FOR A MODEL PUBLIC HEALTH LAW

Go to: **www.publichealthlaw.net/MSEHPA/MSEHPA2.pdf**

FEDERAL RESOURCES

On January 10, 2002, approximately $2.5 billion was awarded to HHS to improve public health systems by building capacities to rapidly and effectively respond to and recover from acts of bioterrorism. Long-term goals for these funds focus on developing and institutionalizing sound public health practices. Within HHS, a majority of funds has gone to CDC to develop bioterrorism preparedness and response programs. Approximately $130 million has been awarded to the Health Resources Services Administration (HRSA) to support hospital preparedness efforts. The Office of Emergency Preparedness (OEP) will award approximately $14 million to continue to build metropolitan medical response systems (MMRS) in cities across the country.

Office of Public Health Preparedness (OPHP)

OPHP directs activities of HHS relating to protecting the civilian population from acts of bioterrorism and other public health emergencies. OPHP acts as the department's liaison with the Office of Homeland Security and serves as the principal department representative to other federal agencies and the private sector in all matters related to bioterrorism and other public health emergencies. OPHP is responsible for implementing a comprehensive HHS strategy to protect the civilian population from acts of bioterrorism and other public health emergencies.

Centers for Disease Control and Prevention (CDC) Office of Terrorism Preparedness and Response

This office is responsible for oversight of all potential terrorist threats—biological, chemical, radiological, and nuclear. CDC established this office to ensure the rapid development of federal, state, and local capacity to address potential terrorism events. The program integrates planning and training to facilitate the development of core competencies and capacities in public health preparedness, including surveillance, epidemiology, rapid laboratory diagnosis, emergency response, and information systems.

Disease Surveillance and Public Health Network. To better detect and respond to a wide range of infectious disease threats, including possible bioterrorist incidents, CDC is upgrading the nation's public health laboratory and epidemiological capacity. It also is enhancing training and expanding communications resources for state and local health agencies. This includes the capacity to detect outbreaks of illness that might have been caused by terrorists, improved laboratory identification and characterization of causal agents for disease outbreaks, and improved electronic communications among public health and other officials regarding outbreaks and responses to them.

The CDC National Pharmaceutical Stockpile.[5] A release of selected biological or chemical agents targeting the U.S. civilian population will require rapid access to large quantities of pharmaceuticals and medical supplies. Such quantities may not be available immediately unless special stockpiles are created. No one can anticipate exactly where a terrorist will strike, and few state or local governments have the resources to create sufficient stockpiles on their own. To address this, the CDC National Pharmaceutical Stockpile (NPS) program has developed a national repository of life-saving pharmaceuticals and medical supplies that can be delivered to the site of a chemical or biological terrorism event. All states are developing plans and protocols to effectively receive and distribute these vital supplies.

The NPS is composed of pharmaceuticals, vaccines, medical supplies, and medical equipment to augment depleted state and local resources used in responding to terrorist attacks and other emergencies. Stored in strategic locations around the U.S., these packages can be delivered rapidly anywhere in the country.

Following the federal decision to deploy, the NPS typically will arrive by air or ground in two phases. The first-phase shipment is called a "12-hour Push Package." It is called this because it will arrive in 12 hours or less; a state need only ask or "push" for help; and it contains a complete package of medical matériel. The package includes nearly everything a state will need to respond to a broad range of threats. Inventory supplies called vendor managed inventory, or VMI packages, are available. VMI packages can be tailored to provide pharmaceuticals, vaccines, medical supplies and/or medical products specific to the suspected or confirmed agent or combination of agents.

[5] National Pharmaceutical Stockpile, Centers for Disease Control and Prevention. Go to: www.bt.cdc.gov

A CDC team of five or six technical advisors also will deploy at the same time as the first shipment. Known as a technical advisory response unit (TARU), this team is composed of pharmacists, emergency responders, and logistics experts who will advise local authorities on receiving, distributing, dispensing, replenishing, and recovering NPS matériel.

The NPS program was tested in the real-life terrorist attacks of September 11. New York State and local officials requested large quantities of medical matériel and logistical assistance. With the support of local and state public health and emergency response officials, all facets of the New York operation performed exactly as intended. The NPS program also provided pharmaceutical and logistical support to areas affected by the anthrax attacks in October and November 2001.

As part of CDC's bioterrorism response, CDC will transfer authority for the NPS matériel to the state and/or local authorities once it arrives at the airfield. State and/or local authorities will then repackage and label bulk medicines and other NPS matériel according to their own terrorism contingency plans. CDC's technical advisors will accompany the NPS to assist and advise state/local officials in putting the NPS assets to prompt and effective use.

When and How is the NPS Deployed? The decision to deploy NPS assets may be based on evidence showing the overt release of an agent that might adversely affect public health. It is more likely, however, that subtle indicators, such as unusual morbidity and/or mortality identified through the nation's disease outbreak surveillance and epidemiology network, will alert health officials to the possibility (and confirmation) of a biological or chemical terrorism incident. To receive NPS assets, the affected state can directly request their deployment from the CDC director. Once requested, the CDC director has the authority, in consultation with the Surgeon General and HHS Secretary, to order NPS deployment.

Metropolitan Medical Response System (MMRS)

Because of the rapid response time required in countering weapons of mass destruction (WMD) terrorist incidents, HHS launched the metropolitan medical response system (MMRS), composed of a highly trained, readily deployable, and fully equipped local response team that can address WMD effects on human health. The MMRS will coordinate and supplement existing emergency response capabilities and develop a comprehensive response and health management plan to deal with any mass casualty incident in a metropolitan area. The system also identifies and remedies gaps in resources and training for such incidents.

U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID)

This institute is a subordinate laboratory under the U.S. Army Medical Research and Material Command. It can respond to terrorist threats, accidents, or incidents involving biological agents or materials. The USAMRIID Aeromedical Isolation Team is composed of specially trained physicians, nurses, medical assistants, and laboratory technicians who can provide care and transport assistance for patients with diseases caused by biological warfare agents or with infectious diseases requiring high containment.

HHS, Office of Emergency Preparedness (OEP)

OEP is an office within HHS with departmental responsibility for managing and coordinating federal health, medical, and related social services and recovery to major emergencies and federally declared disasters. These include natural disasters, technological disasters, major transportation accidents, and terrorism. Working in partnership with the Federal Emergency Management Agency (FEMA) and the federal interagency community, OEP serves as the lead federal agency for health and medical services within the federal response plan. OEP also directs and manages the National Disaster Medical System (NDMS), a cooperative asset-sharing partnership among HHS, the U.S. Department of Defense (DoD), the U.S. Department of Veterans Affairs (VA), FEMA, state and local governments, private businesses and civilian volunteers. OEP also is responsible for federal health and medical response to terrorist acts involving WMD.

Health Resources and Services Administration (HRSA)

HRSA provides health resources to medically underserved populations. HRSA supports a nationwide network of 643 community and migrant health centers and 144 primary care programs for the homeless and residents of public housing. The network serves 8.1 million Americans each year. HRSA also works to build the health-care workforce, maintains the National Health Service Corps, oversees the nation's organ transplantation system, works to decrease infant mortality and improve child health, and provides services to people with AIDS through the Ryan White CARE Act programs.

Disaster Medical Assistance Team (DMAT)

DMAT is a volunteer team organized under the National Disaster Medical System (NDMS) through the U.S. Public Health Service (USPHS) to provide emergency medical care and to augment local medical capabilities during times of disaster. Disasters may be earthquakes, hurricanes, epidemics, explosions, floods, or other devastating events. DMATs are typically composed of 100 to 150 organized and trained medical professionals and support staff. In a disaster, a smaller team of about 35 will deploy as a unit to provide medical and health care to disaster victims.

A DMAT may be requested by any state following a disaster so large that the President declares it a disaster area. This procedure is based on the federal philosophy that states and local jurisdictions must use their own resources prior to requesting federal assistance. Once it has been determined that the event has or can overwhelm local resources, a state's emergency management agency may request assistance through NDMS. NDMS staff will want to know two things: the number of patients and type of injuries. This information, along with location and general conditions, will determine which DMATs are sent. In addition to the DMATs, the OEP also will deploy a management support team (MST) to provide managerial and logistical support to a group of three to five DMATs. The MST and DMATs can function as a self-contained health and medical services provider for as long as supplies and relief personnel last. There are DMATs throughout the U.S.

FOR MORE INFOMATION

U.S. Department of Health and Human Services. Go to: **www.hhs.gov**

Office of Emergency Preparedness. Go to: **www.ndms.dhhs.gov**

Centers for Disease Control and Prevention. Go to: **www.bt.cdc.gov**

Health Resources Services Administration—Hospital Preparedness. Go to: **www.hrsa.gov/bioterrorism.htm**

CHAPTER 6

Agroterrorism

Though it garners less attention than most other terrorism threats, attacks against the nation's food supply and other parts of the agricultural system can be as damaging to the nation as attacks on more conventional targets and harder to detect. As states assess their security needs, security officials must consider vulnerabilities in the agricultural sector. The two most likely threats involve the release of chemical agents, such as liquid mercury or cyanide, or the release of biological agents in the form of viruses, fungi, or bacteria, such as foot-and-mouth disease (FMD).

In preparing to respond to an agroterrorism threat, governors should:

- ★ include agroterrorism response in state emergency plans, assessing the need for improved state surveillance networks, state biosecurity procedures, multistate response agreements, crisis communication plans, and criminal terrorism statutes;
- ★ clarify the roles of key officials in an agroterrorism response, removing redundancies and providing outlets for reporting outbreaks;
- ★ establish relationships with appropriate federal agencies, local authorities, producers, and veterinarians; and
- ★ educate producers, veterinarians, and other members of the state agricultural network about reporting mechanisms, procedures, and state contacts.

THE NATURE OF THE THREAT

Agroterrorism is a deliberate attack by motivated hostile individuals or groups against agricultural targets. Such attacks would commonly employ chemical and biological agents but could include conventional or even nuclear weapons. Agroterrorism differs from other forms of terrorism because, historically, it has been directed primarily toward creating economic damage rather than the destruction of human life. However, that assumption probably is no longer valid. Though chemical and biological agents targeted directly at people represent the greatest threat, many of the classic state-sponsored biowarfare agents are zoonotic (i.e., they are communicable between animals and humans) and can inflict collateral damage in people and in the agricultural sector. Therefore, agroterrorism represents a serious threat to human life as well as to the U.S. economy and the nation's food supply.

In the last century, 21 incidents of nonstate-sponsored agroterrorism have occurred. Of these, five took place within the continental United States, and all were of a small scale.[6] For instance, in 1997, a man in Berlin, Wisconsin, poisoned a business competitor's feed supplies with the

[6] Jason Pate and and Gavin Cameron, "Covert Biological Weapons Attack Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture," BCSIA Discussion Paper 2001-9, ESDP Discussion Paper ESDP-2001-05, John F. Kennedy School of Government, Harvard University, August 2001, p. 7.

fungicide folpet. Previous attacks mostly have involved chemicals, using such agents as cyanide and liquid mercury to infect small quantities of crops or animal feed. However, biological agents pose a potentially more serious threat. FMD and Mad Cow Disease could paralyze the U.S. economy if not handled quickly and carefully. The United Kingdom's recent experiences with controlling FMD and eradicating it from the livestock population suggest the difficulties a state would endure if attacked. Further, the repercussions of such a communicable disease linger long after it is eradicated through the economic "ripple effects" from consumer fears.

FOR MORE INFORMATION

Go to: **www.cns.miis.edu/research/cbw/agromain.htm**

ASSESSING POTENTIAL THREATS

The primary delivery vehicle for agroterrorism is either a chemical or biological agent. Fast-acting and seriously disruptive chemical agents can be used to poison crop yields or livestock. Agents previously used by terrorists have included liquid mercury, sodium cyanide, Agent Orange, and other crop-killing chemicals.[7] However, in the U.S. regulatory environment, such agents rarely go unnoticed. Generally, chemical agents represent a less likely agroterrorist weapon because they require large manufacturing facilities, are difficult to transport and handle, and do not reproduce on their own like some biological agents.

Biological agents can be as effective in despoiling crop or livestock stores as chemical agents and they can be more dangerous, given their penchant to spread and multiply. Agents like FMD are highly contagious and require immediate quarantine or destruction of infected and potentially infected animals.

Agroterrorist biological agents usually come in the form of viruses, fungi, or bacteria. Viruses typically target animals, whereas plants—possessing formidable cell walls—often are impervious to viruses. Plants, however, are subject to fungal or bacterial attack.[8]

From 1951 to 1969, the United States' biological weapons program produced three main biological agents targeted at plant destruction, and all three were fungi. Fungi can be quite effective. For example, the spores of wheat rust can devastate wheat yields. Fungi require certain meteorological conditions—such as wind speed, pressure, and humidity—for an attack

[7] Jason Pate and Gavin Cameron, "Covert Biological Weapons Attack Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture," BCSIA Discussion Paper 2001-9, ESDP Discussion Paper ESDP-2001-05, John F. Kennedy School of Government, Harvard University, August 2001, p. 7.

[8] Anne Kohnen, "Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture," BCSIA Discussion Paper 2000-29, ESDP Discussion Paper ESDP-2000-04, John F. Kennedy School of Government, Harvard University, October 2000, p. 16-19.

to be effective. Bacteria, on the other hand, are less sensitive to meteorological conditions and can attack plants via water or air. However, bacterial agents generally do not spread as effectively as fungi spores.[9]

Communicable diseases, like FMD, represent the greatest threat to U.S. agriculture. Should an outbreak of FMD occur, for example, vaccinations of uninfected animals only would keep them from acquiring the disease and would not preclude them from being carriers. Moreover, the current vaccine may not be effective against a terrorist-modified strain of FMD. For these reasons, quarantine of affected and target populations is an absolute necessity to control the spread of a communicable agent. Additionally, primary and secondary animal populations affected by the disease may need to be sacrificed. For example, not only cattle but local deer and swine populations would be affected by an outbreak of FMD.

FOR MORE INFORMATION

Go to: **www.ianrhome.unl.edu/inthenews/agroterrorism.shtml**

The primary prophylaxis against the unnecessary spread of a virus is initial quarantine of new farm animals or other stock animals. It is recommended that any new animals be separated from other herds of animals for a period of several days. This separation would prevent the spread of most diseases. However, an alarming report released by the USDA suggests that 80 percent of farms do not practice these procedures.[10] The U.S. Department of Agriculture (USDA) is taking steps in the wake of September 11 to correct these problems.

FOR MORE INFORMATION

Go to: **www.aphis.usda.gov/oa/bse**

Another significant consideration in a communicable agent outbreak relates to the movement of people and commerce. During the FMD disaster in the United Kingdom, tourism in rural areas had to be restricted severely through traffic blockades and, in some cases, tourists themselves had to be quarantined or decontaminated. States should plan to respond similarly

[9] Anne Kohnen, "Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture," BCSIA Discussion Paper 2000-29, ESDP Discussion Paper ESDP-2000-04, John F. Kennedy School of Government, Harvard University, October 2000, p. 19.

[10] Ibid, p. 22-23

in the event of a communicable outbreak, recognizing not only that populations need to be controlled but that access to hospitals, airports, industry, military bases, and other key sites must be accommodated.

An additional issue concerns the communicability of agents from animals to humans or interspecies transmissions, known as zoonotics. Typically, viruses from animals do not affect humans in the same fashion. However, a number of animal-borne viruses can infect humans; these include the West Nile virus and Bovine Spongiform Encephalopathy (BSE), or as it is commonly called Mad Cow Disease. BSE is caused by tiny damaged proteins called prions. BSE has caused numerous fatalities in humans in the form of new variant Cruetzfeld-Jakob Disease, a fatal neurological ailment contracted by eating BSE-infected processed beef. Additionally, new variants of other viruses like the Nipah virus in Malaysia and the increasingly robust West Nile Virus that has emerged on the East Coast argue for continued attention to zoonotics and their effects, including the development of surveillance techniques, diagnostics, vaccines and treatments, response assets, and other effective mitigation strategies.[11]

FOR MORE INFORMATION

Go to: **www.aphis.usda.gov/oa/bse**

FEDERAL RESPONSES

The federal government, through the USDA, has substantial research capability, extensive resources, and expertise to assist states in an agroterrorism incident. The USDA can mobilize immediately to address either an animal disease outbreak or an attack on crops.

Animal Disease Outbreak

USDA national teams can be assembled and mobilized within 36 hours or faster in an animal disease outbreak. The typical timeline for response is as follows:[12]

- **1.** A farmer or herd manager notices a sick animal or animals and contacts the local veterinarian.
- **2.** The veterinarian diagnoses a domestic disease or suspects an abnormality.
- **3.** The veterinarian notifies the state veterinarian or Animal and Plant Health Inspection Service (APHIS) area veterinarian in charge.

[11] Ibid, p. 20-21.

[12] Timeline provided by the Animal and Plant Health Inspection Service.

★ **4.** A foreign animal disease diagnostician (FADD) visits the premises and begins an investigation as soon as possible. The FADD may be a state or federal veterinary medical officer. The FADD works with labs to describe the situation and takes the appropriate samples to diagnose the disease.

★ **5.** An early response team (ERT) may be called upon to characterize an unconfirmed or emerging disease outbreak or to describe the pathogenesis and epidemiology of the disease. The ERT recommends further action or controls.

★ **6.** If it is determined that an outbreak is occurring, local and state resources, along with USDA resources in that state, will be used to address the outbreak. If a state needs greater resources, a national APHIS team will respond and integrate with the state's response using incident command structure (ICS) principles. Its roles are to give additional technical support, coordinate national communication, and manage national consequences and federal response resources.

FOR MORE INFORMATION

Go to: **www.aphis.usda.gov**

Plant Disease Outbreak

The Surveillance and Emergency Program Planning and Coordination (SEPPC) section of the USDA has responsibility for early detection and rapid response to plant pest outbreaks and eradication. A typical response resembles the following.

★ **1.** A producer recognizes a problem with crops, takes a sample, and submits the sample for diagnosis or identification to a local agricultural diagnostic center.

★ **2.** If the center recognizes the pest as being particularly serious or new, it will notify the state plant health authority.

★ **3.** If an emergency plan already exists, it is implemented by SEPPC and other regional response teams (RRTs), state personnel, and industry groups.

★ **4.** If the species is a new one, USDA calls upon the New Pest Advisory Group to assess the significance of the pest and to determine a response plan. This process takes at most 21 days for pests that are not considered critical, or significantly less for a major pest that is likely to spread quickly and that may have significant economic or other effects.

★ **5.** A RRT can be at the site of disease in 48 hours.

Although federal assistance is a vital link in responding to agroterrorism, states, counties and local entities remain the primary responders in an outbreak containment, along with producers and other members of the private sector. Further, federal assistance may be delayed or nonexistent in some crises. As such, the state plan for responding to acts of agroterrorism must be robust. The top priorities for states should be ensuring that the state plan addresses all variables, including surveillance and quarantine; clarifying the roles of various actors in the emergency management scheme (i.e., who acts as the incident commander, the state agricultural director or the homeland security director?); and formulating procedures for the concise dissemination of information. Washington State recently completed a communications plan that outlines the roles of state authorities in managing a FMD outbreak. Additionally, states should consider formulating compacts with other states to ensure coordinated action in a cross-border outbreak. Iowa recently released its homeland security initiative addressing the importance for a multistate compact to combat such outbreaks.

WHAT GOVERNORS SHOULD DO

State emergency management authorities should conduct an appraisal of their respective emergency planning structures. Among other things, state authorities should determine whether their agricultural system has the necessary safeguards in place, including response capability, compacts with neighboring states, resources for identification and surveillance of animal and plant pest outbreaks, and quarantine authority for the governor and other state agricultural actors.

Address Agroterrorism in State Emergency Management Plans

Regardless of whether a state has a significant agricultural base or not, all states need to prepare to respond to agroterrorism because many agroterrorist agents are highly communicable and capable of affecting regional areas quickly with devastating results. In state response plans, roles need to be clarified, state surveillance ability assessed, and biosecurity procedures enforced. For example, Kansas addressed the issue of procedural clarity by including a special section of its state emergency procedures to cover acts of bioterrorism and agroterrorism, including a section that outlines the roles of all levels of expertise and jurisdictions from townships to federal agencies.

In formulating state plans, a governor should:

- ★ determine the status of state agroterrorism surveillance assets, including on-site monitoring from plant pathologists and field veterinarians, databases that are accessible to state responders and linked to state health or veterinarians' offices and that identify locations and types of pathogens, and rapid diagnostic tools designed to determine quickly the type of disease being tested;
- ★ ensure producers comply with biosecurity guidelines relating to initial multiday quarantines of new animals and limiting the planting of a single type of crop in too high a concentration. Both practices prevent the unnecessary spread of disease;

- ★ engage neighboring states by entering into agreements to coordinate responses to agroterrorism where the outbreak crosses borders, including exercises that test state-to-state coordination;
- ★ prepare communication plans that address outbreaks by providing information to the public about what the outbreak is, what is being done, and how to avoid being harmed by the outbreak or how to avoid making the outbreak worse; and
- ★ consider legislation that renders criminal forms of agroterrorism, including tampering with food-producing plants, animals, or plants.

Develop a Clear Communication Process

There should be a clear process for communication among city and local authorities and state managers, as well as with producers and the private sector. Those responding to the initial outbreak, including veterinarians, producers and others, should know who to contact and when in the event a potential plant or animal disease is discovered. Further, coordination with members of the private sector during an outbreak will be vital, especially in assuring that uniform terminology and trustworthy, salient information is disseminated. Pre-event communication plans best address this important issue. Washington State's "Public Notification Plan for Foot-and Mouth Disease" embodies many of the key points discussed above. It clarifies the roles of state agricultural responders to avoid duplicative or conflicting efforts, identifies state, local, and federal points-of-contact, and provides sample messages and news releases in the event of an outbreak.

Utilize Available Federal Resources

Governors also will want to use the available expertise of the federal government. The USDA leads the attack on safeguarding farms, factories, and other related facets of the agricultural network in the U.S. Governors should ensure that clear channels of communication also exist at this level, including points of contact and developed relationships. Additionally, the federal government has provided nearly $2 million in grants to 32 states to help bolster emergency animal disease prevention, preparedness, response, and recovery systems. In the fiscal 2003 budget, USDA has pledged $11.6 billion to support rural community development programs; $2.3 billion to support ongoing research on such deadly outbreaks as BSE and FMD; and $905 million to support the Food Safety and Inspection Service program. For more information on available grants from the USDA for states, see the *Catalog of Federal Domestic Assistance*, which outlines the procedures, eligibility, and deadlines for all forms of U.S. domestic funding.

FOR MORE INFORMATION

Go to: **www.cfda.gov/public/browse_by_typast.asp**

Educate Members of Agricultural Community

First responders to acts of agroterrorism are often producers, veterinarians, and other private-sector members. Governors should disseminate, through state agencies and participating private entities, educational information and resources designed to provide outlets for quick reporting of possible outbreaks, as well as procedures that could be taken immediately by first responders to reduce the harmful effects of an agroterrorist event. North Carolina has amassed an impressive array of information on its state department of agriculture Web site, including background pieces on FMD, West Nile, and other concerns, and points of contact in the case of an outbreak.

FOR MORE INFORMATION

Go to: **www.ncagr.com/vet/DiseaseAlerts.htm**

Strategic Partnerships

Governors should consider partnerships with educational institutions as a key asset in preparing to respond to agroterrorism incidents. Academic institutions, particularly land grant universities, have unique missions and capabilities that make them important potential partners in the agroterrorism arena. Basic and applied research programs in plant and animal diseases, especially those that address regional agricultural vulnerabilities, can provide critical information and assets to state leadership. The existing agricultural extension infrastructure that already reaches down to the producer level should be refined to complement education and surveillance programs for plant and animal disease. Agricultural subject matter expertise found in academic institutions can greatly strengthen state agroterror programs by providing focused research on plausible threats and technical problems, veterinary and plant diagnostics, education, and expert consultation. Land grant institutions, such as Kansas State University and Texas A&M have created research centers to address emerging threats of agroterrorism. States should maximize the potential collaborative and cooperative interaction with these stakeholders.

FOR MORE INFORMATION ON KANSAS STATE UNIVERSITY'S RESEARCH PROGRAM

Go to: **www.vet.ksu.edu/depts/fahm**

GOVERNOR'S CHECKLIST FOR AGROTERRORISM PREPAREDNESS

- ✔ Ensure that state emergency management guidelines include agriculture as a potential target, and have procedures for addressing possible attacks, including a robust surveillance network, proper biosecurity procedures, compacts with other states for cross-border outbreaks, crisis communication plans, and criminal terrorism statutes;
- ✔ provide clear channels of communication among local authorities, producers, veterinarians, and state authorities;
- ✔ establish relationships with federal authorities, taking advantage of federal programs and grants assisting in homeland security; and
- ✔ educate the state agricultural network on important aspects of protecting against agroterrorism.

FOR MORE INFORMATION

American Veterinary Medical Association. This Web site provides up-to-date information on issues related to animal disease. Go to: **www.avma.org**

Belfer Center for Science and International Affairs. This Web site provides policy background on agroterrorism response. Go to: **www.ksgnotes1.harvard.edu/BCSIA/Library.nsf/pubs/ESDP4Kohnen**

Center for Nonproliferation Studies. Go to: **www.cns.miis.edu/research/cbw/agromain.htm**

The Farm Bureau. Go to: **www.fb.com/fbn/html/agriculturalterrorism.html**

National Biosecurity Resource Center for Animal Health Emergencies. Go to: **www.biosecuritycenter.org/nbrctoc.htm**

U.S. Department of Agriculture. Go to: **www.usda.gov**

CHAPTER 7

The Threat of Chemical Weapons

The United States is part of a world in which the proliferation and use of chemical weapons are growing. While the potential exists for terrorists to build chemical weapons, the enormous complexity of creating a chemical weapon makes such a scenario less likely than an intentionally triggered chemical release from an industrial facility. Additionally, chemical weapons are tactical weapons and are limited in their ability to cover large land areas.

However, chemical facilities in high-population areas that use and store hazardous chemicals are attractive targets for terrorists. These facilities provide relatively easy access to chemicals at locations from which a significant chemical release could harm large numbers of people. The Agency for Toxic Substances and Disease Registry published a study in 1999 evaluating the chemical industry's vulnerability to terrorism. It reported that industrial chemicals provide terrorists with "effective and readily accessible materials to develop improvised explosives, incendiaries, and poisons."[13] Several industrial facilities are taking precautions to reduce chemical stockpiles and prevent theft of materials. However, most industry efforts have not focused on preventing the type of attack that would destroy the plant and cause toxic releases.[14]

Because plausible threats exist against chemical facilities, governors should:

- ensure that state and local health, fire, police, safety, and other governmental officials can obtain detailed information about the identity, characteristics, and quantities of hazardous substances and chemicals used and stored in communities within their jurisdictions;
- assess their state's preparedness and response capabilities to handle a chemical attack;
- ensure that the state emergency management plan addresses all chemical-related acts of terrorism, including the deliberate targeting of a chemical facility, chemical spills, accidents, and the use of chemical agents as weapons;
- ensure that the state has the necessary resources for responding to a chemical attack, including hospital facilities, first responders' capacity, and emergency authority to evacuate;
- develop resources for response, assess training needs, and prepare responders to address a major chemical release;
- develop a crisis communications plan and communication capabilities (including alerts and notifications);
- appoint a state emergency response commission (SERC);
- establish relationships with key members of the private sector, including operators and owners of chemical facilities and hospitals;
- conduct drills and exercises to prepare for a chemical weapons attack; and
- become familiar with the Chemical Stockpile Emergency Response Program and with the National Contingency Plan and the resources they provide to state authorities.

[13] Eric Pianin, "Toxic Chemicals' Security Worries Officials," *Washington Post*, November 2001.

[14] Jeremiah Baumann, *Protecting Our Hometowns, Preventing Chemical Terrorism in America, A Guide for Policymakers and Advocates*, U.S. PIRG Education Fund, 2002.

BACKGROUND: HISTORY OF CHEMICAL WARFARE

Chemical agents are poisonous gases, liquids, or solids that have toxic effects on people, animals, or plants. Chemical weapons can disable or kill humans upon contact and are characterized by the rapid onset of medical symptoms and easily observed signatures, such as colored residue, dead foliage, pungent odor, and dead animals and insects. Most chemical agents cause serious injuries or death. They are classified by their effects: nerve, blood, choking or blister. These weapons kill by destruction or disruption. For example, the infamous mustard gas used in World War I essentially burns away parts of the respiratory system.

Because of the terrible toll on the battlefield from mustard gas—including the long-term effects on survivors—the use after World War I of such gases has been rare. Fear of retaliation has been a motivating factor as well. During the 1930s, both Italy and Japan used limited chemical warfare against their opponents (Ethiopia and China, respectively) who could not respond in kind. Most major powers stockpiled chemical weapons during World War II but refrained from first use. In the 1980s, Iraq under Saddam Hussein used chemical weapons during the 1980–1988 Iran-Iraq war; he also used such weapons against the Kurdish people in his own country.

The threat of chemical weapons came to the forefront in 1995 when the Japanese cult Aum Shinrikyo released the nerve agent sarin in a Tokyo subway. Formed in 1987, the cult was led by Shoko Asahara, a former health food dealer who lost his bid for political office in the late 1980s. After his defeat, Asahara increasingly grew antigovernment, wanting to separate his growing cult from the government of Japan. Aum Shinrikyo's followers grew to encompass tens of thousands of members—not just in Japan, but also in Korea and Russia. The cult amassed a huge fortune and developed a significant armaments capability. This capability included the ability to manufacture chemical and biological weapons. The cult worked throughout the 1990s to develop various agents, including botulinum, anthrax, and sarin.

On March 20, 1995, Aum Shinrikyo members activated crude devices on the Tokyo subway designed to release sarin into the underground structure. The episode killed 12 people and as many as 5,000 received hospitalization of some kind. It was the first well-publicized chemical or biological terrorist incident, and it stunned the world. Defense experts in the U.S. realized that chemical terrorism was a reality and we needed to reassess our vulnerability to such an attack and take precautions.

The Impact of Chemical Weapons

Chemical agents are generally stored in liquid form and disseminated as an aerosol or gas. To be effective, chemical agents must be dispersed in sufficient quantity to create high enough concentrations in the atmosphere to cause serious damage. These agents are affected by weather conditions, such as temperature, wind speed and direction, and humidity and air stability, which make it difficult to achieve sufficient concentrations to be effective in an open-air environment.

Chemical agents also are classified as either persistent or nonpersistent. A persistent agent remains in the target area for a long period of time. Hazards from both vapor and liquid may

exist for hours, days or, in exceptional cases, weeks after dispersion of the agent. A nonpersistent agent will remain in the target area for a relatively short period of time. The hazard, which is predominantly posed by vapor, will exist for minutes or, in exceptional cases, hours after dispersion of the agent.

Nerve gases—sarin and VX—disrupt the chemical processes through which one nerve cell communicates with another. Severity of injuries depends on the type and amount of the chemical agent used and the duration of exposure. Unlike biological and radiological weapons, chemical agents act quickly. Protection from these agents requires full respiratory and skin protection.

Falling somewhere between chemical and biological agents is ricin. Ricin is a naturally derived substance made from processing castor beans, but its effects are essentially chemical in nature, rather than pathogenic. Ricin, which causes organ failure, is extremely deadly, though most of our knowledge is based on animal studies and nonfatal accidental human exposures. There is currently no known antidote or vaccine, although some of the effects of ricin may be treated by normal medical procedures. Injected, as opposed to ingested, ricin is thought to be 100-percent fatal.

Current Threat of Chemical Weapons

Experts believe that state-sponsored terrorists are the most likely to create and use chemical weapons because they have the resources of a state supporting them. They also often have clear targets (their state's enemies). However, a state may be subject to retaliation for an attack, which may provide a serious deterrent. The state sponsors might also be wary about providing such technology to a group over which they lack total control.

Nationalistic or ethnic terrorists also may be inclined to use chemical weapons as they would have less to fear by retaliation because their acts would be directed against their own government, which would be less likely to retaliate severely against its own citizens than those of another state. A secondary factor, but still of major importance, is that many such movements depend to some extent on external (i.e., international) support for their continued existence. It is unlikely such support would continue after the use of chemical weapons.

Chemical Targets in America. Sites where a terrorist could trigger a chemical release are numerous and widespread in the U.S. Approximately 15,000 facilities in the U.S. have submitted risk management plans (RMPs) to the U.S. Environmental Protection Agency (EPA) as required under the 1990 Clean Air Act Amendments. The Risk Management Program is EPA's primary chemical accident prevention program. Nearly 5,000 of these facilities have a maximum of at least 100,000 pounds of chemicals on site that are considered extremely hazardous. At least 100 facilities each store more than 30 million pounds of extremely hazardous substances. The potential for a catastrophic chemical release is widely distributed: every state in the U.S., except Vermont, has at least one facility storing more than 100,000 pounds of extremely hazardous substances.[15]

[15] Jeremiah Baumann and Paul Orum, U.S. PIRG Education Fund and Working Group on Community Right to Know, *Accidents Waiting to Happen: Hazardous Chemicals in the U.S. Fifteen Years After Bhopal*, December, 1999.

Facts about Nerve Gases

★ Sarin. Sarin is a highly toxic nerve gas. It made headlines when members of a Japanese cult released sarin in a Tokyo subway, killing 12 people. Sarin can cause death within minutes of exposure. It enters the body through the eyes and skin. Signs and symptoms vary but include a runny nose, watery eyes, dimmed vision, drooling, sweating, difficulty in breathing, nausea, twitching, and headache. Sarin kills by paralyzing the muscles used for breathing.

★ Mustard gas. Mustard gas was used in World War I and World War II to sicken soldiers, and it reportedly was used in the Iran-Iraq war in the mid-1980s. Mustard gas is yellow to brown in color. It has a garlic-like smell. The gas irritates the eyes and causes skin burns and blisters. When inhaled, it can cause coughing, bronchitis, and long-term respiratory problems. Mustard gas has been linked to later development of lung cancer in survivors. Exposure to a large amount may be fatal. There's no antidote to mustard gas exposure.

★ Chlorine. Chlorine is a disinfectant used in drinking water and in swimming pools. In its pure form, it is a greenish-yellow gas with a pungent odor. Chlorine is corrosive to the eyes and skin. It can cause blurred vision and burns. Inhaled chlorine can cause labored breathing and the buildup of fluid in the lungs. High exposure levels may result in death.

★ Phosgene. This colorless gas is normally used in chemical manufacturing. If inhaled at high concentrations long enough, it causes severe breathing problems and fatal lung congestion. It was used in World War I as a poison gas. Although there's no known treatment for phosgene exposure and mortality is high, some people exposed to phosgene do survive.

★ Hydrogen cyanide. Hydrogen cyanide is a colorless gas or liquid. Exposure irritates the eyes, the skin, and the respiratory tract. Inhalation causes confusion, drowsiness, and shortness of breath. The substance can affect the central nervous system and lead to death.

WHAT GOVERNORS SHOULD DO

The proliferation of chemical facilities that use and store hazardous chemicals and that are located in high-population areas are attractive targets for terrorists. These facilities provide relatively easy access to chemicals at locations from which a significant chemical release could harm large numbers of people. Additional challenges for governors are the constantly increasing number and variety of hazardous substances and the many routes of exposure to them, which make it difficult and expensive to adequately monitor and detect adverse health effects.

There are several steps a governor can take to prepare for acts of chemical terrorism. Many of the necessary preparations focus on response to attacks rather than prevention, largely because of the difficulty in detecting chemical agents once they have been acquired by terrorists. Governors should:

★ require detailed information from chemical facilities;

★ include chemical emergency response in state emergency plans;

- ★ develop resources for response;
- ★ develop a crisis communications strategy;
- ★ appoint a state emergency response commission;
- ★ build relationships with the private sector;
- ★ conduct drills and exercises;
- ★ know the chemical stockpile emergency preparedness program; and
- ★ know the national contingency plan.

Require Detailed Information from Chemical Facilities

State and local health, fire, police, safety, and other governmental officials should require detailed information about the identity, characteristics, and quantities of hazardous substances and chemicals used and stored in communities within their jurisdictions. This will allow them to adequately plan for and respond to emergencies and to enforce compliance with applicable laws and regulations concerning these substances.

Governors should require information about security at chemical facilities and ensure their security forces are well trained and in sufficient numbers to repel possible attacks. Although security is primarily the responsibility of the facility owners and operators, following the attacks of September 11, some states temporarily augmented security at facilities with National Guard units.

Include Chemical Emergency Response in State Emergency Plans

State emergency management plans must address all chemical-related acts of terrorism, including the deliberate targeting of a chemical facility, chemical spills, accidents, and the use of chemical agents as weapons. These plans should include specific points of contact for the injured as well as the responding agencies. A designated lead response group, such as a state hazardous materials (HAZMAT) team should direct immediate action in responding to the release of chemical agents or a chemical spill. Otherwise the potential exists for the emergency agency that first responds to the hazardous material release to fail to identify the material or exercise the right precautions for handling the material. This could result in the use of incorrect emergency procedures, thus endangering both members of the emergency agency and the public.

Develop Resources for Response

The lead response agency, whether it is the state emergency management agency, National Guard, or other designated agency, must have proper equipment, including mobile decontamination units and protective suits. Exposure to chemical agents can be fatal. Specific treatments and antidotes, such as atropine, are available for some exposures, while only supportive measures can be provided for others. Emergency kits with appropriate treatments and antidotes should be available and stocked by hospitals, ambulances, and other emergency personnel. Furthermore, the public health sector—a vital component of a state's response capability—needs to be properly trained and equipped as well.

Develop a Crisis Communications Strategy

A governor should ensure he or she has a strategy for communicating with the public during a chemical attack or release (Chapter 2 discusses crisis communication in detail). The importance of the governor in communicating comprehensive, current information to the public in the aftermath of such an attack cannot be overemphasized, even if it is disturbing information. It is also important for the governor to have medical and scientific leaders to be trained in the difficult skill of media communication. The potential for positive or negative impact is so great that governors must make this a priority.

Appoint a State Emergency Response Commission

The federal Superfund Amendments and Reauthorization Act (SARA) became law in 1986. Title III of these SARA provisions is also called the Emergency Planning and Community Right-to-Know Act (EPCRA). SARA Title III requires states to:

- ★ promote outreach for developing local emergency preparedness programs to respond to chemical releases;
- ★ receive reports from the regulated community; and
- ★ organize, analyze, and disseminate the resulting information on hazardous chemicals to local governments and the public.

One SARA Title III provision requires a governor to appoint a state emergency response commission (SERC). The SERC, through implementation of emergency planning and community right-to-know laws and through establishment and support of its local emergency planning committees (LEPCs), assists in chemical emergency planning, provides public access to chemical data, raises public awareness of chemical risks, and encourages public participation in local chemical safety issues. The SERC typically consists of a chair, co-chair, executive secretary, and members appointed by the governor to represent private industry, local and state government, media, fire and medical services, the legislature, and the general public.

It is in the public interest to establish a comprehensive program to disclose information about hazardous substances in the workplace and the community and to provide a procedure for citizens to get this information. Individuals are often able to detect and to minimize effects of exposure to hazardous substances if they are aware of the identity of the substances and the early symptoms of unsafe exposure. Governors should ensure that their citizens have information on the full range of risks in their communities so they can make reasoned decisions and take informed action concerning their employment and their living conditions.

Build Relationships with the Private Sector

The nationwide regulated community of manufacturers and nonmanufacturers of hazardous chemicals must report the following to their state SERC and LEPCs: their emergency chemical releases; their material safety data sheets (MSDS); their facility hazardous chemical inventories (Tier I and Tier II reports); and toxic chemical releases to the air, land, or water (toxics release inventory). Because of this activity, businesses have reassessed their chemical inventories and their manufacturing processes.

More businesses are working cooperatively with local governments to plan for and prevent an accidental chemical release. Governors should build relationships with the private sector as an intentional chemical release or accident will undoubtedly include members of the private sector, either in a response capacity or communications capacity. By opening channels of communication, a governor will ensure an effective response by the private sector to acts of chemical terrorism. Additionally, a close working relationship between the state and the private sector will avoid the release of potentially confusing multiple messages from state authorities and private-sector communicants.

Conduct Drills and Exercises

Governors and their senior staff should participate in training events, drills, and exercises. Large-scale exercises provide an excellent opportunity to build relationships and evaluate strengths and weaknesses. Federal agencies often participate in these exercises and training events as well. States should also consider including neighboring states in chemical accident exercises, as a release of chemical agent will often include multiple jurisdictions.

Know the Chemical Stockpile Emergency Preparedness Program

The U.S. Army has maintained stockpiles of chemical munitions since the 1950s. In 1985, Congress passed Public Law 99-145 directing the Army to destroy the aging chemical weapons while providing maximum protection to the public and the environment. As part of this protection, an agreement was developed between the Army and the Federal Emergency Management Agency establishing the Chemical Stockpile Emergency Preparedness Program (CSEPP). The CSEPP enhances emergency preparedness of the communities around the eight stockpile sites.[16] The program aims to improve emergency preparedness, response, and recovery activities.

The Army is under a congressional mandate to destroy its stockpile of unitary (single component) nerve agents, including VX, by 2004. Plans currently call for the construction of an incinerator at each of the eight chemical weapons storage sites around the country.

Know the National Contingency Plan

The National Oil and Hazardous Substances Pollution Contingency Plan, more commonly called the National Contingency Plan or NCP, is the federal government's blueprint for responding to both oil spills and hazardous substance releases. The NCP is the result of efforts by the U.S. to develop a national response capability and promote overall coordination among the hierarchy of responders and contingency plans.

The first NCP was developed and published in 1968 in response to a massive oil spill from the oil tanker *Torrey Canyon* off the coast of England the year before. More than 37 million gallons of crude oil spilled into the water causing massive environmental damage. To avoid the problems faced by response officials involved in this incident, U.S. officials developed a coordinated approach to cope with potential spills in U.S. waters. The 1968 plan provided the

[16] The affected states and territories are: Alabama, Arkansas, Colorado, Illinois/Indiana, Kentucky, Maryland, Utah, and Washington/Oregon and the territories of American Samoa, Guam, and other Micronesian entities.

first comprehensive system of accident reporting, spill containment, and cleanup; and established a response headquarters, a national reaction team, and regional reaction teams (precursors to the current National Response Team and Regional Response Teams).

Congress has broadened the scope of the NCP over the years. It has been revised to include a framework for responding to hazardous substance spills as well as oil discharges. In 1980, it was broadened to cover releases at hazardous waste sites requiring emergency removal actions. Over the years, additional revisions have been made to the NCP to keep pace with the enactment of legislation. The latest revisions to the NCP were finalized in 1994 to reflect the oil spill provisions of the Oil Pollution Act of 1990.

GOVERNOR'S CHEMICAL TERRORISM CHECKLIST

- ✔ Ensure that state and local health, fire, police, safety, and other governmental officials require detailed information be submitted by chemical facilities about the identity, characteristics, and quantities of hazardous substances and chemicals used and stored in communities within their jurisdictions.
- ✔ Assess state's preparedness and response capabilities to handle a chemical attack.
- ✔ Review statewide emergency management plan and ensure that the plan addresses all chemical-related acts of terrorism, including the deliberate targeting of a chemical facility, chemical spills, accidents, and the use of chemical agents as weapons.
- ✔ Ensure that the state has the necessary resources to respond to a nuclear emergency, including hospital facilities, first responder capacity, emergency authority related to quarantines, and evacuations.
- ✔ Develop resources for response. Assess training needs and conduct relevant training for chemical weapons.
- ✔ Develop a crisis communications plan and improve communication capabilities (including alerts and notifications).
- ✔ Appoint a SERC.
- ✔ Establish relationships with key members of the private sector, including operators and owners of chemical facilities and hospitals.
- ✔ Conduct drills and exercises to prepare for chemical weapons attacks.
- ✔ Become familiar with the Chemical Stockpile Emergency Response Program.
- ✔ Become familiar with the NCP and the resources it provides to state authorities.

FOR MORE INFORMATION

Centers for Disease Control and Prevention. The CDC provides a detailed list of chemical agents. Go to: www.bt.cdc.gov/agent/agentlist.asp

EPA's Chemical Emergency Preparedness and Prevention Office, Office of Solid Waste and Emergency Response (OSWER). EPA's Chemical Emergency Preparedness and Prevention Office (CEPPO) provides leadership, advocacy, and assistance to: prevent and prepare for chemical emergencies; respond to environmental crises; and inform the public about chemical hazards in their community. To protect human health and the environment CEPPO develops, implements, and coordinates regulatory and nonregulatory programs. The office carries out this work in partnership with regions, domestic and international organizations in the public and private sectors, and the general public. Go to: www.epa.gov/swercepp

Federal Emergency Management Agency. Go to: www.fema.gov

LEPC Locator. Go to: www.epa.gov/ceppo/lepclist.htm

National Association of SARA Title III Program Officials. Go to: www.geocities.com/capitolhill/6286/index.htm

U.S. Chemical Safety and Hazard Investigation Board. Go to: www.csb.gov

U.S. Department of Transportation. Go to: www.dot.gov

U.S. National Response Team. Go to: www.nrt.org

CHAPTER 8

Nuclear and Radiological Terrorism

Nuclear and radiological terrorism represent two of the most feared forms of terrorism that a governor will need to consider. A nuclear detonation or other radiological release could cause catastrophic loss of life and contaminate buildings, the environment, food, and water.

The three types of nuclear terrorism threats commonly mentioned are: detonation of a fabricated or stolen nuclear device, dispersion of radiological material via a conventional explosion (so-called "dirty bomb"), and an attack on a nuclear reactor with the intent to disperse radioactive material similar to the dirty-bomb scenario, but on a much larger scale. In preparing a response plan, governors and homeland security directors must consider all three threat scenarios, the state's responsibilities to control access to nuclear materials, and the response capabilities and assets available from the federal government.

In addition, govenors should take the following specific steps:

- ★ become familiar with the Federal Radiological Emergency Response Plan (FRERP) and the resources it provides to state authorities;
- ★ establish relationships with federal agencies, such as the Nuclear Regulatory Commission, U.S. Department of Energy, and the Environmental Protection Agency, as well as with key members of the private sector, including operators of nuclear facilities and hospitals;
- ★ include preparations for responding to nuclear and radiological terrorism in state emergency management plans;
- ★ ensure that the state has the necessary resources to respond to a nuclear emergency, including hospital facilities, first responders' capacity, and emergency authority related to quarantines and evacuations;
- ★ conduct forums and exercises that test state responses to radiological incidents, including decisionmaker participation and cross-border cooperation; and
- ★ utilize the expertise of state radiological protection staff in preparing to respond to radiological incidents.

BACKGROUND: THE NATURE OF THE THREAT

Terrorism using nuclear or radiological sources could take three primary forms: a fission device (i.e., a nuclear weapon), a radiological dispersal device (RDD), or an attack on a nuclear reactor. Each could cause significant damage, inflict numerous fatalities, and contaminate large areas for years.

The Fission Device

The most common nuclear explosives use highly enriched Uranium-235 (U-235) to produce a nuclear reaction that ends in a massive explosion. The most likely form of a fission device, due to its technical simplicity, is a "gun"-type weapon. Rudimentary in design, the gun weapon propels a mass of U-235 through a barrel into another mass of U-235, producing a fission reaction.

Since the late 1970s, experts have agreed that a terrorist group could obtain the technical skills and information needed to construct a nuclear weapon. However, even with the requisite technical capability, the process is still a difficult one. The construction of even a crude device would require a handful of individuals with specialized expertise in areas such as high explosives, propellants, electronics, nuclear physics, chemistry, and engineering.[17] Moreover, at least 25 pounds to more than 100 pounds of weapons-grade fissile material would be needed. To obtain such material, move it, and fabricate a weapon without being detected would be difficult, but not impossible for states or for well-financed terrorist groups. A device would likely take several months to construct and would require a large car or truck for transport, contributing to an increased likelihood of detection. For these reasons, the "grounds-up" fabrication of a nuclear weapon by a terrorist group is the least likely of all terrorism scenarios.

FOR MORE INFORMATION

Go to: www.cns.miis.edu/research/nuclear.htm

Less certain is the risk of a terrorist group obtaining a prefabricated nuclear weapon from an existing weapons stockpile. Often mentioned is the scenario of a terrorist group obtaining one of the small "suitcase bombs" (actually, the size of a small refrigerator) reportedly built by the former Soviet Union. In such a scenario, the terrorist group would smuggle the bomb into the country via a shipping container and transport the bomb to the target via a small van. Again, as with fabricating a bomb, detection is the best deterrence. It would be difficult to obtain and transport such a weapon in total secrecy. However, if properly shielded, detecting the bomb would be a difficult prospect. The U.S. Customs Service estimates it can only inspect a maximum of 10 percent of the cargo entering the country. In response to this vulnerability, the federal government is increasing both personnel and detection equipment at U.S. ports and borders.

[17] Kevin O'Neill, *The Nuclear Terrorism Threat*, Institute for Science and International Security, Washington, D.C., August 1997. Available at: www.isis-online.org

A nuclear detonation would cause substantial casualties in the immediate blast area and significant contamination of people and structures in a larger surrounding area from the radioactive fallout. A nuclear explosion of ten kilotons,[18] similar in size to the nuclear bombs detonated over Hiroshima and Nagasaki in World War II, would cause immeasurable damage if exploded in a U.S. city, likely destroying the entire city center as well as most structures within an 1,100-meter blast radius.[19] Basic government, emergency, and medical services in the area would be overwhelmed.

Deaths as a result of the explosion would depend largely on the population density and the buildings in the target area. It is assumed that 5,000–15,000 deaths will occur per square kilometer of a densely populated city.[20] Depending on the prevailing weather conditions, fallout from the explosion would also be a concern, but the extent could be controlled by evacuations and medical treatment.

The Radiological Dispersion Device

A radiological dispersion device (RDD), or "dirty bomb," uses a conventional explosive to widely disperse dangerous radioactive material. A RDD can cause widespread contamination, extensive economic damage, and mass panic. Any number of radioactive elements can be used to build a RDD; however, the most common elements are Cesium-137 (Cs-137), Cobalt-60 (Co-60), and Iridium-192 (Ir-192). All are highly radioactive and can be found in commercial use, such as radiation therapy at hospitals and food processing.

RDDs are the easiest method for nuclear terrorists. While not as destructive as a fission device, a dirty bomb would still cause serious contamination as well as economic and psychological damage. However, the primary result of a RDD is fear. Studies at the Lawrence Livermore National Laboratory indicated that the dispersal of one kilogram of plutonium in a densely-populated area could cause around 1,000 cancer deaths if no protective measures were taken.[21] However, this number is artificially high, as response procedures would mitigate deaths significantly. A release of a pencil-sized rod of Cobalt-60 in a metropolitan area would increase chances for cancer by 0.1 percent for anyone living in the city.[22] Consequently, although RDDs can be deadly, their effects are more economic and psychological.

[18] One kiloton (KT) is equal to the power of 1,000 tons of TNT.

[19] *The Effects of Nuclear Weapons*, 3rd ed. (Washington, D.C.: U.S. Department of Defense and U.S. Department of Energy, 1977).

[20] Ibid.

[21] W.G. Sutcliffe, et al. (Lawrence Livermore National Laboratory), "A Perspective on the Dangers of Plutonium:" April 14, 1995, UCRL-JC-118825. Available at: www.llnl.gov/csts/publications/sutcliffe

[22] Bill Keller, "Nuclear Nightmares," *The New York Times Magazine*, May, 26, 2002. Available at: www.nytimes.com/2002/05/26/magazine/26NUKES.html

The effects of a detonation depend on the element and amount used, where it is detonated, and the prevailing weather conditions. Apart from the immediate deaths caused by the blast itself, there can be contamination casualties if the radioactive source is strong enough and has not been disintegrated by the blast. The fear of contamination will cause a larger population to evacuate the area than is probably necessary, causing traffic jams and other problems related to a large-scale, unplanned evacuation.

Contamination of buildings and other structures is another issue. The contamination of areas affected by the release could be significant, requiring either massive cleanup or demolition of buildings before the area can be reinhabited. Additionally, food and water sources could be seriously contaminated if near the blast site. For this reason, dirty bombs are viewed as an attack on economic targets as well as on people.

FOR MORE INFORMATION

Go to: **www.terrorismanswers.com/weapons/dirtybomb.html**

Attacks Against Nuclear Reactors

U.S. nuclear power plants are potential targets for terrorist attacks. If a terrorist group were to successfully attack a nuclear complex—on the ground or through the air, for example—the likely goal would be a core meltdown or release of radioactive material. Such an attack would not result in a nuclear detonation. For this reason, a terrorist attack on a nuclear facility should be viewed like a terrorist attack using a dirty bomb, but possibly more catastrophic due to the volume of nuclear material available for dispersion.

A large-scale release from a nuclear power plant might result in modest casualties initially, except to those in the immediate area and the first responders who could suffer from radiation poisoning. However, the effects of a release over the long term could be dramatic unless the area was adequately decontaminated. For instance, the Chernobyl disaster saw an alarming increase in the number of cancer-related illnesses for children 10 years after the release.

Like a dirty bomb—but on a much larger scale—an attack on a nuclear facility would have long-term economic and psychological consequences. Large sections of land surrounding the facility would need to be evacuated, secured, and decontaminated. Such areas may not be inhabitable for a generation or more. Chernobyl caused the closure and evacuation of much of the nearby area, as the contamination from the decaying radioactive sources was deemed too great a risk for humans.

FOR MORE INFORMATION

Go to: **www.nrc.gov** and
www.iaea.org/worldatom/Press/Focus/Nuclear_Terrorism/bunn.pdf

PREVENTION THROUGH SECURING NUCLEAR MATERIALS

The key to preventing a terrorist attack using a nuclear device is to stop terrorists from obtaining either the weapons themselves or the materials to make them. After acquisition of the right materials, the next steps of obtaining assistance to construct or use the device are easier.[23]

The federal government has the primary responsibility for engaging nations in nonproliferation efforts and for guarding the security of domestic nuclear weapons. The U.S. has taken an increasingly aggressive stance toward the prevention of nuclear smuggling from such areas as the former Soviet Union, Pakistan, and India. For instance, the U.S. Department of Energy's Second Line of Defense Program provides financial and technical support to Russia, aiding its programs to secure its sizeable store of fissile material. Though the program has been a success, more needs to be done.

In the states, governors can contribute to securing nuclear materials in two ways. First, they can undertake efforts to secure radiological sources within their borders that augment or surpass current Nuclear Regulatory Commission (NRC) activities. Nuclear materials can be found in places as varied as hospitals, food processing plants, and construction sites. Governors can create state plans to regulate these sources, requiring "cradle-to-grave" oversight. Some states have already implemented plans to regulate radiological sources; most require some form of registration and a yearly physical inventory.

For states with regulatory programs, coordination with NRC is both formal and informal. Formally, NRC evaluates each state program to determine compatibility and to ensure that the state program is adequate in protecting the health and safety of the public. During these reviews, NRC inspects the state's control of the radioactive material. As long as a state provides at least as much control over the sources as NRC, the plans are generally considered compatible. Informally, organizations such as the Conference of Radiation Control Program Directors (CRCPD) continue to recommend further control of radiological sources to NRC and to the states.

[23] Owen Cote Jr., "A Primer on Fissile Materials and Nuclear Weapon Design,"*Avoiding Nuclear Anarchy, Containing the Threat of Loose Russian Nuclear Weapons and Fissile Material*, (Cambridge, Mass.: The MIT Press, 1996), Appendix B.

Second, governors can take steps to ensure that security personnel at nuclear plants are well trained and in sufficient numbers to repel possible attacks. Although security is primarily the responsibility of plant owners and operators, several states augmented security with National Guard attachments soon after September 11, though this has largely been discontinued. States can help nuclear power plant operators guarantee better security in and around nuclear power plants by conducting training exercises and forums. (It should be noted that the federal government, although involved in the regulation of nuclear power plants, shares no actual responsibility for privately owned nuclear power plant security, except as the occasional force-multiplier or to test the security at a given plant.)

PREPARING STATES FOR ACTS OF NUCLEAR TERRORISM

A governor has several steps to take to prepare for and respond to acts of nuclear terrorism. Many of the necessary preparations focus on response to attacks rather than prevention, largely because of the difficulty in detecting nuclear materials once they have been acquired by terrorists. A governor should:

- ★ know the Federal Radiological Emergency Response Plan;
- ★ establish relationships with federal agencies and the private sector;
- ★ include nuclear and radiological response in state emergency plans;
- ★ ensure that the state has necessary resources for response;
- ★ conduct forums and exercises; and
- ★ utilize the expertise of state radiological protection staff.

Know the Federal Radiological Emergency Response Plan

The Federal Radiological Emergency Response Plan (FRERP) acts as a support mechanism and as a technical assistance resource for governors. The FRERP dictates the federal response to radiological emergencies, regardless of cause. If an emergency occurs at a state or privately owned facility, the state or owner bears primary responsibility for responding to the emergency at the facility. Further, the state or locality bears the primary responsibility for the protection of citizens and property outside the facility. However, the federal government ultimately reserves the right to respond to severe emergencies. The federal government considers the following factors when deciding to respond:

- ★ the type and amount of radioactive material involved;
- ★ the emergency location;
- ★ the potential impact on the population and the environment; and
- ★ the size of the area affected.

Federal involvement is not contingent on state requests for assistance or on public versus private ownership of the affected area. Rather, the federal government may respond to an emergency at its discretion, in consideration of the aforementioned factors.

FOR MORE INFORMATION

Go to: **www.fas.org/nuke/guide/usa/doctrine/national/frerp.htm**

The FRERP establishes a lead federal agency (LFA) based on the type of radiological emergency. For instance, if a NRC-regulated nuclear facility is affected, NRC would be the lead agency. The Environmental Protection Agency (EPA) is designated as the LFA should the facility fall outside the federal licensing system. EPA is also the LFA for any foreign or unknown sources of radiation.

A governor can also request technical assistance from the federal government during radiological emergencies. These protective action recommendations outline measures that should be taken to lessen or avoid public exposure to radiation. Recommendations are taken from protective action guides (PAGs) issued by EPA and the U.S. Department of Health and Human Services (HHS). In an emergency situation, should a governor desire technical assistance, the protection action request should be made of the LFA. The LFA will consult with other federal agencies where necessary to produce a set of tailored recommendations for the requesting party.

Establish Relationships with Federal Agencies and the Private Sector

Relationships are key to the success of an emergency response. In a radiological emergency, emergency officials should not be forming relationships with federal counterparts or private-sector members of the nuclear community for the first time. State officials can develop a rapport with federal agencies and with the private sector through forums, training exercises, and site visits prior to any radiological emergency. Familiarity with the roles of agencies involved in the FRERP, including the Nuclear Regulatory Commission (NRC), U.S. Department of Energy (DOE), and EPA, as well as points of contact within those agencies should be a high priority for state emergency officials. This familiarity will allow states to avoid communication errors that invariably accompany emergency responses containing multiple players.

Governors should also build relationships with the private sector. More than 80 percent of critical infrastructure is owned by the private sector, so emergency response often involves private actors. By opening channels of communication with the private sector, a governor can better ensure an effective response to acts of nuclear terrorism involving private actors. Furthermore, close relationships with private-sector members allow information to be delivered quickly and accurately. Communications to the public benefit as well, because multiple messages released from both state authorities and private-sector communicants are avoided.

Include Nuclear and Radiological Response in State Emergency Plans

State emergency management plans must address nuclear, radiological, and nuclear reactor-related acts of terrorism. These plans should identify specific points of contact for the injured as well as the agencies responsible for responding to radiological releases. A lead response group should be designated to direct immediate action in responding to the release of radiation. Many states have already undertaken such preparations. For instance, Illinois' Nuclear Safety Preparedness Act requires both industry and the state to bear the costs of producing plans to prevent or respond to nuclear releases. Further, the state has designated the Illinois Department of Nuclear Safety (IDNS) as the primary agency for responding to nuclear incidents in the state, regardless of cause. IDNS has taken steps to educate the public and industry through a number of mass mailings, brochures, and an informational Web site.

FOR MORE INFORMATION

Go to: **www.state.il.us/idns**

A governor should use every possible resource at his or her disposal to train, equip, and coordinate the emergency responders to nuclear and radiological terrorism. A governor should assess whether the lead response agency needs equipment, including protective suits; prophylactic medicine, like potassium iodide; and mobile decontamination capability. Furthermore, the public health sector must have training and equipment. This includes an emergency radiological response plan; proper radiological health training; equipment, such as film badges or thermoluminescent dosimeters (TLDs) designed to monitor doses from external radiation; and instrumentation sensitive enough to detect both penetrating and nonpenetrating radiation. There are great resources for training available from the federal government and certain educational institutions.[24]

Conduct Forums and Exercises

Vital components of a state's response to nuclear threats are forums and exercises. Governors and their senior staff should participate in training events, drills, and exercises. Large-scale reactor exercises, which are federally evaluated, are an excellent opportunity for building relationships and evaluating strengths and weaknesses. Federal agencies often participate in these exercises and training events. States without responsibilities for such exercises might

[24] The Department of Justice's Office for Domestic Preparedness conducts Weapons of Mass Destruction (WMD) training and exercises via grants awarded to states. It is a vital resource for state preparation to respond to nuclear or radiological terrorism. For further information go to: www.odp.usdoj.gov Federal assistance in this effort is also available under the Federal Radiological Emergency Response Plan (FRERP); through DOE Radiological Assistance Program Teams; the Advisory Team on Environment, Food, and Health; and the Federal Radiological Monitoring and Assessment Center (FRMAC). For further information on DOE's Radiological Assistance Program go to: www.gjo.doe.gov/rap/program_information.htm From an academic perspective, see *Disaster Preparedness for Radiology Professionals*.

choose to participate or observe such an exercise at a nearby state. States should also consider including neighboring states in radiological exercises, as a release of radioactive material will often cover multiple jurisdictions.

Utilize the Expertise of State Radiological Protection Staff

Every state has professional personnel responsible for radiation control and radiological health programs. Governors should know these personnel and utilize their expertise. In responding to radiological incidents, these experts will be most familiar with state programs and will be in the best position to provide fast, reliable information to a governor. State radiological protection staff should be included in state planning and state exercises.[25]

GOVERNOR'S CHECKLIST FOR NUCLEAR AND RADIOLOGICAL TERRORISM

- ✔ Become familiar with the Federal Radiological Emergency Response Plan and the resources it provides to state authorities.
- ✔ Establish relationships with federal agencies, such as the Nuclear Regulatory Commission, U.S. Department of Energy, and the Environmental Protection Agency, as well as with key members of the private sector, including operators of nuclear facilities and hospitals.
- ✔ Include preparations for responding to nuclear and radiological terrorism in state emergency management plans.
- ✔ Ensure that the state has the necessary resources to respond to a nuclear emergency, including hospital facilities, first responders' capacity, and emergency authority to quarantine and evacuate.
- ✔ Conduct forums and exercises that test state response to radiological incidents, including decisionmaker participation and cross-border cooperation.
- ✔ Utilize the expertise of state radiological protection staff in preparing to respond to radiological incidents.

[25] The Conference of Radiation Control Program Directors, Inc. (CRCPD) is an excellent resource for determining the resources available to a governor. CRCPD also produces a number of informational publications on the subject of radiation and radiological safety. For further information, go to: www.crcpd.org

CHAPTER 9

Cyberterrorism

Today there is a heightened awareness of the potential for cyberterrorism to shut down public and private information systems from performing essential functions, such as delivering electricity or water to our homes. In the current environment, many of these information systems are integrated and there are many opportunities for cyberterrorists to disrupt our lives. To meet these potential threats, states must have robust cyber protection, detection, warning, response, and recovery capability.

As more states utilize the Internet to provide online services, citizen confidence in the integrity of state systems and the data maintained by these systems are critical. State governments are repositories for important information about the health and public safety of Americans. It is vital that the information is protected against unauthorized use, access, or manipulation, and is available for mobilization of emergency services in the event of a disaster of any kind.

Since the U.S. economy is built on a flourishing information infrastructure, attacks on our critical infrastructure could have a devastating economic impact on states and across the nation. Government systems are linked at all levels. This creates opportunities for one system to potentially infect another with a virus that can shut down critical systems. A cyberattack can have a widespread effect on many systems, and the financial impact has been difficult to quantify. There are many intangible costs, including lost productivity or worker downtime. In addition, cyberattacks are not widely reported because the private and public sectors do not want to expose their vulnerabilities.

To develop an effective cybersecurity program that will manage, monitor, and mitigate the risk of a cyberattack, governors should:

- ★ make cybersecurity a high priority;
- ★ establish a governing body with authority to set cybersecurity policy;
- ★ appoint a designee with cabinet-level authority to oversee cybersecurity policy;
- ★ provide funding resources for cybersecurity;
- ★ leverage cybersecurity resources across agencies; and
- ★ establish private-sector partnerships.

106

WHAT IS A CYBERATTACK?

We have come to rely on the technologies that enable us to work more efficiently. Unfortunately, these technologies also provide new opportunities for criminals. Online crime is rapidly increasing. We are seeing more "pure" computer crimes—that is, crimes where a computer is used as a weapon to attack other computers—and in the spread of malicious code, like viruses. These crimes also include computer intrusions designed to obtain information of the most sensitive sort—such as credit card numbers, companies' trade secrets, or an individual's private information.

Typically, cyberattacks are either undirected or directed.

- **Undirected attacks:** Usually referred to as viruses, worms, or Trojan horses,[26] these attacks can cause the greatest amount of damage because they can take down the entire system, including e-mail, while the system is being cleaned and repaired. These tend to be the most common attacks because they do not require a complex set of skills from the attacker. Indeed, there are Web sites dedicated to hackers that provide instructions on how to unlawfully intrude into computer systems.
- **Directed attacks:** These attacks are mostly done by someone who wants to enter the system for a specific goal. This might include stealing Social Security numbers, credit card numbers, and health information, or defacing Web sites. In many cases, the attacker may be sophisticated enough to enter and leave the system with no trail, making it difficult for someone to know that data have been compromised. This type of attack may also be performed by strong factional groups trying to inflict direct harm on our government.

Cybercriminals look for vulnerabilities in systems and exploit these to commit their crimes. Some of the more common ways to enter systems are via e-mail, the Internet, and cable modems or digital subscriber lines.

- **E-mail:** This is by far the easiest and most common way to spread a virus or worm. The attack comes via a contaminated message that is opened and passed on to millions of people before they even realize what they have done.

[26] **A virus** is a program that can "infect" other programs by modifying them to include a possibly evolved copy of itself. **A worm** is self-propagating malicious code. Unlike a virus, which requires a user to do something to continue the propagation, a worm can propagate by itself. The highly automated nature of worms, coupled with the relatively widespread nature of the vulnerabilities they exploit, allow a large number of systems to be compromised within a matter of hours. **A Trojan Horse** is a useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data. A denial of service attack involves the unlawful intrusion into an unknown number of computers, which are in turn used to launch attacks on the eventual target computer. For further information go to: SANS Institute, www.sans.org/newlook/resources/glossary.htm#F

- **Internet:** Internet security systems have several vulnerabilities that allow information to be compromised, including credit card numbers, Social Security numbers, and other identifiers.
- **Cable modem or Digital Subscriber Line:** Used mainly for home access to the Internet, the average user does not have security measures in place on their home computers, such as a firewall[27] or antivirus software that would protect their information. Information stored on a personal computer can be compromised or the user may unknowingly transfer a virus to the office network.

The Internet is currently one of the most effective means to reach a large population with nearly infinite information. Government relies heavily on the Internet to provide information and to make many services available to citizens. Internet cyberattacks have the potential to:

- deface government Web sites, spreading propaganda and "disinformation";
- inflict large financial losses in resources needed to bring the system back online and in lost productivity by employees and citizens who are unable to do business with the state;
- intrude into networks, potentially resulting in infrastructure outages and corruption of vital data. This impacts citizen confidence in government systems and may result in identity theft or manipulation and loss of data; and
- hamper public safety and health officials' abilities to respond effectively during emergencies.

If the cyberattack is from a terrorist organization, then it would have a more sweeping impact on citizen confidence and our ability to combat terrorist threats. State networks can serve as mounting points for other attacks, so they are a liability if the security policy, processes, and technology are not in place.

[27] A **firewall** is a system or combination of systems that enforces a boundary between two or more networks. It is a gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive microbased UNIX box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

DEVELOPING AN EFFECTIVE STATE CYBERSECURITY PROGRAM

Protecting technology resources from potential attacks has always been a normal course of business for states. This protection is part of their overall strategic plan for information technology (IT). Now there is a heightened awareness beyond the IT community of the potential for large-scale cyberattacks that might be used with other terrorist tactics. To thwart such cyberattacks, states must enhance their efforts to enact consistent policies and procedures and provide education and training programs. Without executive leadership and accountability, states will continue to be vulnerable to cyberattacks.

Make Cybersecurity a High Priority

Citizens and businesses need to know that their vital information is secure and that in the event of a crippling cyberattack, there will be a continued delivery of government services. Loss of citizen confidence in interacting with government information systems will hinder e-governance programs that have given citizens greater convenience and provided government with more efficient ways to do business. Governors can advocate their commitment to cybersecurity on the state Web portal and provide guidelines to citizens and businesses on how to protect their vital information on home and office computers.

Establish a Governing Body with Authority to Set Cybersecurity Policy

Whether creating a new governing body or bringing together existing ones, governors need an executive board that is responsible for setting cybersecurity policy. Many states have existing governing bodies for IT, homeland security, and emergency management and each may have a cybersecurity component. Governors should ensure that all stakeholders, including legislative and judicial representatives, are part of a coordinating body to effectively prevent and respond to cyberattacks.

Governors should link their cybersecurity efforts to homeland security initiatives. Efforts to coordinate with other levels of government and the private sector will minimize redundancies in homeland security actions and ensure integration of efforts.

The governing body should:

- ★ provide oversight and support to the state on cybersecurity policy;
- ★ create a strategic plan that includes enterprise architecture as the underlying foundation to security measures;
- ★ prepare an incident management and response plan based on best practices and including contingencies for every kind of event;
- ★ prepare a statewide security assessment that is carried out by an independent body;

- ★ identify performance measures for the operation of secure information systems;
- ★ establish a computer security response center with clear roles and responsibilities, updated contact lists, thorough communications plans, and appropriate resources; and
- ★ establish a restoration priority list of agencies if multiple agencies are disabled concurrently and resources are scarce.

Appoint a Designee with Cabinet-Level Authority to Oversee Cybersecurity Policy

In addition to having a governance structure in place, a cabinet-level designee should have day-to-day authority over cybersecurity policy. In many states, this is often the state chief information officer (CIO) or the chief information security officer (CISO). The designee should be a member of the state's homeland security task force and participate in cyberterrorism discussions. The designee should be accountable for ensuring that the state's technology security capability adheres to industry best practices and for enforcing consistent security policies.

Provide Funding Resources for Cybersecurity

Cybersecurity policy will not be effective without sustained and committed support. Governors should recognize that systems security is integral to the state's IT strategy. Funding should be allocated for awareness education, training on policies and procedures, hiring security professionals, and external security assessments and analysis. Since the vulnerabilities to a cyberattack lie in the people using the technology—not the technology itself—emphasis on awareness and training should be high priorities. A leading IT consulting company indicated that clients should spend 70 cents of every available dollar on cybersecurity training and awareness programs before investing in new security technologies.[28] There should also be a plan for annual maintenance and site updating of the cybersecurity program.

Leverage Cybersecurity Resources Across Agencies

With limited state resources, the most valuable approach to information security is finding ways to leverage how security is deployed throughout state agencies. As more states have established centralized IT departments, these departments can develop security policies and procedures for all agencies and provide antivirus and other security software instead of having each agency implement its own solution. By using this approach, non-IT state agencies can focus on their core business rather than spending precious time on purchasing and maintaining software for which they do not have enough resources to keep current.

[28] Matt Caston, Senior Principal, AMS, Inc., Enterprise Security Group. Comments made at IT Management Seminar, Chicago, Ill., July 2002.

Establish Private-Sector Partnerships

With the private sector managing more than 80 percent of the nation's critical infrastructure, the public and private sector must collaborate to protect those resources.[29] Critical systems, such as power plants, are run by information systems, so they need protection from a cyberattack. Governors should encourage private-sector companies to uphold strong cybersecurity policies. One way to do this is to include the private sector in the state's cybersecurity governance structure, such as through the formation of a government-industry cybersecurity task force. Government and the private sector can provide each other with meaningful information about a potential cyberthreat and encourage appropriate mechanisms for mitigating and responding to cyberattacks. Moreover, the private-sector security industry can provide input on best practices, trends, lessons learned, and new technology, as well as help states implement best practices for protecting information systems.

GOVERNORS' CHECKLIST TO ADVANCE AND PROMOTE CYBERSECURITY

- ✔ Make cybersecurity a high priority;
- ✔ Establish a governing body with the authority to set cybersecurity policy;
- ✔ Appoint a designee with cabinet-level authority to oversee cybersecurity policy;
- ✔ Provide funding resources for cybersecurity;
- ✔ Leverage cybersecurity resources across agencies; and
- ✔ Establish private-sector partnerships.

[29] Dan Caterinicchia, "Sharing Seen as Critical for Security," *Federal Computer Week*, May 9, 2002. Available at: www.fcw.com/fcw/articles/2002/0506/web-crit-05-09-02.asp

NATIONAL EFFORTS

Several ongoing national efforts can assist states in securing their information systems. For instance, the National Association of State Chief Information Officers (NASCIO) has several initiatives. One creates a working relationship with the President's Critical Infrastructure Protection Board that includes state and local representation. Another is a memorandum of understanding with the National Infrastructure Protection Center (NIPC) that allows participating states to begin receiving sensitive alerts regarding cyberthreats and physical terrorism threats. It is the first step toward a full-featured Interstate Information Sharing and Analysis Center (Interstate ISAC).[30]

The National Governors Association is helping states protect the disclosure of sensitive security information about cyberattacks compiled by state governments. Governors have proposed that the federal Freedom of Information Act (FOIA) be amended to protect this information from general disclosure.[31] In response, the current Administration has included exemptions to FOIA for homeland security in its bill to establish a U.S. Department of Homeland Security.[32] Although not specifically stated, the vulnerabilities that would allow a terrorist to commit a cyberattack may be covered under this exemption.

State and local officials have requested federal training on the identification, investigation, and enforcement of cyber-related crimes and terrorism. The current Administration has tasked the FBI, in coordination with other relevant federal organizations, to assist local law enforcement in obtaining training in these areas.

[30] Interstate ISAC, Section 5(b) of E.O. 13231: "Work with…state and local governments…to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers established on a voluntary basis…in coordination with the NCS, the Federal Computer Incident Response Center, the NIPC, and other departments and agencies, as appropriate." The White House, "Executive Order on Critical Infrastructure Protection," 16 October 2001. Available at: www.whitehouse.gov/news/releases/2001/10/20011016-12.html

[31] FOIA includes specific provisions protecting classified information, trade secrets, and confidential commercial and financial information from disclosure. Although these provisions may apply to homeland security information, FOIA provisions do not specifically address the protection of sensitive security information. Information which may need protection from disclosure includes: (1) vulnerability assessments; (2) details concerning the location, storage, and transportation of hazardous material; (3) Federal Emergency Management Agency assessments; (4) grant proposals and receipts describing security vulnerabilities; (5) private-sector information gathered to assess security vulnerabilities; and (6) federal agency requests from states to assess state security vulnerabilities, response capacities, and government infrastructures.

[32] SEC. 204. Information Voluntarily Provided. "Information provided voluntarily by non-Federal entities or individuals that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism and is or has been in the possession of the Department shall not be subject to section 552 of title 5, United States Code."

FOR MORE INFORMATION

- **Computer Emergency Response Team Coordination Center**. The Computer Emergency Response Team (CERT®) Coordination Center is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. Go to: **www.cert.org**
- **Critical Infrastructure Assurance Office**. The Critical Infrastructure Assurance Office (CIAO) was created because of a Presidential Decision Directive (PDD-63) in May 1998 to coordinate the federal government's initiatives on critical infrastructure assurance. The CIAO's primary areas of focus are to raise issues that cut across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services. Go to: **www.ciao.gov**
- **Critical Infrastructure Protection Board**, Executive Order, October, 16, 2001. Go to: **www.whitehouse.gov/news/releases/2001/10/20011016-12.html**
- **The FBI Computer Crime Squad.** The FBI's National Computer Crime Squad (NCCS) investigates violations of the Federal Computer Fraud and Abuse Act of 1986. Their Web page includes contact information for the squad. Go to: **www.emergency.com/fbi-nccs.htm**
- **Federal Incident Response Center**. The Federal Incident Response Center (FedCIRC) is an organization that provides incident response and security-related services to federal civilian agencies. Go to: **www.fedcirc.gov**
- **National Association of State Chief Information Officers**. The National Association of State Chief Information Officers (NASCIO) represents state chief information officers and information resource executives and managers from the 50 states, 5 U.S. territories, and the District of Columbia. State members are senior officials from any of the three branches of state government with executive-level, statewide responsibility for information resource management. For more information. Go to: **www.ciao.gov**

  NASCIO New Releases:
  Enterprise Architecture Development Toolkit v2.0.
  Available at: **www.nascio.org/publications/index.cfm**

- **Public-Sector Information Security**: A Call to Action for Public-Sector CIOs. Go to: **www.endowment.pwcglobal.com/pdfs/HeimanReport.pdf**
- **National Infrastructure Protection Center**. The missions of the National Infrastructure Protection Center (NIPC) are national security and law enforcement efforts to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and cyber that threaten or target critical infrastructures. Go to: **www.nipc.gov**
- **National Institute of Standards and Technology**. The National Institute of Standards and Technology (NIST) was established by Congress to help industry develop technology, improve product quality, modernize manufacturing processes, ensure product reliability, and facilitate rapid commercialization of products based on new scientific discoveries. Go to: **www.nist.gov**
- **InfraGard.** InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. Go to: **www.infragard.net**
- **Internet Risk Impact Summary** produced by Internet Security Systems, Inc. (888) 901-7477. Go to: **www.iss.net**
- **ISO 17799 Security Policy Standards.** ISO 17799 is an internationally recognized generic information security standard. According to its Web site, ISO 1799 is a comprehensive set of controls comprising best practices in information security. Go to: **www.iso.ch/iso/en/ISOOnline.openerpage**
- **SANS Institute.** The SANS (System Administration, Networking and Security) Institute is a cooperative research and education organization that enables security professionals, auditors, system administrators, and network administrators to share lessons learned and find solutions to challenges they face. Go to: **www.sans.org**
- **U.S. Department of Justice Computer Crime and Intellectual Property Section.** This site provides information about topics related to computer crime, including sample cases, intellectual property rights, encryption and computer crime, privacy and speech issues, international aspects of computer crime, and law enforcement coordination for high-technology crimes. Go to: **www.usdoj.gov/criminal/cybercrime**

CHAPTER 10

The Federal Response

THE FEDERAL RESPONSE PLAN

The Federal Response Plan (FRP) is the mechanism for the response of federal agencies to all natural and technological domestic disasters. The FRP carries out the provisions of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, which authorizes the Federal Emergency Management Agency (FEMA) to assign tasks to any federal department or agency in support of a disaster or emergency declared by the President. It also provides the framework that allows 26 federal departments and agencies and the American Red Cross to organize into interagency functions based on the authorities and expertise of its members and the needs of state and local counterparts.

The FRP is implemented in anticipation of a significant event likely to result in a request for federal assistance or in response to an actual event requiring federal assistance under a Presidential declaration of a major disaster or emergency as described in volume one of the *Governor's Guide to Emergency Management*.

The Terrorism Incident Annex to the FRP provides a new governor with current information about the federal Office of Homeland Security, other federal support agencies, and brief descriptions of their plans. Additionally, it identifies federal technical assistance and training resources that are available from FEMA's Office of National Preparedness (ONP) and the U.S. Department of Justice (DOJ) Office of Domestic Preparedness (ODP). It should be noted that the lead and supporting agencies of the FRP are developing new strategies and programs that reflect the goals and objectives of the national strategy for homeland security.

Terrorism Incident Annex

A Terrorism Incident Annex was added to the FRP in 1997 in compliance with Presidential Decision Directive 39 (PDD-39), the U.S. Policy on Counterterrorism. This annex:

- ★ applies to all threats or acts of terrorism within the U.S. that the White House determines require a response under the FRP;
- ★ identifies all federal departments and agencies that may be directed to respond to the consequences of a threat or act of terrorism within the U.S.; and
- ★ builds upon the process and structure of the FRP by addressing unique policies, situations, operating concepts, responsibilities, and funding guidelines required to respond to terrorism.

The Terrorism Incident Annex defines and provides the context for the federal response to terrorism by focusing on the concepts of crisis management and consequence management. Crisis management includes measures that identify, acquire, and plan the use of resources to anticipate, prevent, and/or resolve a threat or act of terrorism. Under this annex, the FBI retains lead responsibility for preventing, preempting, and terminating threats or acts of terrorism and apprehending and prosecuting the perpetrators. State and local governments provide assistance as required.

Consequence management refers to measures implemented to protect public health and safety; restore essential government services; and provide emergency relief to governments, businesses, and individuals impacted by the consequences of terrorism. While state and local governments exercise primary authority to respond to these consequences, the federal government provides the necessary assistance through FEMA.

Federal Office of Homeland Security (OHS)

President George W. Bush created OHS to develop and implement a comprehensive strategy to secure the United States from terrorist threats or attacks. OHS is responsible for coordinating the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks.

OHS has released the National Strategy for Homeland Security, which outlines prioritized strategic objectives of homeland security and addresses threats and vulnerabilities. The document also identifies critical mission areas including:

- ★ intelligence and warning;
- ★ border and transportation security;
- ★ domestic counterterrorism;
- ★ protecting critical infrastructure and key assets;
- ★ defending against catastrophic threats; and
- ★ emergency preparedness and response.

The strategy establishes a foundation upon which to organize and prioritize homeland security efforts.

FOR MORE INFORMATION

On the national strategy for homeland security, go to:
www.whitehouse.gov/homeland/book/index.html

About state and local actions for homeland security, go to:
www.whitehouse.gov/homeland/stateandlocal/index.htm

FEDERAL SUPPORT AGENCIES

U.S. Department of Defense (DOD). DOD is responsible for activating technical operations to support the federal response to threats or acts of terrorism using weapons of mass destruction (WMD). It coordinates military operations with the appropriate civilian lead agency for technical operations.

U.S. Department of Energy (DOE). In addition to performing its support role in the federal response to threats or acts of terrorism using WMD, DOE is a party to an agreement with the FBI that provides for interface, coordination, and technical assistance to support FBI responsibilities under the Federal Radiological Emergency Response Plan (FRERP). The FRERP coordinates the federal response to incidents involving nuclear materials and is supported by 17 federal agencies and departments.

U.S. Department of Health and Human Services (HHS). HHS has drafted a number of objectives that address homeland security. These include enhancing the ability of the nation's health-care system to effectively respond to bioterrorism and other public health challenges; and building the capacity of the health-care system to respond to public health threats in a more timely and effective manner, especially bioterrorism threats. These objectives will be accomplished by:

- ★ stockpiling sufficient products, including vaccines and therapeutics, to counteract the most likely bioterrorism threats;
- ★ upgrading the capacity of federal, state, tribal, and local public health, hospital, and other health-care facilities;
- ★ upgrading the nation's laboratory capacity to quickly identify and characterize suspected biological threat substances and respond to actual incidents;
- ★ creating a national electronic communications system to link federal, state, tribal, and local public health and other health officials so relevant information about public health threats can be shared rapidly;
- ★ establishing continuity of operations plans that ensure personnel and analytical capability will remain operational in a terrorist attack;
- ★ upgrading the skills of the health-care workforce to meet new and emerging threats; and
- ★ conducting and supporting research to produce more effective vaccines, therapeutics, rapid diagnostic tests, and other monitoring technologies to address bioterrorism and other public health threats.

Environmental Protection Agency (EPA). EPA is responsible for providing technical operations capabilities to support the federal response and may coordinate with individual agencies identified in the National Contingency Plan (NCP). The NCP coordinates the federal environmental response to incidents involving oil spills and, in the context of terrorism, chemical agents.

FEDERAL INTERAGENCY RESPONSE PLANS

When state and local assets are overwhelmed by a disaster, the federal government deploys federal personnel, technical expertise, equipment, and other resources. The authority to coordinate the federal response with state and local agencies impacted by terrorism is provided in several interagency response plans previously described as well as those provided below.

U.S. Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN). The CONPLAN provides overall guidance to federal, state, and local agencies concerning how the federal government would respond to a potential or actual terrorist threat or incident that occurs in the United States, particularly one involving WMD. It establishes conceptual guidance for assessing and monitoring a developing threat; notifying appropriate federal, state, and local agencies of the nature of the threat; and deploying the required advisory and technical resources to help the lead federal agency facilitate interdepartmental coordination of crisis and consequence management activities. The plan designates the FBI as the lead federal agency for crisis management and FEMA as the lead federal agency for consequence management.

FEDERAL TECHNICAL ASSISTANCE AND TRAINING RESOURCES

Assistance Available from DOJ, Office of Domestic Preparedness

DOJ's Office of Domestic Preparedness (ODP) provides a wide range of training and technical assistance. Specifically, ODP offers a comprehensive training program to public safety personnel who will be called upon to respond to a terrorist incident involving WMD. This training is available in a variety of formats, including distance learning, Internet-based training, train-the-trainer, and direct delivery at specialized training facilities.

FOR MORE INFORMATION

Go to: **www.ojp.usdoj.gov/terrorism/technical_assistance.htm** and **www.ojp.usdoj.gov/ocpa/ataglance/terrorism.htm**

Other ODP terrorism response topics address:

- ★ WMD awareness for sheriffs;
- ★ personal scene safety training for firefighters and emergency medical personnel;
- ★ state and local antiterrorism training (SLATT); and
- ★ personal protective equipment (PPE) classes for state and local law enforcement.

ODP continues to administer grants to combat domestic terrorism called State Domestic Preparedness Equipment Grants. These grants support the acquisition of specialized equipment to enhance state and local capabilities to respond to WMD terrorist incidents using chemical or biological agents or radiological, explosive, or incendiary devices. ODP also can provide assistance to state and local government through its State and Local Exercise Support Program.

Assistance Available from FEMA's Office of National Preparedness

FEMA has created the Office of National Preparedness (ONP) to lead the coordination of all federal efforts to assist state and local first responders—including fire, medical, law enforcement personnel, and emergency management organizations—with planning, training, equipment, and exercises to build and sustain a sufficient response capability for terrorist incidents. ONP also works closely with OHS in its efforts related to terrorism preparedness and WMD consequence management. Governors and their homeland security officials should become familiar with the assistance ONP can provide to state emergency management and emergency response organizations to ensure their planning, training, and equipment needs are met.

In addition to its role as a single point of contact among the several federal programs that address terrorism preparedness, ONP has identified implementation of the President's First Responder Initiative as a top priority. This initiative will enhance current first responder capabilities at the state, local, and federal level. It also includes the development of standards to maximize interoperability and provides incentives to develop programs that maximize capability through mutual aid and assistance among all levels of government.

FOR MORE INFORMATION

- ★ Federal CONPLAN **www.fbi.gov/publications/conplan/conplan.pdf**
- ★ Federal Response Plan **www.fema.gov/rrr/frp**
- ★ Federal Response Plan, Terrorism Incident Annex **www.fema.gov/rrr/frp/frpterr.shtm**
- ★ HHS Health and Medical Services Support Plan for Acts of Chemical and Biological Terrorism **www.ndms.dhhs.gov/CT_Program/Response_Planning/C-BHMPlan.pdf**

APPENDIX A

Sources of Emergency Management Information

FEDERAL AGENCIES

U.S. Department of Agriculture
Animal and Plant Health Inspection Service
USDA-APHIS-VS-Emergency Programs
Unit 41
4700 River Road
Riverdale, MD 20737-1231
301/734-8073 (phone)
202/690-1117 (fax)
www.aphis.usda.gov/vs/area_offices.htm (animal-related emergency)

U.S. Department of Agriculture
Animal and Plant Health Inspection Service
USDA, APHIS, PPQ, ISPM
4700 River Road
Riverdale, MD 20737-1229
301/734-8427 (phone)
301/734-8584 (fax)
www.aphis.usda.gov/travel/aqi.html (plant-related emergency)

U.S. Centers for Disease Control and Prevention
Bioterrorism Preparedness and Response Program
1600 Clifton Road
Atlanta, GA 30333
404/639-0385 (phone)
404/639-0382 (fax)
770/488-7100 (24-hour emergency response line)
www.bt.cdc.gov/EmContact/index.asp

U.S. Coast Guard
National Response Center
2100 Second Street, SW
Room 2611
Washington, DC 20593
202/267-2185 (phone)
202/267-2165 (fax)
800/424-8802 (hotline)
www.nrc.uscg.mil/index.htm

U.S. Department of Energy Radiological Assistance Program Offices

Region 1: Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont,
BNL ALARA Center
Radiological Sciences Division
Building 703M
Brookhaven National Laboratory
Upton, NY 11973
516/344-7309 (phone)
516/344-2200 (24-hour phone line)
516/344-1377 (fax)
www.dne.bnl.gov/alara/brochure.htm

Region 2: Arkansas, Kentucky, Louisiana, Missouri, Mississippi, Puerto Rico, Tennessee, Virgin Islands, Virginia, West Virginia
Oak Ridge Operations Office, Department of Energy
P.O. Box 2008
Oak Ridge, TN 37831
865/576-1005 (Emergency assistance #1)
865/525-7885 (Emergency assistance #2)
865/576-9780 (fax)
www-external.ossd.ornl.gov/rap/moreon.htm

Region 3: Alabama, Florida, Georgia, North Carolina, South Carolina
Savannah River Operations Office, Department of Energy
P.O. Box A
Aiken, SC 29808
803/725-1791 (24-hour phone line)
803/725-3376 (fax)
www.sro.srs.gov/inside1.htm

Region 4: Arizona, Kansas, New Mexico, Oklahoma, Texas
Albuquerque Operations Office, Department of Energy
P.O. Box 5400
Albuquerque, NM 87185-5400
505/845-4959 (phone)
505/845-4667 (24-hour phone line)
505/845-4643 (fax)
www.doeal.gov

Region 5: Illinois, Indiana, Iowa, Michigan, Minnesota, Nebraska, North Dakota, Ohio, South Dakota, Wisconsin
Argonne National Laboratory, Department of Energy
9700 South Cass Avenue
Argonne, IL 60439
630/252/6020 (phone)
630/252-6020 (24-hour phone line)
630/252-2835 (fax)
www.anl.gov/OPA/anlil.html

Region 6: Colorado, Idaho, Montana, Utah, Wyoming
Idaho Operations Office, Department of Energy
850 Energy Way
Idaho Falls, ID 83401-1563
208/526-0199 (phone)
208/526-1515 (24-hour phone line)
208/526-7245 (fax)
www.inel.gov

Region 7: California, Hawaii, Nevada
Livermore Site Office, Department of Energy
P.O. Box 808, L-293
Livermore, CA 94551
925/422-0138 (phone)
925/422-8951 (24-hour phone line)
925/423-6727 (fax)
www.oak.doe.gov/OakHomeWF.html

Region 8: Alaska, Oregon, Washington
Richland Operations Office, Department of Energy
P.O. Box 550
Richland, WA 99352
509/376-8519 (phone)
509/373-3800 (24-hour phone line)
509/376-4485 (fax)
www.hanford.gov/rl/index.asp

U.S. Environmental Protection Agency
Chemical Emergency Preparedness and Prevention Office
Office of Solid Waste and Emergency Response
401 M Street, SW
Washington, DC 20460
www.epa.gov/swercepp/index.html

U.S. Fire Administration
National Emergency Training Center
16825 South Seton Avenue
Emmitsburg, MD 21727
301/447-1018 (phone)
301/447-1270 (fax)
www.usfa.fema.gov

Federal Emergency Management Agency
Office of Intergovernmental Affairs
500 C Street, SW
Suite 801
Washington, DC 20472
202/646-4515 (phone)
202/646-4039 (fax)
www.fema.gov

Federal Emergency Management Agency Regional Offices

Region I: Connecticut, Massachusetts, Maine, New Hampshire, Rhode Island, and Vermont
J.W. McCormack Post Office and Courthouse Building, Room 442
Boston, MA 02109-4595
617/223-9540 (phone)
617/223-9519 (fax)
www.fema.gov/Reg-I/index.htm

Region II: New Jersey, New York, Puerto Rico, and the Virgin Islands
26 Federal Plaza, Room 1337
New York, NY 10278-0002
212/225-7209 (phone)
212/225-7281 (fax)
www.fema.gov/Reg-II/index.htm

Region III: District of Columbia, Delaware, Maryland, Pennsylvania, Virginia, and West Virginia
615 Chestnut Street, Sixth Floor
Philadelphia, PA 19106
215/931-5608 (phone)
215/931-5621 (fax)
www.fema.gov/Reg-III/index.htm

Region IV: Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee
3003 Chamblee-Tucker Road
Atlanta, GA 30341
770/220-5200 (phone)
770/220-5230 (fax)
www.fema.gov/Reg-IV/index.htm

Region V: Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin
536 South Clark Street
Chicago, IL 60605
312/408-5503 (phone)
312/408-5234 (fax)
www.fema.gov/Reg-V/index.htm

Region VI: Arkansas, Louisiana, New Mexico, Oklahoma, and Texas
Federal Regional Center, Room 206
800 North Loop 288
Denton, TX 76201-3698
817/898-5104 (phone)
817/898-5325 (fax)
www.fema.gov/Reg-VI/index.htm

Region VII: Iowa, Kansas, Missouri, and Nebraska
2323 Grand Boulevard, Suite 900
Kansas City, MO 64108-2670
816/283-7061 (phone)
816/283-7582 (fax)
www.fema.gov/Reg-VII/index.htm

Region VIII: Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming
Denver Federal Center
Building 710, Box 25267
Denver, CO 80225-0267
303/235-4812 (phone)
303/235-4976 (fax)
www.fema.gov/Reg-VIII/index.htm

Region IX: American Samoa, Arizona, California, Guam, Hawaii, Nevada, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Republic of the Marshall Islands, and the Republic of Palau
Presidio of San Francisco
Building 105
San Francisco, CA 94129-1250
415/923-7100 (phone)
415/923-7112 (fax)
www.fema.gov/Reg-IX/index.htm

Region X: Alaska, Idaho, Oregon, and Washington
Federal Regional Center
130 228th Street, SW
Bothell, WA 98021-9796
425/487-4600 (phone)
425/487-4622 (fax)
www.fema.gov/Reg-X/index.htm

U.S. Food and Drug Administration
Division of Federal-State Relations
5600 Fishers Lane
Rockville, MD 20857-0001
301/827-6906 (phone)
301/443-2143 (fax)
301/443-1240 (24-hour emergency number)
www.fda.gov/ora/fed_state/directorytable.htm

Department of Housing and Urban Development (HUD)
451 7th Street SW
Washington, DC 20410
202/708-1112 (phone)
www.hud.gov

U.S. Public Health Service
Office of Emergency Preparedness
National Disaster Medical System
Parklawn Building, Room 4-81
5600 Fishers Lane
Rockville, MD 20857
800/872-6367 (phone)
800/872-5945 (fax)
www.ndms.dhhs.gov

Department of Veterans' Affairs
Emergency Medical Preparedness Office
VA Medical Center
Martinsburg, WV 25401
304/264-4825 (phone)
304/264-4499 (fax)
www.va.gov

Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response
T4D18, USNRC
Washington, DC 20555
301/415-8003 (phone)
301/415-6382 (fax)
www.nrc.gov

Small Business Administration
Disaster Assistance Division
409 Third Street, SW
Washington, DC 20416
202/205-6734 (phone)
202/205-7728 (fax)
www.sbaonline.sba.gov/disaster

Small Business Administration Disaster Area Offices

Area 1: Connecticut, District of Columbia, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Puerto Rico, Rhode Island, Vermont, Virgin Islands, Virginia, and West Virginia
360 Rainbow Boulevard South, Third Floor
Niagara Falls, NY 14303
716/282-4612 (phone)
716/282-1472 (fax)

Area 2: Alabama, Florida, Georgia, Illinois, Indiana, Kentucky, Michigan, Minnesota, Mississippi, North Carolina, Ohio, South Carolina, Tennessee, and Wisconsin
One Baltimore Place, Suite 300
Atlanta, GA 30308
404/347-3771 (phone)
404/347-4183 (fax)

Area 3: Arkansas, Colorado, Iowa, Kansas, Louisiana, Missouri, Montana, Nebraska, New Mexico, North Dakota, Oklahoma, South Dakota, Texas, Utah, and Wyoming
4400 Amon Carter Boulevard, Suite 102
Fort Worth, TX 76155
817/885-7600 (phone)
817/885-7616 (fax)

Area 4: Alaska, American Samoa, Arizona, California, Guam, Hawaii, Idaho, Nevada, Oregon, and Washington
P.O. Box 13795
Sacramento, CA 95853-4795
916/566-7240 (phone)
916/566-7280 (fax)

DOMESTIC ORGANIZATIONS

American College of Emergency Physicians
1125 Executive Circle
Irving, TX 75038-2522
800/798-1822 or 972/550-0911 (phone)
972/580-2816 (fax)
www.acep.org

American Red Cross
National Headquarters
Disaster Services Department
8111 Gatehouse Road, Second Floor
Falls Church, VA 22042
703/206-7460 (phone)
703/206-8822 (fax)
www.redcross.org

Association for Professionals in Infection Control and Epidemiology, Inc.
1275 K Street, NW, Suite 1000
Washington, DC 20005-4006
202/789-1890 (phone)
202/789-1899 (fax)
www.apic.org

Association of State and Territorial Health Officials
1275 K Street, NW, Suite 800
Washington, DC 20005-4006
202/371-9090 (phone)
202/371-9797 (fax)
www.astho.org

Belfer Center for Science and International Affairs
John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge MA 02138
617/495-1400 (phone)
617/495-8963 (fax)
www.ksg.harvard.edu/bcsia

Brookings Institution
1775 Massachusetts Avenue, NW
Washington, DC 20036
202/797-6000 (phone)
202/797-6004 (fax)
www.brookings.org

Center for Nonproliferation Studies
Monterey Institute for International Studies
460 Pierce Street,
Monterey, CA 93940
831/647-4154 (phone)
831/647-3519 (fax)
www.cns.miis.edu

Center for Strategic and International Studies
1800 K Street, NW
Washington, DC 20006
202/887-0200 (phone)
202/775-3199 (fax)
www.csis.org

Conference of Radiation Control Program Directors, Inc.
205 Capital Avenue
Frankfort, KY 40601
502/227-4543 (phone)
502/227-7862 (fax)
www.crcpd.org

Congressional Fire Services Institute
900 2nd Street, NE, Suite 303
Washington, DC 20002
202/371-1277 (phone)
202/682-3473 (fax)
www.cfsi.org

Federation of American Scientists
1717 K Street, NW, Suite 209
Washington, DC 20036
202/546-3300 (phone)
202/675-1010 (fax)
www.fas.org

Institute for Business and Home Safety
1408 North Westshore Boulevard, Suite 208
Tampa, Florida 33607
813/286-3400 (phone)
813/286-9960 (fax)
www.ibhs.org

International Association of Emergency Managers
111 Park Place
Falls Church, VA 22046-4513
703/538-1795 (phone)
703/241-5603 (fax)
www.iaem.com

International Association of Fire Chiefs
4025 Fair Ridge Drive
Fairfax, VA 22033-2868
703/273-0911 (phone)
703/273-9363 fax)
www.ichiefs.org

International Association of Fire Fighters
1750 New York Avenue, NW, 3rd Floor
Washington, DC
202/737-8484 (phone)
202/737-8418 (fax)
www.iaff.org/iaff/index.html

National Association of Counties
440 First Street, NW
Washington, DC 20001
202/942-4239 (phone)
202/942-4281 (fax)
www.naco.org

National Association of Development Organizations
400 North Capitol Street, NW, Suite 390
Washington, DC 20001
202/624-7806 (phone)
202/624-8813 (fax)
www.nado.org

National Association of State Fire Marshals
1245 Farmington Avenue, Suite 101
West Hartford, CT 06107
860/676-3070 (phone)
860/676-3200 (fax)
www.firemarshals.org

National Emergency Management Association
P.O. Box 11910
Lexington, KY 40578-1910
606/244-8000 (phone)
606/244-8239 (fax)
www.nemaweb.org/index.cfm

National Fire Protection Association
1 Batterymarch Park
P.O. Box 9101
Quincy, MA 02669-9101
617/770-3000 (phone)
617/770-3500 (fax)
www.nfpa.org

National Guard Association of the United States
One Massachusetts Avenue, NW
Washington, DC 20001
202/789-0031 (phone)
202/682-9358 (fax)
www.ngaus.org

National Institute for Urban Search and Rescue
P.O. Box 91648
Santa Barbara, CA 93190-1648
800/767-0093 (phone)
805/569-3270 (fax)
www.emergencyservices.com/niusr

National League of Cities
1330 Pennsylvania Avenue, NW
Washington, DC 20004-1763
202/626-3025 (phone)
202/626-3043 (fax)
www.nlc.org

New England States Emergency Consortium
607 North Avenue, Suite 16
Wakefield, MA 01800
617/224-9876 (phone)
617/224-4350 (fax)
www.serve.com/NESEC

Nuclear Control Institute
1000 Connecticut Avenue, NW, Suite 410
Washington, DC 20036
202/822-8444 (phone)
202/452-0892 (fax)
www.nci.org

Nuclear Energy Institute
1776 Eye Street, NW, Suite 400
Washington, DC 20006-3708
202/739-8000 (phone)
202/785-4019 (fax)
703/644-8805 (off-hours emergency number)
www.nei.org

Nuclear Threat Initiative
1747 Pennsylvania Avenue, NW, Seventh Floor
Washington, DC 20006
202/296-4810 (phone)
202/296-4811 (fax)
www.nti.org

United States Conference of Mayors
1620 Eye Street, NW
Washington, DC 20006
202/293-7330 (phone)
202/293-2352 (fax)
www.usmayors.org

APPENDIX B

State Homeland Security Organization Web Sites

Alaska:	www.state.ak.us/local/pr101701.html
Arizona:	www.az.gov./webapp/portal/displaycontent.jsp?id=1442&contenttype=feature
Colorado:	www.ops.state.co.us
Connecticut:	www.state.ct.us/dps/P5/index.htm
Georgia:	www.gahomelandsecurity.com
Illinois:	www.state.il.us/security
Indiana:	www.in.gov/c-tasc/about
Iowa:	www.iowahomelandsecurity.org/index.htm
Kentucky:	www.homeland.state.ky.us
Minnesota:	www.dps.state.mn.us/HomelandSecurity/index5.htm
Missouri:	www.homelandsecurity.state.mo.us
Montana:	www.discoveringmontana.com/homelandsecurity/css/default.asp
Nebraska:	www.nol.org/homeland
New Hampshire:	www.nhoem.state.nh.us/Terrorism/terrorism.asp
New Mexico:	www.wmd-nm.org
North Carolina:	www.ncgov.com/asp/subpages/safety_security.asp
North Dakota:	www.state.nd.us/dem/HomeSec.html
Ohio:	www.state.oh.us/odps/sos/sosfaq.htm
Pennsylvania:	www.homelandsecurity.state.pa.us
South Carolina:	www.state.sc.us/homeland/homeland.html
South Dakota:	www.state.sd.us/homeland
Tennessee:	www.state.tn.us/homelandsecurity
Texas:	www.demwmd.net
Utah:	www.cem.utah.gov
Vermont:	www.dps.state.vt.us/homeland
Virginia:	www.commonwealthpreparedness.state.va.us
Wisconsin:	www.wisconsin.gov/state/core/domestic_prep.html
Wyoming:	www.attorneygeneral.state.wy.us/ctc.htm