A Governor's Guide to

HOMELAND SECURITY

NGA Center for
BEST PRACTICES

THE NATIONAL GOVERNORS ASSOCIATION (NGA), founded in 1908, is the instrument through which the nation's governors collectively influence the development and implementation of national policy and apply creative leadership to state issues. Its members are the governors of the 50 states, three territories and two commonwealths.

The NGA Center for Best Practices is the nation's only dedicated consulting firm for governors and their key policy staff. The NGA Center's mission is to develop and implement innovative solutions to public policy challenges. Through the staff of the NGA Center, governors and their policy advisors can:

- **Quickly learn about what works,** what doesn't and what lessons can be learned from other governors grappling with the same problems;
- **Obtain specialized assistance** in designing and implementing new programs or improving the effectiveness of current programs;
- **Receive up-to-date, comprehensive information** about what is happening in other state capitals and in Washington, D.C., so governors are aware of cutting-edge policies; and
- **Learn about emerging national trends** and their implications for states, so governors can prepare to meet future demands.

For more information about NGA and the Center for Best Practices, please visit www.nga.org.

A Governor's Guide to

HOMELAND SECURITY

Carmen Ferro
David Henry
Thomas MacLellan
NGA Center for Best Practices
Homeland Security & Public Safety Division

NOVEMBER 2010

NGA Center for BEST PRACTICES

Acknowledgements

A Governor's Guide to Homeland Security was prepared by the Homeland Security & Public Safety Division of the National Governors Association Center for Best Practices (NGA Center) including Allison Cullin, Carmen Ferro, David Henry, Thomas MacLellan and Alisha Powell. Other current and former NGA staff including Heather Hogsett, Christopher Logan, Will Ware, and Taryn Hunter helped to produce the guide. NGA Center Director John Thomasian also contributed to the report.

The authors also appreciate the valuable insights from Trina Sheets, National Emergency Management Association; Major General Timothy Lowenberg, Adjutant General, State of Washington; and William Pelgrin, director, Multi-State Information Sharing & Analysis Center.

Additional review was conducted by the U.S. Department of Homeland Security, the Federal Emergency Management Agency, and the Governors Homeland Security Advisors Council.

The authors also thank Karen Glass for editing the report and Middour Nolan Design for designing the report.

Contents

PART III: RESPOND

PART IV: RECOVER

Preface

As chief executive, governors are responsible for ensuring their state is adequately prepared for emergencies and disasters of all types and sizes. These emergencies and disasters will likely be handled at the local level, and few will require a presidential disaster declaration or attract worldwide media attention. Yet governors must be as prepared for day-to-day events—tornadoes, power outages, industrial fires, and hazardous materials spills—as for catastrophes on the scale of Hurricane Katrina or the September 11 terrorist attacks.

Homeland security can be divided into four major components: prepare, prevent, respond, and recover. These components encompass the cycle of most major and routine homeland security incidents and are found in federal guidance documents provided by the U.S. Department of Homeland Security. *A Governor's Guide to Homeland Security* gives governors an overview of their homeland security roles and responsibilities and offers guidance on how to approach issues like developing mutual aid agreements, sharing information, obtaining assistance from the military, and protecting critical infrastructure. Each chapter includes examples of the many innovations states are using to prepare, prevent, respond, and recover. This update to the 2007 guide has new chapters on grants and funding, citizen preparedness, fusion centers, cyber security, and long-term recovery.

The suggestions for gubernatorial and state actions draw heavily from the experiences of governors, homeland security advisors, and other state officials nationwide. The goal is to help governors effectively manage homeland security incidents of all types and sizes in their states.


FIRE
FIRE
FIRE

Executive Summary

Protecting citizens, property, and businesses from the threat of terrorism and natural and man-made disasters is arguably a governor's most important responsibility. This responsibility is also one of the most daunting because of the potentially disastrous consequences for missteps. Further difficulty comes from the randomness and unpredictability of terrorism and other large-scale disasters. The terrorist attacks of September 11, the Hutaree militia group's plot to kill police officers, the Gulf oil spill, and Hurricane Katrina demonstrate the diverse events to which governors must be ready to respond from their first hour in office.

The threats individual states face and the resources to which they have immediate access are distinct and ever-changing, so each state's homeland security functions will be organized and operated differently. Governors have considerable authority to organize and operate homeland security functions according to their state's needs and priorities. Yet, to do this effectively, they need to answer critical questions, including:

- How are the state's homeland security functions and emergency management agencies coordinated?
- What is the role and authority of the governor's homeland security advisor?
- Are state emergency response plans adequate to respond to the current threat environment?
- How is the state's fusion center organized, and what intelligence products does it produce?
- Are the state's first responders' communications sufficiently interoperable?

How governors address these and other critical issues has tremendous implications. Their decisions will have a direct impact on the safety and security of their state.

Information to help governors make the best decisions possible when organizing and operating their state's homeland security functions can be found in this guide. *A Governor's Guide to Homeland Security* gives governors a high-level overview of homeland security and shares state strategies and initiatives.

The U.S. Department of Homeland Security (DHS) identifies four major components of homeland security: **prepare, prevent, respond, and recover**. These components afford a useful rubric for thinking about the cycle of disasters and emergencies and for organizing recommendations for state action.

PREPARE

Governors can take several steps to **PREPARE** their state as best as possible for natural disasters, criminal acts, and acts of terrorism. **Selecting the state's homeland security advisor is one of the most important gubernatorial decisions.** After the governor, the homeland security advisor (HSA) is the state's lead point of contact with DHS. This individual must have the authority to reach across the state's entire homeland security enterprise and make critical decisions during times of crisis. Moreover, HSAs need access to key intelligence networks, especially because one of their chief responsibilities is to keep the governor informed on emerging threats, events, and responses.

Governors must make other critical decisions regarding the structure and governance of their homeland security functions. Many different ways to organize a state's homeland security functions exist, and trade-offs are associated with each approach. For example, federal homeland security funds must be managed through the state administrative agency (SAA). The SAA determines funding priorities and handles the administrative requirements of federal grant applications. Some states house the SAA within the entity carrying out homeland security operations. If this is not the case, close coordination between the two must be ensured.

Governors must also ensure that appropriate stakeholders are involved in preparedness activities. For example, public health professionals are critical players in most homeland security incidents and should be included in discussions before an incident occurs. In addition, the value of citizen preparedness must be recognized and communicated through public service announcements and social media campaigns. Finally, all states must conduct preparedness exercises to assess readiness and capabilities to respond to homeland security incidents.

PREVENT

Governors can help **PREVENT**, or at least minimize, the risk of future attacks. At the heart of these efforts is the state's fusion center. Fusion centers provide a central location where local, state, and federal law enforcement and public safety officials can work together to receive, integrate, and analyze information and intelligence to identify potential threats. Through efforts such as the U.S. Department of Justice's Nationwide Suspicious Activity Reporting Initiative, fusion centers can also aggregate intelligence on a national scale to identify patterns of suspicious activities that previously may not have been recognized as a potential threat.

To help maximize the use of a fusion center, governors need to ensure key personnel, such as the state homeland security advisor, have proper security clearances and adequately coordinate with and are informed by the fusion center. Specifically, fusion centers must meet a baseline level of capabilities, including use of privacy protections, to ensure recognition from federal authorities.

Governors also have a central role in preventing attacks, including cyber attacks, on their state's critical infrastructure and key resources. This is particularly challenging, because the private sector owns 85 percent of the nation's critical infrastructure. **Governors still need to ensure their state has a current and comprehensive inventory of these assets and has conducted adequate assessments to determine their risk and vulnerability.** A hierarchy of critical infrastructure and key resources should be determined based on these assessments. **Understanding the interdependencies of key assets both within the state and across state lines also is important.** An attack on critical infrastructure in an adjacent state, for example an interstate bridge or electrical transmission line, could have the same impact as if the attack occurred in a governor's home state.

RESPOND

When an attack or a disaster occurs, governors need to ensure their state is prepared to **RESPOND** immediately. The first few hours following a disaster will likely be extremely chaotic. **Ensuring the principals involved in an emergency already know and have practiced their roles and responsibilities—whether tactics, operations, or communications—will greatly improve a state's ability to respond effectively and reassure citizens.** Besides the governor, the principals include the governor's chief of staff and communications director, the homeland security advisor, the emergency management director, the fusion center and operational command center directors, the commander of the state police, chiefs of local law enforcement agencies, and public health directors. The more a governor can promote relationships among these individuals prior to an event the better. As one HSA notes, "the site of a disaster is not the place to be exchanging business cards."

Governors have considerable authority to call for additional resources. They can deploy the National Guard to access equipment and expertise in communications, logistics, and decontamination; request a presidential disaster or emergency declaration under the Stafford Act to obtain federal assistance; and activate the Emergency Management Assistance Compact to facilitate interstate aid and other support. Although these resources can be significant when responding to a disaster or an emergency, governors need to review and understand the limits to their authority to call for additional resources. Knowing how to effectively and expediently use these assets and assistance is essential to how quickly a state can respond to an event.

RECOVER

Following an incident, governors must act quickly to help citizens and communities **RECOVER**. In cases where the scale of an incident exhausts the capabilities of state and local governments, federal assistance often is available to states, individuals, and businesses in the forms of resources, personnel, and loans. **Building a working relationship with the Federal Emergency Management Agency regional administrator before an incident occurs will help governors act quickly in the event of a disaster or an emergency.**

To help coordinate recovery efforts, governors can create a central agency to help local areas access state and federal resources. These one-stop shops can be extremely beneficial to individuals, businesses, local governments, and non-profit organizations. For example, the Rebuild Iowa Office and Rebuild Iowa Advisory Commission were created following severe flooding in 2008; the Louisiana Recovery Authority was established following severe hurricanes in 2005; and the Indiana Office of Disaster Recovery became a new lead agency for long-term recovery from damaging storms in 2008.

The responsibility for preventing and preparing for threats and hazards and, following an event, for responding to and recovering from threats and hazards is unquestionably difficult. Yet appropriate attention to key legal authority, governance, information, and communications issues, along the lines suggested in this guide, can help governors effectively meet today's challenges to state homeland security.

PREPARE

CHAPTER 1.

State Homeland Security Governance

Key Concepts

- Selecting the governor's homeland security advisor is essential to fulfill a state's homeland security mission. This advisor must have the authority to reach across all domains of a state's homeland security enterprise, have access to state intelligence networks and personnel, and be empowered to make critical decisions quickly during an incident.
- The structure of state homeland security organizations varies from state to state, but all are charged with ensuring their state's capabilities to prepare, prevent, respond, and recover from events.

To adequately prepare for the safety and security of their state, governors need to make some essential decisions about how their state's homeland security functions are governed and organized. These foundational decisions have a significant impact on a state's ability to prepare, prevent, respond to, and recover from all hazards including terrorist and criminal acts and natural disasters. While there is no universal approach to organizing homeland security at the state level, governors should ensure that their state is prepared for a range of incidents such as hurricanes, homegrown terrorist plots, and terrorist attacks on the scale of September 11.
Developing an effective approach to homeland security governance requires governors to:

- Define the state's homeland security mission;
- Appoint a state homeland security advisor;
- Designate the state's homeland security organization; and
- Understand federal homeland security policy documents.

Define the State's Homeland Security Mission

Defining the homeland security mission sets the tone for how the various aspects of a state's homeland security enterprise are coordinated. Each state's homeland security mission should reflect the four key operations (prepare, prevent, respond, and recover) identified by the U.S. Department of Homeland Security (DHS). It should also incorporate the priorities, authorities, and capabilities the governor wants to address during his or her term in office.

The following are examples of state homeland security mission statements representing the range of homeland security governance structures across the country:

Alaska: The mission of the Office of Homeland Security is to be the single, statewide focal point for coordinating the state's efforts to prevent terrorist attacks, reduce Alaska's vulnerability to terrorism, and minimize the loss of life or damage to critical infrastructure, and recover from attacks if they occur.[1]

Indiana: The Indiana Department of Homeland Security will provide statewide leadership, exemplary customer service, and subject matter expertise for assurance of local, state, and federal collaboration to continually develop Indiana's public safety capabilities for the well-being, protection, and resiliency of our citizens, property, and economy.[2]

Minnesota: The mission of Homeland Security and Emergency Management (HSEM) is to help Minnesota prevent, prepare for, respond to and recover from natural and human-caused disasters. Our team develops and maintains partnerships; collects and shares information; plans; trains and educates; coordinates response and resources; and provides technical and financial assistance.[3]

Virginia: The Office of Commonwealth Preparedness was created in the Office of the Governor to work with and through others – including federal, state, and local officials, as well as the private sector – to develop a seamless, coordinated security and preparedness strategy and implementation plan. The office also serves as the liaison between the governor and the federal Department of Homeland Security.[4]

As evidenced from these examples, governors must ensure that their homeland security mission includes an all-hazards approach (see definitions of homeland security, homeland defense, and emergency management on this page). Homeland security and emergency management need to work together, along with other agencies such as agriculture, law enforcement, and public health, to effectively coordinate the state's response to a wide range of threats, including natural disasters, criminal acts, and acts of terrorism.

Appoint a State Homeland Security Advisor

Governors should choose a homeland security advisor to implement their state's homeland security mission, whether its scope is broad or narrow. This person will be the primary representative to DHS and will receive communications from this federal agency. Most importantly, the advisor will act on behalf of the governor in the event of a disaster or an emergency. Governors should also recognize that their designated homeland security advisor is a member of the Governors Homeland Security Advisors Council, which affords a forum for homeland security advisors nationwide.

Homeland security is the concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.[5] The 2007 National Strategy for Homeland Security, published by the Department of Homeland Security, recognizes that while the Department must continue to focus on the persistent and evolving terrorist threat, it also must address the full range of potential catastrophic events, including man-made and natural disasters, due to their implications for homeland security.[6] The Department of Homeland Security is the lead federal agency for homeland security.

Homeland defense is the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats, as directed by the President. The Department of Defense is responsible for homeland defense.[7]

Emergency Management is a subset of incident management, the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters.[8]

Role of the State Homeland Security Advisor

All major homeland security functions should flow through the homeland security advisor, who should have the authority to make critical decisions regarding policies, procedures, and communications. Governors need to appoint a strategic and collaborative homeland security advisor who can manage and coordinate diverse, but related, disciplines with an interest in the state's security.

No single model has emerged for carrying out the role and responsibilities of the homeland security advisor. In several states, the advisor staffs the governor on homeland security issues and serves as a liaison between the governor's office, the state homeland security organization, DHS, and other outside organizations. The advisor often chairs a committee that is charged with developing preparedness and response strategies and is composed of representatives from relevant state agencies, including public safety, public health, emergency management, and the National Guard.

A number of factors will influence a governor's choice of homeland security advisor. Key questions to ask include:

- Will he or she be able to carry out the state's homeland security mission and the governor's vision?
- How much public safety experience does he or she have?
- Can this person be trusted with critical intelligence information and can he or she attain a secret level clearance?
- Can he or she make critical decisions in the governor's place should the need arise?
- Is the governor prepared to give him or her budget oversight?
- Does he or she possess the leadership, managerial, and political qualities necessary for this responsibility?

In many states, the advisor also serves as the head of a state agency, either as a cabinet secretary or in another

senior role. According to a recent survey of state homeland security advisors conducted by the NGA Center, about half of them serve in a cabinet-level role reporting directly to the governor. Nearly 25 percent serve in multiple capacities, including homeland security advisor to the governor, emergency management director, head of state law enforcement operations, or the adjutant general. In other states, the advisor serves as the head of a noncabinet-level agency but reports directly to the governor.

The state homeland security advisor must manage and administer a wide variety of operations and disciplines and maintain the critical position of advising the governor on terror-related issues. The advisor should also have the ability to manage large organizations with disparate objectives. In addition, he or she must have the authority to coordinate all activities and training, ensure collaboration and strategic planning, and influence the state's mission.

Role of the Governors Homeland Security Advisors Council

In 2006, the NGA Center, in cooperation with the nation's governors and DHS, created the Governors Homeland Security Advisors Council (GHSAC) to provide a forum for the homeland security advisors from each state and territory to inform the work of the NGA Center. The council shares ideas and best practices by identifying emerging issues, reviewing and analyzing the impacts of federal homeland security activities on states, and informing governors of the impacts of federal homeland security legislation, regulations, and policies on states.

Council members maintain frequent communication via conference calls and biannual meetings. Often, these calls include briefings from federal agencies. The GHSAC convenes twice each year for more formal discussions with senior-level officials and members of the GHSAC Executive Committee. GHSAC members also maintain eight committees that focus on key areas of homeland security such as infrastructure protection, catastrophic planning, and grant guidance.

Designate the State's Homeland Security Organization

Every state has an established homeland security organization, whether it is a stand-alone department or agency, a division of a larger department or agency, or an entity within the governor's office. As governors consider the appropriate governance structure for their homeland security operations, they should ensure the organization has sufficient budget authority to allocate funds based on the four key operations (prepare, prevent, respond, and recover). No one structure has been identified as a model or best practice, nor are there federal requirements dictating a particular structure.

The size, capability, and jurisdictional reach of the homeland security organization vary considerably among states, but most are charged with uniting their state's preparedness and response capabilities across multiple agencies and jurisdictions. A coordinated state homeland security effort involves many stakeholders, such as:

- The governor's office;
- State agencies, including agriculture, transportation, public health, homeland security, emergency management, law enforcement agencies, and the military;

- Local public safety agencies;
- State fusion centers;
- Private-sector critical infrastructure owners;
- State chief information officers; and
- Fire services, public works agencies, and emergency medical services.

Governors must also ensure that their homeland security organizations have the ability to share information within the state as well as with neighboring states. Additionally, governors need to establish a protocol by which they receive notifications and updates during incidents from their homeland security personnel, specifically their homeland security advisor.

Types of State Homeland Security Organizations

State homeland security organizations have evolved since the early 2000s. In most states, their homeland security organization now falls into one of three categories: a stand-alone department or agency, a division of a larger department or agency, or an entity within the governor's office.

Stand-Alone Homeland Security Department or Agency. Approximately 13 states and territories have established a stand-alone department or agency for homeland security. These states task the department or agency with administering the state's homeland security strategy, working with partners to prevent acts of terrorism and safeguarding lives and property. Most operate with an all-hazards approach that puts equal emphasis on accidents, disease outbreaks, natural disasters, technological failures, and acts of terrorism.

Homeland Security Division within an Existing State Department or Agency. Approximately 33 states and territories have established a homeland security division under the jurisdiction of another department or agency, such as the emergency management agency, the department of military and veteran's affairs, or the state police. Several states have also developed homeland security councils, task forces, and/or commissions to identify specific homeland security priorities. Some states combine operations so two or more unique departments or agencies share homeland security responsibilities.

Homeland Security Entity within the Governor's Office. Approximately nine states and territories have councils/commission, offices, or divisions within their governor's office to oversee homeland security operations. These homeland security entities report directly to the governor. Coordination with appropriate state agencies and local homeland security stakeholders is essential for successful daily operations.

Responsibilities of State Homeland Security Organizations

Besides uniting preparedness and response capabilities across multiple agencies and jurisdictions, the state homeland security function is involved in managing the billions of dollars in grant funding from Washington, D.C. Additional responsibilities include tracking and implementing federal grant guidance.

DHS provides grant funding directly to states and large urban areas; states, in turn, allocate resources to local agencies. The state-local relationship has, at times, been strained by the limited amount of funding available, the tension between meeting local needs and achieving statewide strategies, and the practical requirement that localities be self-reliant during the early stages of a disaster.

Each governor must designate an entity to serve as the state administrative agency (SAA). The SAA is responsible for carrying out the administrative requirements of federal homeland security grants, including making sure application requirements are satisfied, ensuring funds are properly allocated, meeting required deliverables, and submitting necessary paperwork. In some states, the homeland security organization and SAA are one and the same. Other states maintain two entities for homeland security operations and grant management. Under both approaches, however, the homeland security advisor must have significant input into how federal homeland security grant funds are allocated. Moreover, the agency serving as the SAA must engage with all appropriate state agencies with a stake in accomplishing the homeland security mission.

Federal agencies other than DHS also provide homeland security-related funding to states, and those funding streams must be integrated with other funding supporting the state strategy. The U.S. Department of Justice, for example, provides grants to state and local governments for public safety projects. These projects frequently have a homeland security function, but the funding streams often flow to different agencies within the state.

The U.S. Department of Health and Human Services also provides financial assistance to states through public health preparedness grants that are focused on building capacity

for bioterrorism, pandemic outbreaks, and mass casualty incidents. These grants go directly to each state's health agency and to private-sector hospitals. States should use their homeland security governance structures to coordinate the use and prioritization of all federal funds.

For additional information regarding the structure of state homeland security organizations, see the NGA Center's publication *Overview of State Homeland Security Governance,* which can be found on the Center's website, www.nga.org/center.

Understand Federal Homeland Security Policy Documents

The federal government provides many reports, strategies, and plans to which states should refer when developing their homeland security strategy. Twenty-five **homeland security presidential directives** (HSPDs) govern the federal government's homeland security policy initiatives. These directives are considered executive orders issued by the President. Each HSPD provides background and policy guidance for homeland security missions affecting the United States today.

Released in 2010 and developed by DHS, the **Quadrennial Homeland Security Review** specifies key homeland security mission priorities, outlines goals for each of those mission areas, and lays the necessary groundwork for next steps. The document involves commentary from thousands of stakeholders. The **Quadrennial Defense Review** (QDR), also released in 2010, is a review of U.S. Department of Defense (DoD) strategy and priorities that sets a long-term course for DoD as it assesses the threats and challenges facing the nation.

The 2009 **Cyber Storm II Final Report** describes a comprehensive, dynamic cyber security exercise held by DHS. The exercise simulated a large-scale coordinated cyber attack on critical infrastructure sectors, including the chemical, communications, transportation, and information technology sectors. The exercise afforded the opportunity to establish and strengthen cross-sector, intergovernmental, and international relationships that are critical during exercise and actual cyber response situations.

Issued in 2008, the **National Response Framework** (NRF) establishes a comprehensive, all-hazards approach to domestic incident response. NRF describes how communities, tribes, states, the federal government, and private-sector and nongovernmental partners work together to coordinate national response; describes best practices for managing incidents; and builds on the National Incident Management System that provides a consistent template for managing incidents.

The **National Infrastructure Protection Plan,** released in 2008, provides a framework for identifying and protecting critical infrastructure and key resources. The plan's goal is to strengthen national preparedness, timely response, and rapid recovery of critical infrastructure in the event of a terror attack, natural disaster, or other emergency.

The 2008 **National Emergency Communications Plan** (NECP) is a strategic plan to improve emergency response communications and complements overarching homeland security strategies and initiatives. It aims to drive measurable and sustainable improvements for interoperable communications nationwide. NECP aligns with statewide communication plans to move emergency communications forward while promoting a coordinated nationwide strategy with the cooperation of more than 150 public- and private-sector emergency communications officials.

The **National Incident Management System**, established in 2008, is a comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines. It is applicable across a broad range of potential incidents, improves coordination and cooperation between public and private entities, and provides a common standard for overall incident management.

Released in 2007, the **National Strategy for Homeland Security** guides, organizes, and unifies federal homeland security efforts. It provides a framework for preventing and disrupting terrorist attacks, protecting critical infrastructure and key resources, and responding to and recovering from incidents.

CHAPTER 2.

Federal Funding and Grant Guidance for States

Key Concepts

- Many state homeland security activities are funded by federal grants.
- Some federal grants are based on formulas with required matches, while others are discretionary. Still others are awarded based on factors such as population and risk. Grants based on the unique characteristics of particular states (e.g., border states, states with ports, and states with several large cities) also are available.
- Significant reporting requirements are associated with federal homeland security grants. To maximize the amount of federal assistance, governors should ensure their state administrative agency for homeland security works closely with federal officials to take advantage of available guidance.

The federal government provides billions of dollars each year to state and local governments to help them cover the costs of homeland security. Many of these grant funds are allocated based on a calculation of the relative risk faced by each jurisdiction. Federal homeland security grants totaled approximately $2.7 billion in fiscal 2010. Since 2002, the U.S. Department of Homeland Security (DHS), through the Federal Emergency Management Agency (FEMA), has provided more than $28 billion in grants to help states, urban areas, tribal governments, and non-profit organizations improve their preparedness for all hazards.[9] In recent years, federal officials have engaged state and local officials to discuss the allocation process, and they have improved the guidance to clarify how recipients can use funds, particularly to sustain long-term projects.

Additional funds are administered by the U.S. Department of Justice through the Office of Justice Programs (OJP) for efforts such as the State and Local Anti-Terrorism Training Program, the Nationwide Suspicious Activity Reporting Initiative, the Fusion Center Training and Technical Assistance Program, and the Criminal Intelligence Operating Policies Program. In fiscal 2009, OJP made 8,229 grant awards, totaling more than $5 billion, to state and local law enforcement and community organizations.[10] OJP grant funds are coordinated by a state administrative agency (SAA) which performs a similar function to the SAA for DHS grants. Interagency coordination within the state is necessary when working with grants received from multiple federal agencies.

Major Homeland Security Grant Programs

The Homeland Security Grant Program suite consists of five sub-programs: the State Homeland Security Program, the Urban Areas Security Initiative, Operation Stonegarden, the Metropolitan Medical Response System, and the Citizen Corps Program.

The State Homeland Security Program (SHSP) provides funds to build capabilities at the state and local levels and to implement the goals and objectives identified in state preparedness reports (see Role of the State Preparedness Report on page 11). States must ensure that at least 25 percent of SHSP funds are dedicated to law enforcement terrorism prevention-oriented planning, organization, exercises, and equipment activities, including activities that support the development and operation of fusion centers. SHSP funds are available to the 56 states and territories. Funds are allocated based on minimum amounts as legislatively mandated and DHS risk methodology. A total of $842 million was available in fiscal 2010 under the SHSP grant.

The Urban Areas Security Initiative (UASI) focuses on enhancing regional preparedness in major metropolitan areas. It directly supports the national priority on expanding regional collaboration in the National Preparedness Guidelines and assists participating jurisdictions in developing integrated regional systems for prevention, protection, response, and recovery. States must ensure that at least

Role of the State Preparedness Report

The state preparedness report is required for any state applying for federal homeland security grants. The state preparedness report enables states to communicate to Congress their accomplishments in building national priorities and capabilities and reveal how they will continue to increase statewide preparedness. It provides a strategic perspective of a state's all-hazards preparedness program, plays a key role in reinforcing a common approach to preparedness, helps state program managers make informed decisions relative to their own preparedness, and facilitates communication with multiple audiences.

25 percent of UASI funds are dedicated to law enforcement terrorism prevention-oriented planning, organization, exercises, and equipment activities, including activities that support the development and operation of fusion centers. Eligible recipients include the 64 highest-risk urban areas. A total of $832.5 million was available for UASI in fiscal 2010.

Operation Stonegarden (OPSG) improves coordination among local, state, and federal law enforcement agencies to secure U.S. borders. Eligible recipients include local units of government at the county level and federally recognized tribal governments in the states bordering Canada (including Alaska), southern states bordering Mexico, and states and territories with international water borders. A total of $60 million was available under OPSG in fiscal 2010.

The **Metropolitan Medical Response System** (MMRS) supports the integration of health, medical and emergency management systems into a coordinated response to mass casualty incidents caused by any hazard. Successful MMRS grantees reduce the consequences of a mass casualty incident during the initial period of a response by having augmented existing local operational response systems before the incident occurs. Eligible MMRS recipients include the 124 MMRS jurisdictions. A total of $39.36 million was available under MMRS in fiscal 2010.

The mission of the **Citizen Corps Program** (CCP) is to bring community and government leaders together to coordinate community involvement in emergency preparedness, planning, mitigation, response, and recovery. Eligible recipients for CCP include the 56 states and territories. A total of $12.48 million was available under the Citizen Corps Program in fiscal 2010. Citizen Corps allocations are determined using the U.S. Patriot Act formula, which specifies that the 50 states, the District of Columbia, and the commonwealth of Puerto Rico will receive a minimum of 0.75 percent of the total available grant funding and that four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S.Virgin Islands) will receive a minimum of 0.25 percent of the total available grant funding. The balance of CCP funds will be distributed on a population-share basis.

Targeted Homeland Security Grant Programs

DHS provides additional financial support for targeted programs and activities through several other grant programs (see table on page 13 for more information).

The **Buffer Zone Protection Program** provides funding to support preparedness capabilities and plans to prevent and protect communities surrounding high-risk critical infrastructure sites.

The **Driver's License Security Grant Program** supports measures to reduce fraud and strengthen the reliability and accuracy of personal identification documents issued by states and territories.

The **Emergency Management Performance Grant Program** helps state and local governments sustain and enhance the effectiveness of their emergency management programs.

The **Emergency Operations Center Grant Program** improves emergency management and preparedness capabilities by supporting flexible, sustainable, secure, and interoperable emergency operation centers to address identified needs and deficiencies.

The **Interoperable Emergency Communications Grant Program** supports improved interoperable emergency communications at the state and local levels, including communications in multijurisdictional response to natural disasters, acts of terrorism, and other man-made disasters.

The **Regional Catastrophic Preparedness Grant Program** provides funding to support coordination of regional all-hazard planning for catastrophic events, including the development of integrated planning communities, plans, protocols, and procedures.

Other preparedness grants support specific activities to strengthen security at ports and enhance intercity bus systems, transit, and trucking.

The **Transit Security Grant Program (TSGP)** provides grant funding to the nation's key high-threat urban areas to enhance security measures for their critical transit infrastructure including bus, ferry and rail systems, specifically:

The **Intercity Bus Security Grant Program** focuses on vulnerability assessments, security plans, and preparedness exercises for explosives and nonconventional threats.

The **Port Security Grant Program** protects critical port infrastructure from terrorism and enhances maritime domain awareness and risk management capabilities to protect against improvised explosive devices and other nonconventional weapons. Funds can also be used to conduct training and exercises and support implementation of the transportation worker identification credential.

The **Transit Security Grant Program** supports sustainable, risk-based efforts to protect critical freight and intercity passenger rail infrastructure.

The **Trucking Security Program** recruits highway professionals to participate in an anti-terrorism and security awareness program.

The **Freight Rail Security Grant Program (FRSGP)** which funds freight railroad carriers and owners of railroad cars to protect critical infrastructure from all hazards.

Additional federal grant programs include:

The **Nonprofit Security Grant Program (NSGP)** which provides funding support for target-hardening activities to nonprofit organizations at a high risk of a terrorist attack and are located within a UASI eligible urban area.

The **Tribal Homeland Security Grant Program** which provides funds to directly eligible tribes to help strengthen the Nation against risks associated with potential terrorist attacks.

Grant Guidance Available from the Federal Government

Most federal homeland security dollars are distributed through FEMA. Several mechanisms exist to guide states through the federal grant process. The Grants.gov website was established as a governmental resource to provide information and assistance on grant processes to the public. Grants.gov stores data on more than 1,000 grant programs and provides access to approximately $500 billion in annual awards. DHS and FEMA publish annual grant guidance documents that can be viewed electronically on Grants.gov or on their respective websites.

Guidance sections include the funding opportunity description, eligibility information, submission deadlines, funding restrictions, and administrative and national policy requirements. Applicants will also find information on the period of performance and exact dollar amount available; a list of allowable costs and training opportunities; information on the review and selection process; and eligibility of cost matching or cost sharing.

National Incident Management System

In 2003, the President issued Homeland Security Presidential Directive 5 (HSPD–5), "Management of Domestic Incidents," which required the development of a framework that enables federal, state, tribal, and local governments, nongovernmental organizations, and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity. The framework, known as the National Incident Management System (NIMS), is adaptable to any incident and includes a core set of doctrines, concepts, principles, terminology, and organizational processes for all hazards to improve coordination among stakeholders.[11]

Homeland Security Grant Programs

Grant Program	Fiscal 2010 Funding	Eligible Applicants	Award Factors
State Homeland Security Program (SHSP)	$842,000,000	State administrative agency (SAA) in the 56 states and territories.	Minimum amounts as legislatively mandated, DHS' risk methodology, and effectiveness of proposed investments.
Urban Areas Security Initiative (UASI)	$832,520,000	SAA in the 64 high-risk urban areas.	Funds allocated based on DHS' risk methodology.
Operation Stonegarden	$60,000,000	SAA in border states and local communities.	Competitively allocated to border states.
Metropolitan Medical Response System (MMRS)	$39,359,956	SAA in the 124 MMRS jurisdictions.	Each jurisdiction receives $317,419 to establish or sustain local capabilities.
Citizen Corps Program	$12,480,000	SAA in the 50 states.	All states receive a minimum of 0.75% of the available funds, and territories receive a minimum of 0.25% of the available funds.
Buffer Zone Protection Program (BZPP)	$48,000,000	SAA in the 56 states and territories.	Tier 1 and Tier 2 critical infrastructure sites.
Driver's License Security Grant Program (DLSGP)	$48,000,000	Department of motor vehicles in the 56 states and territories.	Grantees receive base amount with the balance distributed based on number of driver's licenses issued in each state.
Emergency Management Performance Grant Program (EMPG)	$329,799,991	SAA or emergency management agency in the 56 states and territories.	All states receive a minimum of 0.75% of the available funds, and territories receive a minimum of 0.25% of the available funds.
Emergency Operations Center Grant Program (EOC)	$57,600,000	SAA in the 56 states and territories.	A portion is allocated for congressionally designated projects, while the remainder is allocated competitively.
Freight Rail Security Grant Program (FRSGP)	$15,000,000	Class I, II, and III freight railroad carriers that transport sensitive materials and owners of railroad cars that transport toxic inhalation hazardous materials.	Competitive process based on their ability to deliver protection to underground rail and other high-risk assets, counter-terrorism training, security plans, and vulnerability assessments.
Intercity Bus Security Grant Program (IBSGP)	$11,520,000	Operators of fixed-route intercity and charter buses.	Competitive process based on the ratings of the National Review Panel.
Interoperable Emergency Communications Grant Program (IECGP)	$48,000,000	SAA in the 56 states and territories.	Grant funds based on risk. Each state will receive a minimum of 0.45% of the available funds, and territories will receive a minimum of 0.08% of the available funds.
Non-profit Security Grant Program (NSGP)	$19,000,000	Non-profits that are at high risk of a terrorist attack and located within a UASI-eligible urban areas must apply for funding through the SAA.	Funds will be based on risk analysis, effectiveness, and integration with broader state and local preparedness efforts.

Homeland Security Grant Programs *continued*

Grant Program	Fiscal 2010 Funding	Eligible Applicants	Award Factors
Port Security Grant Program (PSGP)	$288,000,000	Group I and Group II ports are preselected; all others are eligible to apply as a Group III or "All Other Port Areas."	Group I and Group II ports are designated a specific amount of money based on the fiscal 2010 risk analysis; others are competitive.
Regional Catastrophic Preparedness Grant Program (RCPGP)	$33,600,000	11 predesignated high-risk urban areas within the 10 RCPGP sites that received funding under RCPGP in fiscal 2009.	One noncompetitive award will be made to each of the predesignated 11 urban areas within the 10 RCPGP sites.
Transit Security Grant Program (TSGP)	$253,000,000	Eligible agencies are determined by the UASI list and the National Transit Database.	TSGP Tier I awards are subject to a non-competitive review process, whereas TSGP Tier II awards are determined by a competitive review process.
Tribal Homeland Security Grant Program (THSGP)	up to $10,000,000	Tribes applying for a grant shall designate an individual to serve as a tribal liaison with DHS and other federal, state, local, and regional government officials.	THSGP funds will be allocated based on tribal eligibility per the 9/11 Act, and the effectiveness of the applicant's THSGP Investment Justification as determined through a peer review process.
Trucking Security Program (TSP)	$7,772,000 (FY 2009)	Eligibility for funding is limited to applicants who have a current security plan subject to Title 49 CFR 172.800 Transport Tier I Commodities as defined by TSA through the issuance of Highway Security-Sensitive Materials Security Action Items.	Applicants must demonstrate that they have the financial and resource capabilities to successfully address the Security Action Implementation and Monitoring and Planning priorities.

HSPD–5 requires federal agencies to make adoption of NIMS by state, tribal, and local organizations a condition for receipt of federal preparedness grants. Building on the foundation provided by existing emergency management and incident response systems, NIMS integrates best practices into a comprehensive framework for use nationwide by emergency management personnel. The system encourages the development of specialized technologies that facilitate emergency management and incident response activities and allows for the adoption of new approaches that will improve over time. The Incident Management Systems Integration Division of FEMA's National Integration Center provides strategic direction, oversight, and coordination of NIMS.

Target Capabilities List

The Target Capabilities List (TCL) is a companion to the National Preparedness Guidelines. TCL supports an all-hazards approach to building capabilities that may be needed in the event of terrorist attacks, natural disasters, health emergencies, and other major events. It identifies 37 capabilities that were developed with the active participation of stakeholders representing all levels of government, nongovernmental organizations, and the private sector.

CHAPTER 3.

Homeland Security Exercises

Key Concepts

- Many federal grants require homeland security exercises. However, governors should encourage state agencies to conduct additional multi-agency exercises to collaborate and build relationships with local and federal officials, as well as regional coordinators for the Federal Emergency Management Agency (FEMA).
- The FEMA-administered Homeland Security Exercise and Evaluation Program (HSEEP) provides a blueprint for developing, conducting, and evaluating exercises. To use available grant dollars to pay for exercises, states must follow HSEEP guidelines.
- An after action report (AAR) is a required component of any homeland security exercise. Follow-up and evaluation are conducted to review performance and identify corrective actions. An after action conference is an effective forum for the governor and homeland security advisor to review the findings of the AAR and plan improvements.

Exercises are critical to preparedness and are key components of any homeland security program. Specifically, exercises enable homeland security and emergency management personnel to train and practice prevention, protection, response, and recovery capabilities in a realistic environment. They also enable states to evaluate the capabilities of first responders and the effectiveness of response plans to determine which areas need improvement. At the same time, exercises can demonstrate community resolve to prepare for major incidents. Exercises also have the benefit of bringing together agencies from the local, state, and federal levels to foster collaboration and build relationships.

Governors must ensure their state conducts and learns from preparedness exercises. At a minimum, consideration of these issues is necessary:

- How can the state use the Homeland Security Exercise and Evaluation Program?
- Who should participate in homeland security exercises?
- What is the role of the private sector and individuals in homeland security exercises?
- Why should homeland security exercises be evaluated?
- What are other resources for homeland security exercises?

How Can the State Use the Homeland Security Exercise and Evaluation Program?

Many states use the Homeland Security Exercise and Evaluation Program (HSEEP) to conduct exercises. States must follow HSEEP guidelines to be eligible for federal funds to pay for exercises. Administered by FEMA, HSEEP is a capabilities- and performance-based exercise program that provides a standardized policy, methodology, and terminology for exercise design, development, conduct, evaluation, and improvement planning in five reference documents or toolkits. Capabilities-based planning facilitates planning under uncertainty and building capabilities suitable for a wide range of threats and hazards, while working within an economic framework that necessitates choice and prioritization.

HSEEP includes consistent terminology that can be used by all exercise planners, regardless of the nature and composition of their sponsoring agency or organization. It is compliant with several federal directives and initiatives, including the National Strategy for Homeland Security, HSPD-5 (Management of Domestic Incidents), HSPD-8 (National Preparedness), and the National Incident Management System.

Seven types of exercises are defined within HSEEP:[12]

Seminar: is an informal discussion designed to orient participants to new or updated plans, policies, or procedures;

Workshop: is similar to a seminar but builds specific products, such as a draft plan or policy;

Tabletop Exercise: involves key personnel discussing simulated scenarios in an informal setting and is used to assess plans, policies, and procedures;

Game: enables a simulation of operations that often involves two or more teams, usually in a competitive environment designed to depict a real-life situation;

Drill: is a coordinated, supervised activity usually employed to test a single specific operation or function within a single entity;

Functional Exercise: examines the coordination, command, and control among various multi-agency coordination centers and does not involve first responders or emergency officials responding to an incident in real time; and

Full-Scale Exercise: is a multi-agency, multijurisdictional, and multidiscipline exercise involving functional and real-time response.

California's Golden Guardian Exercise Series, created by Governor Arnold Schwarzenegger, provides a useful model of an integrated statewide exercise program.[13] The series begins with seminars and tabletop exercises at the local and state levels and culminates with an annual full-scale exercise that each year focuses on a different scenario, capability, or theme. The governor, state agency officials, and representatives of federal agencies participate in the annual exercises, which in the past have focused on natural disasters and terrorist attacks.

Who Should Participate in Homeland Security Exercises?

The participants in each type of exercise should be determined by the capabilities and the purpose and objectives of the exercise. Tabletop exercises examining an emergency operations plan, for example, should involve officials from all agencies with a role specified in that plan. State exercises can include intrastate and regional representatives, public health professionals, intelligence officers, and public utilities personnel.

Intrastate Partners

Local officials are generally the first to respond to the scene of an incident, emergency, or disaster. Their capabilities are also the first to be overwhelmed and, in large events, assistance from surrounding jurisdictions and the state may be necessary. Exercises that test responses to large-scale incidents, in particular those that result in a governor's declaration of emergency, should involve agencies from across the state to ensure familiarity with common plans and procedures and the individual capabilities and resources of local jurisdictions.

In the aftermath of Hurricane Katrina, for example, **Alabama**'s emergency management agency dispatched 44 standardized response teams, drawn from local jurisdictions throughout the state, to assist with emergency response in the state's most impacted areas. Since then, the state has

included those response teams in statewide exercises, leading to increased familiarity among the teams with resources, capabilities, response plans, and regional threats. [14]

Regional Partners

Large incidents often involve assistance from surrounding states through the national Emergency Management Assistance Compact (EMAC), an interstate agreement that facilitates the movement of equipment and people across state lines in response to an emergency. Consequently, exercises that test a state's response to large incidents should include out-of-state partners when possible. In the Washington, D.C., region for example, where interstate mutual aid is commonplace, **Maryland, Virginia**, and the **District of Columbia** have participated in joint disaster-response exercises since 2003. The exercises examine gaps in crisis communications, information-sharing, and decision-making. They have led to improved planning, better interagency relationships, and more streamlined responses.

Large disasters often require some response and resources from the federal government. Therefore, federal agencies should be involved in exercises with a federal-state coordination component. For example, the **New York** City Police Department, in collaboration with several local and federal agencies and surrounding states, developed an exercise program to test the region's ability to intercept terrorists' attempts to smuggle a radiological "dirty bomb" into Manhattan.

What Is the Role of the Private Sector and Individuals in Homeland Security Exercises?

The private sector is also an important partner in incident response. Employers of all sizes can assist state and local officials with communications, mass sheltering, and, in some cases, large-scale responses. In 2004, the **Georgia** Emergency Management Agency launched an effort to strengthen its partnership with the state's private sector to increase the resources available to respond to an incident and to enhance the state's overall capabilities. As part of that effort, the state involved private companies in an exercise to examine the use of volunteer, private-sector employees in dispensing antibiotic drugs to large populations in response to a bioterrorism attack.

Individual citizens are also important players in any emergency response. Individuals, whether bystanders or those immediately affected by an event, are on the scene even before local first responders, so involving the public in emergency response drills and exercises is essential. The Citizens Corps Program, a federal program that coordinates volunteerism and individual citizen preparedness, provides an additional resource at the local level and should play a role in full-scale exercises.

Why Should Homeland Security Exercises Be Evaluated?

An essential component of any exercise program is an evaluation process that enables participants and agency officials to review their performance and identify areas for improvement. Exercise evaluation guides provide a standardized method for collecting data and measuring strengths and weaknesses. An after action report (AAR) contains the final assessment of how well the participants responded to assigned tasks, reviews the strengths of the exercise, and suggests improvements. An after action conference should be held to review the AAR and begin the process of reviewing and improving plans and procedures. Governors must enforce the recommendations of these improvement plans as they are frequently monitored and tracked by FEMA. Reviewing AARs is recommended to provide additional ideas from states with similar demographics and critical infrastructure.

What Are Other Resources for Homeland Security Exercises?

The Naval Postgraduate School, Center for Homeland Defense and Security, offers seminars to help states develop the capabilities to respond to incidents and bolster multi-agency cooperation. The seminars are conducted by mobile education teams composed of nationally recognized experts in various areas related to homeland security. The Executive Education Seminar focuses exclusively on enhancing the capacity of top government officials to successfully address new homeland security challenges.

CHAPTER 4.

Public Health Preparedness

Key Concepts

- Governors should ensure that public health preparedness is a homeland security priority.
- The state homeland security advisor and state public health officials should work together to coordinate preparedness, planning, and information-sharing activities regarding public health emergencies.
- The threat of bioterrorism is a major concern among homeland security officials. However, the distinction between a naturally occurring outbreak and a terrorist attack (e.g., a pandemic influenza or an Anthrax attack) may not be immediately clear. An effective state response requires timely assessment, accurate information, and multi-agency coordination.
- The governor should encourage and maintain public-private partnerships as a tool for public health emergency response.

As new governors develop their vision for homeland security in their state, an essential partner in preparedness is the public health community. State public health systems perform functions similar to those of homeland security—preparation, surveillance, mitigation, and recovery—but focus exclusively on the public health and health care of the community. Many homeland security incidents will involve public health—whether identifying pathogens, caring for mass casualties, or monitoring available hospital beds. Therefore, public health preparedness is a core function of homeland security planning.

Governors should help forge relationships between their state's public health and homeland security officials early in their administration to coordinate the diverse resources each can bring to bear in an emergency. Together, these officials should focus on:

- Public health threats and challenges;
- Public health implications for homeland security;
- Public health and homeland security collaboration;
- Information-sharing between public health and homeland security;
- Public health as a top homeland security priority; and
- Public-private partnerships for public health preparedness.

Public Health Threats and Challenges

Threats to public health occur frequently and cause more fatalities worldwide each year than acts of terrorism. Diseases alone have killed hundreds of millions of people—more than all the wars of the 20th century combined.[15] In short, the health of the public is routinely at risk. Yet because public health threats are not singular events—like a subway bombing—and are diffused over the entire population, maintaining concern for public health threats is difficult. The threats may vary in their origin and in the populations they affect, but all carry the potential to damage not just the well-being of individuals, but also the social and economic fabric of a society.

The 2009 H1N1 pandemic did not develop into a repeat of the catastrophic 1918 Spanish influenza, but it did illustrate the unpredictable threat and potentially dire consequences of a public health disaster. However, pandemic diseases are not the only threat to public health. The anthrax attacks that followed the September 11 terrorist attacks and a 2007 incident in which the deadly toxin ricin, along with a "terrorist handbook," were discovered in a **Nevada** hotel room both demonstrated the ongoing threat of bioterrorism. In 2009, outbreaks of salmonella traced to a specific peanut butter plant triggered the collapse of a major food producer and spotlighted the danger of food-borne illnesses that occur naturally or through negligence.

Governors must be aware of public health threats, including:

- Acts of bioterrorism, such as the intentional release of anthrax or bubonic plague;

- Outbreaks of novel and/or naturally occurring diseases, such as influenza, tuberculosis, hepatitis, and smallpox;
- Food-borne illnesses that threaten public health, such as E.coli and salmonella; and
- Natural disasters that cause mass dislocations of people and disrupt supplies of food, shelter, potable water, and health care.

Public Health Implications for Homeland Security

The varied and significant threats to public welfare posed by diseases necessitate close coordination between state homeland security and public health agencies. Any discussion of homeland security and emergency preparedness must include public health. Not all public health incidents develop into a homeland security or an emergency management incident. However, most homeland security incidents have public health implications, whether in the treatment and care of survivors, the analysis of a biological threat, or considerations of the environmental and population health impacts of hazardous materials spills.

State and local public health agencies bring numerous tools to bear on an incident. In many states, planning for potential biological hazards predates the development of the homeland security and emergency management disciplines. Public health agencies have plans and procedures for specific threats, epidemiological programs to track outbreaks back to their source, isolation and quarantine procedures to stop the spread of disease, and thorough inventories of medical supplies, hospital capabilities, and licensed medical personnel in the state. When they are properly integrated with homeland security efforts, public health activities can provide a powerful tool for gathering information relevant to an incident, including the health of first responders, the availability of resources to care for the injured, and the location and availability of resources to provide medical interventions (e.g., vaccines) to large populations.

Despite these capabilities, public health agencies are often not well integrated with the homeland security and emergency response communities. The culture of public health—that it is science-based, requires methodical examination of health threats, and relies on time-consuming epidemiological investigations—is often at odds with the rapid-fire, lifesaving decision-making culture of the homeland security and emergency response communities. Governors need to ensure the state improves collaboration among state public health, homeland security, and emergency management agencies.

Public Health and Homeland Security Collaboration

Public health is assigned a crucial support function within the National Incident Management System. Moreover, in some cases, such as the H1N1 influenza outbreak, public health is the principal response discipline. Traditionally, however, public health agencies have managed health incidents with little consultation or coordination with outside agencies. Likewise, emergency management and other response agencies have historically managed incidents without the input and participation of public health agencies. The terrorist attacks of September 11 and Hurricane Katrina underscored that all incidents require a collaborative response to fully care for victims and survivors. Nonetheless, public health's role and responsibilities in incident response are often not clearly

understood by fire, emergency management, and homeland security officials. A governor's commitment to improve interagency collaboration before an incident may ensure that all the state's resources and capabilities are used effectively during and after an incident.

Closer coordination between the public health and public safety communities will provide additional resources and a new perspective for the emergency response community. Collaboration among emergency response partners—including public health—in the planning and preparedness phase will improve coordination when an incident occurs. Although improved coordination between preparedness grant programs administered by the Centers for Disease Control and Prevention and U.S. Department of Homeland Security would help states better synchronize their preparedness activities, governors can take steps—and, in many cases, already have taken steps—to improve that coordination.

In **Virginia**, a system of advisory and oversight committees guide statewide public health preparedness planning. The committees develop the tactics, strategies, and policies the state uses during pandemics and other public health incidents and focuses on issues affecting individual departments and agencies. The process ensures that multiple state agencies and all branches of government collaborate, rather than operate individually.[16]

To address the real threat of food-borne illnesses, **Pennsylvania** Governor Edward Rendell created a Food Safety Council to provide better oversight of the state's food supplies. Council members advise the governor on security protocols and practices at all stages of the food supply chain. Included among the council's members are representatives from the food production, processing, and retailing industries, as well as public health and emergency response personnel who are responsible for investigating and responding to outbreaks of food-borne illnesses or other suspected threats to the food chain.[17]

Information-Sharing Between Public Health and Homeland Security

Accurate and timely public health information can contribute to an efficient and effective response to incidents of any scale. For example, information on available hospital capacity, data on the expected effects of a chemical release, or guidance on the use of personal protective equipment during a pandemic can enhance first responders' capabilities. The flow of public health information to frontline firefighters, police officers, and other emergency responders is essential to an effective incident response. States are using different technology platforms to monitor, visualize, and manage various data streams to assist with emergency response. Governors should ensure that public health information is part of that information flow.

In general, states have adopted geographic information systems (GISs) to improve information sharing. A GIS enables users such as state public safety agencies to digitally map locations in their state to find places with common features and patterns. For example,Virtual **Alabama** offers a shared statewide database of all state infrastructure and assets, including hospitals, ambulance fleets, and public health clinics.[18]

Under the wider umbrella of interstate information-sharing, **Florida, Georgia, Louisiana, Mississippi, Tennessee, Texas,** and **Virginia** formed Virtual USA, based on the Virtual Alabama model. Virtual USA integrates a set of processes and solutions that complements existing policies in each state, builds on existing investments and technologies, and draws on state and local practitioner input to manage data access. The initiative improves emergency response by ensuring practitioners at all levels have immediate access to the information they need to make critical decisions. For example, the Virginia Interoperability Picture for Emergency Response (VIPER) linked feeds on the 2009 H1N1 pandemic outbreak in

Virginia into Virtual USA to provide a layer of public health information alongside additional public health and homeland security assets in the state.[19]

New Jersey combines multiple public health and emergency management resources through Hippocrates, a knowledge management and information brokerage system that incorporates GIS layering technology to present an operational picture of state public health before, during, and after an incident. The system enables data such as hospital bed availability and medical supply inventories to be tracked against other data points, including weather, traffic, and plume models. This information is shared throughout the emergency preparedness community and enhances response times and capabilities.

More importantly, Hippocrates is used by agencies besides the public health agency, including the New Jersey State Police, the regional U.S. Department of Health and Human Services office, and external health associations. This provides situational awareness to transcend the public health sector and results in real-time information from around the region being incorporated into decisionmaking and incident command.

Public Health as a Top Homeland Security Priority

Although significant public health events such as an influenza pandemic or anthrax attack can harm many people and cause enduring damage to communities, these types of major incidents are relatively infrequent compared with other natural disasters and smaller-scale disease outbreaks. This results in an attitude of complacency among the public, media commentators, and some government officials who believe dire warnings of disastrous disease outbreaks are overblown or inaccurate.

Prior to the outbreak of the H1N1 pandemic in April 2009, for example, interest in pandemic preparedness had ebbed after five years of planning for a potential avian influenza that never occurred. In 2008, Congress chose not to renew funding for a Centers for Disease Control and Prevention state pandemic preparedness grant program. As a result, state programs supported by the grants were cut as routine and more-pressing public health priorities—such as food sanitation, environmental management, and childhood vaccination clinics—elbowed out pandemic planning in the competition for increasingly scarce resources. Governors should not only encourage continued federal support for preparedness activities, but also call on state homeland security leadership to coordinate existing state resources to provide the capabilities for an all-hazards response.

Public-Private Partnerships for Public Health Preparedness

An effective public health response to any incident relies on partnerships among local, state, tribal, and federal governments and with non-profit and private-sector organizations. Understanding each partner's roles, responsibilities, and capacities to respond are necessary to develop a coordinated response system.

During the 2009 H1N1 pandemic, public health agencies in many states worked with commercial retail pharmacies and major employers to coordinate the distribution of vaccines to at-risk populations. The private sector also has a role in planning. In **Hawaii**, for example, the state enlisted an advisory group composed of mediation experts and representatives of religious groups and the business community to help public health planners develop a pandemic influenza vaccination priority list that was used to determine who would receive vaccines in the event initial vaccine stockpiles were limited.[20]

CHAPTER 5.

Citizen Preparedness

Key Concepts

- Governors need a plan to address their state's citizen preparedness and ensure messages are tailored to address unique state characteristics.
- Using new communication tools such as text message alerts and social media websites to communicate emergency notices publicly can help ensure message timeliness, consistency, and accuracy.
- Governors should communicate to their citizens about the need to be prepared to be self-sufficient for at least 72 hours in the aftermath of a disaster, including maintaining an ample supply of food, water, and other necessities.

State homeland security officials consistently rank citizen preparedness among their top priorities in annual NGA Center surveys. Some Americans report having taken steps to prepare themselves for disasters by stockpiling food and water, developing household emergency plans, and educating themselves about the threats facing their communities. In 2009, Citizen Corps of the Federal Emergency Management Agency (FEMA) conducted a survey of 4,461 U.S. households regarding citizen preparedness. The survey results demonstrated the limited extent to which individuals are prepared for disasters, identified some of the perceived barriers to preparedness, and described how preparedness varies based on household member demographics (see Findings of FEMA's Citizen Corps National Survey on page 23).

Governors must communicate to citizens on how to prepare for a disaster. Specifically, they should:

- Identify essential messages to communicate to the public;
- Learn best practices and innovations from other states; and
- Use campaigns and incentives to raise public awareness.

Identify Essential Messages to Communicate to the Public

Convincing the public of the need to prepare for disasters and following up that message with tips and practical advice on how to prepare are tasks uniquely suited to the governor's office. Using existing drafts, templates, guidance, and other materials from FEMA will assist in making the messages simple and consistent.

For example, the federal government's Ready Initiative provides standard templates and other information to encourage preparedness. The initiative's message is straightforward and easy to remember: **Prepare, Plan, and Stay Informed**. Each household is reminded that assistance may not be available for at least 72 hours.

Prepare: Preparedness is the understanding that common services and utilities may be unavailable for days or weeks after a disaster and that self-sufficiency will be essential during this period. Governors should ensure their citizens are aware of the following:

- A disaster kit will help citizens survive until outside assistance arrives. Each kit should include the necessities of daily living, including food, water, blankets, prescription medication, and first aid kits, as well as flashlights, radios, and spare batteries.
- Families should be sure to address any unique circumstances, such as children with asthma or senior citizens with special assistance needs.
- Each family member must know the contents and location of the disaster kit.

Plan: Disasters can down communications systems, disrupt transportation networks, and cut off family members at work from those at school or at home. Governors should encourage their state's citizens to think about and write a

Findings of FEMA's Citizen Corps National Survey

The 2009 FEMA Citizen Corps National Survey examined the extent to which individuals are prepared for disasters, identified some of the perceived barriers to preparedness, and described how preparedness varies based on household member demographics. The survey found that:

- 57 percent of individuals reported having "supplies set aside in their home to be used only in the case of a disaster," but less than half of those respondents reported updating their supplies once a year;
- 44 percent of individuals reported having a household emergency plan that included instructions for household members on what to do in the event of a disaster;
- 29 percent of individuals reported that they did not need to self-prepare because emergency responders would help them;
- 42 percent of individuals said they would need help to evacuate in the event of a disaster; and
- 14 percent of individuals reported thinking that a terrorist act would never occur in their community.

This survey includes some encouraging statistics related to the number of individuals who stock emergency supplies in their households and the number of respondents who would rely on their neighborhood, non-profit organizations, and faith-based groups during and after an incident. However, room for improvement does exist. The survey found that many people who report being prepared have not completed important preparedness activities or do not have a sound understanding of community plans. Of those who perceived themselves to be prepared, more than one-third has no household plan and 70 percent did not know their community's evacuation routes.

Source: Federal Emergency Management Agency, Citizen Corps, "Personal Preparedness in America: Findings from the 2009 Citizen Corps National Survey August 2009," revised December 2009, 3, http://www.citizencorps.gov/downloads/pdf/ready/2009_Citizen%20Corps_National%20Survey_Findings_SS.pdf (accessed September 3, 2010).

plan for how family members will contact one another after a disaster, how to reach affected children in schools or at child care centers, and where the family will reunite if access to home is impossible (see Sample Family Communications Plan on page 24).

Stay Informed: Many of the fundamental activities of disaster preparedness will be effective regardless of the nature of the emergency. In some cases, specific steps must be taken to address unique risks or threats. Understanding these unique risks and threats are essential to any robust preparedness effort. Individuals, households, communities, and businesses should be educated on the kinds of natural disasters occurring most often in their community or region and what other threats may exist. The public must also know and understand the emergency plans that have been established by state and local governments. The Ready Initiative includes guidance specific to a range of disasters, including fires, floods, blackouts, earthquakes, landslides, hurricanes, pandemics, tornadoes, tsunamis, volcanoes, winter storms, chemical releases, biological threats, and radiation releases.

Learn State Best Practices and Innovations for Citizen Preparedness

Governors nationwide have launched programs and initiatives to encourage and improve disaster preparedness in their state. Even in states where disasters are a common and almost-predictable occurrence, robust efforts to encourage ongoing individual and community planning and preparedness are important components of the state's homeland security and emergency management activities.

Louisiana, a state with a long history of natural disasters, created a website, GetAGamePlan.org, that includes tips on getting individuals and their families prepared for a disaster. The plan's three components are:

- Putting together an emergency kit with essential supplies and important papers;
- Making preparations for home evacuations, protecting valuables, and sheltering pets; and
- Staying informed of weather and emergency alerts via radio, television, the Internet, or a hand-held device.

GetAGamePlan.org includes evacuation guides, hotline and contact telephone numbers, scenario-based planning efforts, emergency alert sign-up, and public service announcements. It also lists contact information for community shelters and provides information for people with disabilities and pet owners.[21]

Sample Family Communications Plan

- ✔ Identify an out-of-town contact that may be in a better position to communicate among separated family members.
- ✔ Ensure all family members know the phone number and have a cell phone or prepaid phone card to call the emergency contact. This contact should be designated as the "in case of emergency" (ICE) contact in each cell phone's contact list. In the event of an accident, emergency personnel will often check the ICE listing to contact someone the victim knows. Make sure friends and extended family members know if they are listed as an emergency contact.
- ✔ Teach family members how to use text messaging. Text messages often get through network disruptions when a phone call cannot.
- ✔ Subscribe to alert services. Many communities have systems that will send instant text alerts or e-mails to communicate information on bad weather, road closings, local emergencies, and more.
- ✔ Depending on the circumstances and the nature of the emergency, the first important decision is whether to stay or evacuate. Governors should recommend that citizens have a plan for both scenarios.

Source: U.S. Department of Homeland Security, http://www.ready.gov/america/makeaplan/index.html (accessed September 3, 2010).

The Ready **North Carolina** program provides information on potential threats to the state as well as a 23-minute video on how citizens can prepare before a disaster to improve their safety during and after the event. Hurricane preparedness is a specific focus. The state's preparedness website also includes information for residents with special needs. A section for people with hearing impairments includes videos with American Sign Language interpreters who provide advice on how to prepare for the different emergencies listed on the site.[22]

Oklahoma's McReady program is a public-private partnership designed to prepare families for emergencies and increase awareness of severe weather threats. In April, deemed McReady Oklahoma Family Preparedness Month, the statewide severe weather preparedness campaign features displays in McDonald's restaurants. Weather safety movies are shown in schools throughout the state. Officials with the National Weather Service hold weather radio programming events as part of the program, and Oklahoma's first lady can be seen on a weather safety DVD to help families prepare for the storm season.[23]

Use Campaigns and Incentives to Raise Public Awareness

In addition to providing basic preparedness planning information, several states have launched awareness and incentive programs to further encourage their citizens to prepare themselves for a disaster. Awareness programs include Volcano Awareness Month in **Hawaii** and **Washington** and Earthquake Awareness Month in **California, Missouri**, and **Oregon**. These are marked by public education campaigns informing residents and visitors of the immediate and lingering effects of volcanic eruptions and earthquakes. Similar campaigns are common at the start of hurricane season in hurricane-prone states. The legislatures in **Louisiana**[24] and **Virginia**[25] have established tax holidays each May for emergency supplies as an incentive for state residents to prepare disaster kits. Covered goods include coolers, portable generators, waterproof sheeting, battery-powered radios and flashlights, gas or diesel fuel tanks, and carbon monoxide detectors.


PREVENT

CHAPTER 6.

State Fusion Centers

Key Concepts

- State fusion centers bring together information and personnel from various agencies and levels of government to develop crucial homeland security and public safety intelligence. Currently, 72 fusion centers are operating across the nation.
- Governors and homeland security advisors should ensure they have an active security clearance accepted by the U.S. Departments of Defense, Justice, and Homeland Security. This clearance allows them to receive intelligence products from their state's fusion center and participate in classified briefings.
- Despite their growing importance, sustained funding for fusion centers remains a challenge.
- The federal government has deployed secure networks aimed at improving information flow among state and local law enforcement officials and the federal government. These networks can help support the flow of information to fusion centers.
- Fusion centers must have a baseline level of capabilities, including privacy protections, to ensure recognition from federal authorities.

Even before September 11, 2001, states looked to improve the flow and quality of information coming from the federal government to state and local law enforcement agencies. Later, emphasis was placed on removing silos of information at the federal level, which led to the establishment of state fusion centers (see State Fusion Centers Improve Information Flow and Quality on page 28). At these central locations, local, state, and federal officials can work in close proximity to receive, integrate, and analyze information and intelligence. The fusion centers were designed to encourage interagency and intergovernmental cooperation and to help integrate information into a network that can support homeland security and counterterrorism programs. Funded through federal grants from the U.S. Department of Homeland Security (DHS), state fusion centers are still evolving in scope and capacity.

Governors can play an active role in ensuring effective information-sharing. Specifically, they can:

- Review fusion center core capabilities;
- Become acquainted with information-sharing standards and networks;
- Recognize the state role in intelligence and information-sharing;
- Understand the challenges facing fusion centers; and
- Learn from fusion centers in other states.

Review Fusion Center Core Capabilities

Basic functions of a fusion center include gathering, processing, analyzing, and disseminating terrorism, homeland security, and law enforcement information. The Baseline Capabilities for State and Major Urban Area Fusion Centers, released in September 2008 by DHS, the U.S. Department of Justice (DOJ), and the Global Justice Information Sharing Initiative, identifies 12 core capabilities and provides specific instructions on how to achieve each capability. Core capabilities are:[26]

1. Planning and requirements development;
2. Information gathering/collection and recognition of indicators and warnings;
3. Processing and collation of information;
4. Intelligence analysis and production;
5. Intelligence/information dissemination;
6. Reevaluation;
7. Management/governance;
8. Information privacy protections;
9. Security;
10. Personnel and training;
11. Information technology/communications infrastructure, systems, equipment, facility, and physical infrastructure; and
12. Funding.

State Fusion Centers Improve Information Flow and Quality

Currently, 72 fusion centers are operating nationwide. All states now have at least one fusion center, and several major cities have a separate facility to share and analyze information. States with more than one fusion center must designate a primary fusion center for their state that serves as the lead source of information flow among the federal, state, tribal, and local levels.

Between fiscal 2004 and fiscal 2007, the federal government provided more than $254 million to state and local governments to support the centers. The Homeland Security Data Network, which enables the federal government to move information and intelligence to the states at the secret level, is deployed at 27 fusion centers.[27]

The makeup of fusion centers varies based on the demographics and population of the state in which they are located. Some operate on an "all-crimes" approach with emphasis on terrorism prevention and have heavy representation from state and local law enforcement agencies. Other fusion centers operate on an "all-hazards" approach and include members of the emergency response community and other state representatives. Other state fusion centers use both "all-crimes" and "all-hazards" approaches. Most state fusion centers emphasize collaboration with joint terrorism task forces, the Federal Bureau of Investigation's ongoing and counterterrorism program at the state level.

Source: U.S. Department of Homeland Security, "State and Local Fusion Centers," revised September 16, 2009, http://www.dhs.gov/files/programs/gc_1156877184684.shtm (accessed September 3, 2010).

By incorporating this baseline level of capabilities, fusion centers will have the necessary tools to support gathering, processing, analyzing, and disseminating information to support specific operational capabilities.

DOJ provides additional guidelines to state and local fusion centers to streamline their vision and role in homeland security protection, including:

- Clearly defining the roles and responsibilities of law enforcement, public safety, and the private sector;
- Ensuring policies exist for the protection of privacy and civil liberties;
- Developing a communication plan among fusion center personnel, law enforcement, public safety, private-sector agencies, and the public;
- Establishing an incident reporting system in a manner consistent with the suspicious activity report (SAR) [see Nationwide SAR Initiative on page this page];
- Disseminating alerts, warnings, and notifications, as appropriate, to state, local, and tribal authorities; the private sector; and the public;
- Conducting scenario-based exercises and statewide risk assessments; and
- Adhering to preexisting information-sharing plans, such as the National Criminal Intelligence Sharing Plan.

Nationwide SAR Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative is a process for reporting suspicious activity that ensures the privacy and civil liberties of all citizens. The SAR initiative includes common processes for information-sharing about terrorism-related suspicious activities. The long-term goal is for private-sector entities and state, local, tribal, and federal law enforcement organizations to participate in the SAR initiative, enabling them to share information about suspicious activity that is potentially terrorism-related. The Program Management Office of the U.S. Department of Justice is responsible for nationwide implementation of suspicious activity reporting.

Become Acquainted with Information-Sharing Standards and Networks

As information-sharing improved and expanded, national technical standards for exchanging data among law enforcement, public safety, emergency management, and National Guard networks were developed. The National Information Exchange Model (NIEM), formerly known as the Global Justice XML Data Model, was adopted by DOJ and DHS for sharing information and emerged as the de facto national information-sharing technical standard. NIEM removes the need for agencies to independently create exchange standards and provides flexibility to deal with unique agency requirements. Many state and local governments have initiated programs to assess and adopt NIEM for information exchange within law enforcement, public safety, transportation, health and human services, and education operations.[28]

While NIEM represented a set of technical requirements, a separate information-sharing framework was created to focus on the processes and policies required to coordinate information-sharing among federal, state, local, private, and international organizations. In 2005, President George W. Bush signed Executive Order 13388 to further strengthen the sharing of terrorism information to protect Americans.[29] The order mandated the development of an Information Sharing Environment (ISE), a framework that defines the roles and responsibilities of federal, state, and local agencies in terms of when and how they need to share information. ISE is not a new communication pipeline, but it will rely on systems that state and local agencies already use every day to create multiple channels of information.

Recognize the State Role in Intelligence and Information-Sharing

The federal government has introduced secure computer networks and web-based services aimed at improving the flow of information among intelligence and law enforcement agencies at the federal, state, local, and tribal levels. Requests to access those federal systems must come from law enforcement agencies or state fusion centers. The owner of the information network will then authenticate and authorize access to the user. Several information-sharing networks exist, but a few systems are particularly noteworthy.

The **Regional Information Sharing Systems Network** (RISS.Net), sponsored by DOJ, supports regional law enforcement efforts to promote officer safety and combat terrorist activity, drug trafficking, organized crime, gang activity, violent crimes, and other regional criminal priorities. Six regional centers coordinate the various functions of the network. States sign on to RISS through their regional center.

Law Enforcement Online (LEO) is an encrypted communications service for law enforcement agencies on a virtual private network and also supports multimedia and periodical libraries, online training, and collaboration among special interest groups of law enforcement officials. State officials request access to LEO by filling out an application online and providing an explanation for how they intend to use the network's capabilities.

The **Homeland Security Information Network** (HSIN) is a connectivity point for several networks. HSIN was established to strengthen the flow of real-time threat information to state, local, and private-sector partners at the sensitive but unclassified security level. The program is built on the Joint Regional Information Exchange System (JRIES), a secure network currently operating at the sensitive but unclassified security level. Participants include federal agencies, states, municipalities, and other local government entities, with a significant number of users from the law enforcement community.

JRIES enables multiple jurisdictions, disciplines, and emergency operation centers to receive and share the same intelligence and tactical information so all users can have the same situational awareness. Stakeholders may gain access to HSIN through membership in one or more communities of interest (COI), but they must be homeland security professionals in one of the many homeland security mission areas or affiliated with an organization with a recognized homeland security mission. Once admitted, users can collaborate with other HSIN users in that community. To request membership, stakeholders must first decide which COI meets their needs. COIs are organized by state organizations, federal entities, or mission areas such as emergency management, law enforcement, and critical infrastructure.

NLETS, the **International Justice & Public Safety Information Sharing Network**, is owned and governed by its state members. NLETS is a message switching system that links together local, state, and federal law enforcement and justice agencies for the purpose of information exchange. The system supports data communications links to state networks through a common interface. Users include all states and territories, all federal agencies with a justice component, and selected international agencies. Motor vehicle, driver's license, and state criminal history data are among the types of data exchanged by users.

Understand Intelligence and Information-Sharing Challenges

Some information-sharing initiatives have achieved success. Yet governors should be aware that challenges remain to the integration of information from intelligence, law enforcement, public safety, and other agencies across all levels of government. Striking the appropriate balance between openness of information and security of information should always be at the forefront of the discussion on the role of fusion centers. Additional challenges include:

- Multiple points of access and statutory conflicts;
- Security clearance inconsistency;
- Privacy concerns; and
- Homeland security advisory and fusion center director coordination.

Multiple Points of Access and Statutory Conflicts

Many federal information-sharing networks exist, but some are not compatible with state and local systems. As a result, users at the state and local levels are required to sign on to multiple systems to access information. Moreover, conflicts may exist between state and federal regulations on intelligence-related issues. Statutory changes are often needed to reduce conflicts between state and federal regulations.

Security Clearance Inconsistency

Public safety officials need security clearances to receive sensitive and sometimes classified information. Security clearances issued by one federal agency are not always recognized by other federal agencies, exacerbating an already lengthy clearance process.

Privacy Concerns

Privacy and/or civil liberty policies are necessary when sharing sensitive information. Currently, all state fusion centers have developed or are developing a privacy policy that DHS must review and approve. Both DHS and DOJ have resources to help state policymakers navigate federal privacy protection regulations.

Homeland Security Advisor and Fusion Center Director Coordination

The state homeland security advisor and the state's fusion center director have unique but related responsibilities. Every effort should be made to ensure these important leaders in the state collaborate. As the primary contact for homeland security with the governor's office, homeland security advisors need to be aware of all intelligence and counterterrorism efforts occurring at the fusion center level.

Learn from Other State Fusion Centers

The **Georgia** Information Sharing and Analysis Center (GISAC) serves as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence for the state. GISAC was not intended to replace or duplicate the counterterrorism functions of the FBI. It aims to enhance and facilitate the collection of information from local and state sources and to integrate that information into a system that would benefit homeland security and counterterrorism intelligence programs at all levels. GISAC is composed of personnel from the Georgia Emergency Management Agency's Office of Homeland Security, the Georgia Bureau of Investigation, the Georgia Department of Public Safety, the Georgia Sheriff's Association, the Georgia Association of Chiefs of Police, the Georgia Association of Fire Chiefs, and the Georgia Department of Corrections.

The **Illinois** Statewide Terrorism Intelligence Center (STIC) was one of the first 24-hour fusion centers created after the terrorist attacks of September 11, 2001. Representatives come from the Illinois State Police, the Illinois National Guard, the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency, and the Department of Homeland Security. The facility is outfitted with wipe boards, multiple television screens, and a virtual command center that links to the FBI and state and local emergency operations centers. STIC is collocated with the state emergency management agency's emergency operations center for better communication and accessibility between emergency responders and the law enforcement intelligence community. STIC serves as a model for other state agencies nationwide through public-private partnerships and innovative technology solutions.

Significant progress has been made to improve the flow of information and intelligence among all levels of government—particularly from the federal government to state and local governments. Nonetheless, effective information sharing is a process, not an end point, and sustaining an effective information-sharing regime requires constant effort and attention. The proper collection, analysis, and dissemination of information and intelligence at the state and local levels will enhance the capabilities required at the regional and national levels to better connect the dots and disrupt criminal and terrorist acts.

CHAPTER 7.

Critical Infrastructure Protection

Key Concepts

- The nation's critical infrastructure includes 18 sectors spanning agriculture, energy, and telecommunications. Protecting critical infrastructure and ensuring continuity of operations are particular challenges for governors and homeland security advisors, because an estimated 85 percent of these assets are owned by the private sector.
- Essential steps to protecting critical infrastructure include conducting vulnerability assessments and prioritizing assets, understanding the interdependencies of key infrastructure, and coordinating with the private sector and other states that share assets.
- The National Infrastructure Protection Plan creates a network of industry-specific sector coordinating councils and government coordinating councils to align infrastructure protection efforts within and between the private and public sectors.

Protecting and ensuring the continuity of the critical infrastructure and key resources in each state is essential to a nationwide security strategy. Critical infrastructure involves physical or virtual assets so vital to the United States that the incapacitation of those systems would cause a debilitating impact on the state and often the entire nation.[30] Identifying the key critical infrastructure and resources in a state is just the beginning. Preserving these assets from potential disaster is a critical component of a governor's homeland security strategy.

Nationally, 18 sectors of critical infrastructure exist: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; health care and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water. [31]

Governors can take several steps to ensure the state is well positioned to respond to electrical blackouts, fuel shortages, cyber attacks, and other crises. Specifically, they can:

- Identify the state's critical infrastructure;
- Conduct vulnerability and risk assessments for critical infrastructure;
- Identify and understand critical infrastructure interdependencies;
- Develop regional strategies to protect critical infrastructure;
- Coordinate with the private sector to protect critical infrastructure; and
- Recognize the federal government's role in protecting critical infrastructure.

Identify Critical Infrastructure within the State

Critical infrastructure and key resources (CIKRs) are physical and cyber-based systems that are essential to the minimum operations of the economy and government.[32] An estimated 85 percent of the nation's CIKRs are privately owned. To fully comprehend the threats that exist in their state, governors must ensure that all critical infrastructure and key resources in their state are fully identified. The federal government has encouraged this cataloguing of critical infrastructure through its establishment of the National Asset Database, a comprehensive inventory of all assets in the nation. That database, however, has been criticized as including businesses and sites that do not appear to meet the federal government's definition of "critical."[33]

Governors should ensure that state officials work not only with their federal counterparts at the Department of

Homeland Security (DHS) and other agencies, but also with local governments, business owners, and other organizations, to identify infrastructure and resources that are critical and assess these assets' vulnerabilities.

Conduct Vulnerability and Risk Assessments for Critical Infrastructure

Governors and their homeland security advisors should first determine whether a risk assessment has already been completed. If not, they will need to decide who will conduct the risk assessment and what methodology will be used. Many states have developed and applied their own risk-and-vulnerability assessment tools, while others have designated agency risk managers or contracted with the private sector to conduct these assessments.

Threats to critical infrastructure should be assessed in the context of natural, man-made, terrorist, and technological events. Risks should be determined based on those threats, including their likelihood of occurrence and the impact these threats would have on the immediate infrastructure and on interdependent systems and facilities. This type of analysis can be used to prioritize infrastructure for protection and to develop and implement a critical infrastructure protection plan that identifies measures to prevent, eliminate, or mitigate a threat.

Some states have gone so far as to enact legislation requiring industries to take specific actions to protect their infrastructure. For example, **New Jersey** amended its Toxic Catastrophe Prevention Act in November 2005 to require the state's 140 chemical facilities to assess vulnerabilities and hazards that terrorists could exploit.[34] The assessments must include critical reviews of:

- Security systems and access to the facility grounds;
- Existing or required security measures outside the facility's perimeter that would reduce vulnerabilities to an attack on the facility;
- Storage and processing of potentially hazardous materials;
- Employee and contractor background checks and other personnel security measures; and
- Information and cyber security systems.

Forty-three facilities that were already subject to the Toxic Catastrophe Prevention Act are also required to adopt safer technologies.

Identify and Understand Critical Infrastructure Interdependencies

The nation's critical infrastructure is not a distinct collection of hospitals, factories, power plants, and other physical entities. Increasingly, it is an interconnected system of systems, each part of which relies on and affects the operations of other parts of the system. Petroleum refineries, for example, rely on the nation's transportation systems, including trains, trucks, and pipelines, to move both raw and refined products. These transportation systems, in turn, rely on a robust and resilient refining capacity to provide the fuels the refineries need to operate. The computer-based systems that control much of the nation's infrastructure—from freight rail lines to nuclear power plants—rely on the electrical grid to operate. In turn, those supervisory control and data acquisition systems are used to detect failures in the nation's energy networks.

State officials need to establish partnerships, facilitate coordinated information sharing, and enable planning and preparedness for interdependent infrastructure protection within their jurisdictions. They should develop and implement statewide programs to protect CIKRs, and these programs must reflect infrastructure interdependencies in their state. Effective statewide and regional CIKR protection efforts should be integrated into the overarching homeland security strategy to ensure prevention, protection, response, and recovery efforts are mutually supportive. CIKR protection must also cut across all sectors present within the

state or territory and support national, state, and local priorities. State officials should also address unique geographical issues (e.g., mountains and coastlines) and interdependencies among key infrastructure.

Develop Regional Strategies to Protect Critical Infrastructure

Just as few critical infrastructures exist as islands unaffected by other infrastructure, events that affect the critical systems and facilities in one state are likely to have an impact across state lines. As a result, governors should develop regional strategies to manage emergencies and disasters that affect the infrastructure in one state. Mutual aid agreements facilitate the rapid movement of replacement equipment and supplies into affected areas, and private-sector utilities and retailers also have systems to back up their operations and supply chains after disasters and emergencies.

Similarly, governors should consider working together to develop strategies for managing events that have regional effects. In some regions, this is already occurring. The Pacific Northwest Economic Region is composed of Alaska, Idaho, Montana, Oregon, and Washington and the Canadian provinces of Alberta, British Columbia, and the Yukon. It formed a Partnership for Regional Infrastructure Security to develop a regional protection, preparedness, and response plan for dealing with infrastructure-related emergencies.

Coordinate with the Private Sector to Protect Critical Infrastructure

States need to work closely with the private sector to develop emergency response and risk communications plans for incidents affecting privately owned systems or infrastructure. Forging a trust-based relationship between emergency response officials and the private sector is essential to ensure effective security preparations, including accurate vulnerability assessments and the integration of private-sector emergency response plans with those of government agencies. Most of a state's infrastructure is owned by the private sector, so state government needs to communicate a plan for ensuring information obtained from the private sector is protected and stored appropriately.

Several national-level efforts are already underway to encourage private-sector coordination. **The Infrastructure Security Partnership (TISP)**, formed by 11 professional organizations and federal agencies after the September 11 terrorist attacks, promotes collaboration within government and industry to improve the resilience of the nation's critical infrastructure against natural and man-made disasters.[35] TISP members include academics, national organizations, and local, state, and federal agencies as well as representatives of the design, construction, operation, and maintenance communities. A steering committee composed of professional and technical organizations and federal agencies oversees TISP activities.

The partnership's objectives are to:

- Raise awareness of the importance of achieving national and regional disaster resilience for critical infrastructure;
- Create effective, task-focused, multidisciplinary workgroups to improve regional disaster resilience for critical infrastructure;
- Foster the creation and development of regional public-private partnerships to address infrastructure interdependency and interoperability;
- Disseminate knowledge on infrastructure security and disaster preparedness;
- Mobilize TISP members to respond to significant issues and events;
- Promote the improvement and application of risk assessment and management methodologies; and
- Promote the development and review of national and regional plans and policies.

Recognize the Federal Government's Role in Protecting Critical Infrastructure

The basis for the federal government's role in critical infrastructure protection comes from Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection." HSPD-7 establishes a national policy for federal departments and agencies to identify, prioritize, and protect the nation's crit-

ical infrastructure, which it defines as "systems and assets, whether physical or virtual, so vital to the United States that [their] incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[36]

HSPD-7 designates lead federal agencies, known as sector-specific agencies that must collaborate with the private sector to develop information-sharing and analysis mechanisms. In addition, these agencies must work with industry to identify, prioritize, and coordinate the protection of critical infrastructure and key resources as well as facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

Sector-specific agencies are charged with:

- Collaborating with relevant federal agencies, state and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
- Conducting or facilitating vulnerability assessments for the sector; and
- Encouraging risk management strategies to protect against or mitigate the effects of attacks against critical infrastructure and key resources.

The Homeland Security Act of 2002 affords the Department of Homeland Security primary authority for the nation's homeland security mission. It called on DHS to develop "a comprehensive national plan for securing the key resources and critical infrastructure of the United States."[37] The department published this comprehensive plan, known as the National Infrastructure Protection Plan (NIPP), in June 2006. NIPP provides a unifying structure that aligns multiple efforts to protect state critical infrastructure and key resources.

The **National Infrastructure Protection Plan** develops a structure for collaboration among the private sector, state governments, and federal agencies to protect state critical infrastructure and resources. The plan's goal is to set security goals, identify assets, assess risk, prioritize infrastructure, implement protective programs, measure effectiveness, and establish a feedback mechanism for continuous improvement.

The backbone of NIPP is a network of industry-specific **sector coordinating councils** (SCCs) and government coordinating councils through which representatives of the private sector and government will share information, collaborate, and develop strategies for protecting critical infrastructure. SCC members will vary by sector, but they should include a broad base of owners, operators, associations, and other entities within each sector.

Government coordinating councils (GCCs) are the public-sector counterparts to SCCs and are designed to provide interagency and cross-jurisdictional coordination. Each GCC includes representation from federal, state, local, and tribal governments. The various industry sector and government coordinating councils are coordinated through the Partnership for Critical Infrastructure Security, composed of representatives of each of the sector coordinating councils, and the NIPP senior leadership council, composed of representatives of each government coordinating council.

The **Buffer Zone Protection Program** (BZP) provides funding to increase the preparedness capabilities of jurisdictions responsible for the safety and security of communities surrounding high-priority CIKRs, including dams, stadiums, chemical facilities, financial institutions, nuclear and electric power plants, and other high-risk/high-consequence facilities, through allowable planning and equipment acquisition. The state administrative agency (SAA) was the only agency eligible to apply for fiscal 2010 program funds and is responsible for obligating the funds to the appropriate local units of government or other designated recipients. The SAA must coordinate all BZP activities with its respective homeland security advisor.

Information sharing and analysis centers (ISACs) were established jointly by federal agencies and private industry in several sectors. ISACs are used to share threat information among industry members; state, local, and federal agencies; and other industries. The Electricity Sector ISAC, for example, is operated by the North American Electric Reliability Council and provides daily infrastructure reports from DHS; advisories, alerts, and notices from federal agencies; and security standard and guideline information.

CHAPTER 8.

Cyber Security

Key Concepts

- Governors are responsible for significant networks that contain sensitive information and control core government services such as dams, bridges, and 911 networks. They also are an essential partner in protecting non-public networks that control resources such as financial information, electrical grids, and medical records.
- The threat of a coordinated and highly sophisticated cyber attack is a major and growing concern, particularly because a cyber attack on a target, such as a nuclear power plant would have national security implications.
- Governors need to ensure their state has a plan that identifies network vulnerabilities and provides a framework for protecting the state from cyber attacks. At a minimum, governors should ensure their state is doing everything it can to safeguard the networks it directly controls through safe online practices, including encryption and internal usage policies.
- State cyber security efforts should include a focus on recovery in the event of a major attack, including timely system recovery and protection/prevention of essential data from compromise.
- How quickly a state can get systems back online following an attack is essential. Governors who collaborate with the private sector in developing safe and secure cyber policies will greatly improve the speed of recovery after an attack.

Public safety is a foundational tenet of gubernatorial leadership, and all states have layered law enforcement agencies, fire protective services, and emergency response systems to anticipate and respond. During the past few years, the cyber threat has grown in scope and sophistication and must now be considered a part of the public safety umbrella. Citizens rely on cyber networks for virtually every aspect of modern life, including banking, shopping, and communication. Cyber security is no longer a fringe or secondary element of state responsibility. One cyber attack can compromise sensitive data, jeopardize security for thousands of users, and force state networks to shut down for an unknown period. It can also lead to significant unanticipated recovery costs.

State data networks are critical pieces of infrastructure that require the same security attention as physical infrastructure. A major attack on state networks could lead to a mass catastrophic security risk nationwide. Security breaches that compromise private information on state networks could cost millions in unanticipated costs for investigation, lawsuits, overtime pay, and credit insurance protection for citizens whose data was violated. Governors are an essential partner in protecting non-public networks that control essential data, such as electrical grids, financial information, and medical records.

To help ensure public safety and reduce the impacts of cyber attacks, governors need to:

- Learn more about the threat of cyber attacks;
- Understand state vulnerabilities to cyber attacks;
- Develop a cyber security policy;
- Coordinate with the private sector on cyber security; and
- Recognize the federal government's role in cyber security.

Learn More About the Threat of Cyber Attacks

In most cases, the goal of a cyber attack falls into one or more of three categories: steal information, damage systems, and/or disrupt the flow of information. Often, the stolen information includes the loss of very important data, such as banking information, personal records, and sensitive government materials. This can have serious impacts like

identity theft. Moreover, damaged systems can be very costly to repair or replace and can lessen productivity and service delivery. Finally, disrupting the flow of information is not only a nuisance, but also can impede emergency personnel's response time and capabilities during a disaster or an emergency. Consequences such as these pose a significant national security concern and illustrate why it is crucial for states to have network protections.

State information systems face threats both externally and internally. Externally, state systems store and manage sensitive information while interfacing with the public daily. Users often submit personal information on a state website to complete tax forms, apply for a driver's license or professional licenses, conduct online voter registration, pay traffic violations, file annual reports, renew vehicle registration, and request permits. Moreover, citizens often sign up for electronic news updates, really simple syndication (RSS) feeds, and state emergency alert systems. Threats to these external users could result in identity theft and/or financial data compromise. They could also severely diminish a governor's ability to effectively communicate with the public.

Internally, state portals afford staff and other government personnel access to significant amounts of government and personal information, including medical records, biographical data, and direct deposit records. In some cases, internal attacks are intentional. In other cases, personnel may not realize they are contributing to gaps in security.

Understand State Vulnerabilities to Cyber Attacks

Over the years, thousands of state government information systems have been victims of cyber attacks, both small and large. Some of these attacks have been relatively benign, such as defacing a web page, while others have constituted more serious breaches of secure data. These cases highlight both the value of protecting systems from future attacks and the need for systems that have been attacked to get back up and running swiftly.

One state was victimized by an attack that defaced its tax commission website and downloaded "malware" onto visitors' computers. Malware is short for 'malicious software' that infiltrates a computer system without a user's consent. Visitors to the website were told they needed to accept an Adobe license agreement and then download

Role of the Chief Information Security Officer

Most states have a chief information security officer (CISO) to oversee the state's information technology security efforts. Both the state chief information officer and the CISO should develop a state's data protection activities.

Duties of the CISO include technical security-related responsibilities, such as perimeter security, but also administrative security issues, such as policies, procedures, awareness training, compliance audits, and remediation. CISOs provide guidance on classification requirements and data inventory. The state CISO should ensure frequent collaboration with the homeland security advisor, especially as attacks are identified.

software. Once infected, hackers were able to take control of a user's computer and gain access to his or her stored personal information. Although state information technology personnel were able to remove the malicious code and restore the hacked tax site quickly, they are still unclear about how the hackers were able to infiltrate the site.

Another state network was hacked by a foreign attacker who gained access through security vulnerabilities. The hacker used bright images to deface the site where access was gained by exploiting software that lacked a security patch. No sensitive data were compromised, but six state websites were shut down temporarily because of the incident. This was the second incident within a five week period in which the state's investigators concluded that failure to provide adequate safeguards compromised a state agency's online security.

Develop a Cyber Security Policy

Cyber security policies should address operations in, and the security of, cyberspace, focusing on threat reduction, vulnerability reduction, deterrence, incident response, and data recovery. New technologies are introduced often enough that governors and information technology (IT) personnel must review and update state cyber security policies frequently.

No one-size-fits-all approach to effective cyber security exists, because each state faces unique challenges. However, cyber security and information technology experts suggest that, at a minimum, state governments should:

- Implement systems to monitor for vulnerabilities, intrusions, and security breaches;
- Create a log to track threats and repeated attempts to gain access;
- Scan networks frequently to identify potential vulnerabilities;
- Develop statewide polices for baseline cyber security procedures;
- Create user-friendly incident reporting;
- Encourage the use of strategic data encryption tools to protect data;
- Define the roles and responsibilities of key cyber security and IT personnel (see Role of the Chief Information Security Officer on page 36);
- Provide cyber security education and training for state employees and contractors in conjunction with the Multi-State Information Sharing and Analysis Center (see Role of the Multi-State Information Sharing and Analysis Center on this page);
- Engage in exercises to enhance response capabilities; and
- Promote awareness of cyber security via public service announcements.

Efforts in Maryland and Wisconsin illustrate how other states have developed and implemented a cyber security policy. **Maryland**'s Governor Martin O'Malley released the state's IT cyber security policy based on a review of best practices and directed the department of information technology to host cyber security awareness training sessions for state agencies and employees. Highlights of the policy include: an information technology disaster recovery plan, a call for storage areas to house sensitive data, a requirement to use password authentication procedures and change passwords, and clarification on what constitutes a policy violation.[38]

The 2009–2011 **Wisconsin** Homeland Security Strategy makes protecting the state's networks from cyber attacks a top priority and integrates cyber security into homeland security plans and operations. Wisconsin's cyber security initiative also promotes the use of memoranda of understanding to reach agreement on state agency responsibilities for cyber security. In addition, it includes a method to periodically review and update the state's cyber security policies.[39]

Coordinate with the Private Sector on Cyber Security

State officials must include in their cyber security plan the security of networks that run private infrastructure operations, such as telecommunications systems, electrical

Role of the Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative organization with participation from the 50 states and the District of Columbia. The Center aims to provide a common mechanism for raising the level of cyber security readiness and response in each state and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure within states and provides a two-way sharing of information between state and local governments.

grids, gas and oil pipelines, and transportation networks. Such infrastructure is so interdependent that a successful attack on any one infrastructure element could have a cascading effect on several others. A reliable supply of energy, for example, is essential to the operation of hospitals, transportation systems, 911 dispatch centers, and water and wastewater treatment facilities.

The public expects state and local governments to respond to cyber threats as they would to other types of disasters or emergencies. Yet most infrastructure is owned by the private sector, and efforts to legislate or otherwise mandate cyber security programs often meet resistance. Governors should urge their state homeland security advisor, state chief information security officer, and state energy officials to:

- Encourage state agencies to coordinate and cooperate with the private sector;
- Collaborate with private owners of critical infrastructure;
- Use the state's fusion center to share information; and
- Participate in federal and private-sector cyber security initiatives to build partnerships and learn about new tools and practices.

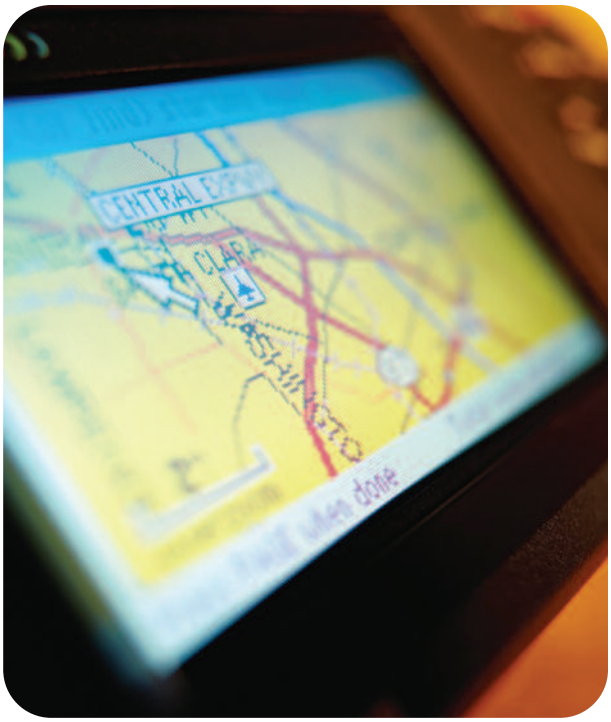
This kind of relationship building between private-sector infrastructure owners and state and local governments is crucial to detecting a cyber threat or responding to a cyber attack.

Recognize the Federal Government's Role in Cyber Security

The federal government provides valuable guidance to states on how to enhance their cyber security practices. In February 2010, the White House revised the classification guidance for the Comprehensive National Cyber Security Initiative (CNCI), which began in 2008, and is an important component of federal cyber security efforts. States can view or download an unclassified description of the CNCI.[40]

Major goals of the initiative include:

- Enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government; state, local, and tribal governments; and private-sector partners;
- Defending against threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies; and
- Expanding cyber education and redirecting research and development efforts.



The Department of Homeland Security's National Cyber Security Division is charged with building and maintaining an effective national cyberspace response system and implementing a cyber risk management program to protect critical infrastructure. The department partners with several cyber security organizations throughout the year to educate citizens on the importance of implementing effective cyber security practices. Numerous other DHS resources are available to states.

The **U.S. Computer Emergency Readiness Team** offers safety tips, incident reports, and the latest cyber alerts.

The **National Cyber Security Alliance** is a collaborative effort among experts in the security, non-profit, academic, and government fields to teach consumers, small businesses, and educators about Internet security.

The Federal Trade Commission's **OnGuard Online** website provides practical tips and downloadable materials on how to avoid Internet fraud and protect personal information.

Cyber Storm is an international cyber security exercise series that takes place every two years to assess the preparedness capabilities of governments and the private sector.


RESPOND

CHAPTER 9.

National Guard and Military Assistance

Key Concepts

- Governors have at their disposal a crucial state resource in the National Guard. These state military forces have equipment and expertise in communications, logistics, and decontamination and can serve as a key partner with the state's emergency management entity and the governor's office before, during, and after an emergency or a significant event.
- The governor and the adjutant general should review state and federal authorities regarding the use of the National Guard as well as statutory limitations found in the Posse Comitatus Act and the Insurrection Act.
- The governor should be aware of the three types of National Guard deployment (state active duty, Title 32 full-time National Guard duty, and Title 10 active duty) including how and when guardsmen can be activated.
- In 2010, the Council of Governors was formed to provide a forum for 10 state governors and key federal officials to discuss ensuring unity of effort among state and federal military forces as well as other key issues regarding National Guard missions, personnel and resources.

National Guard capabilities can be deployed to meet various needs before, during, or after an emergency or a significant event. During the 2008 presidential inauguration, for example, the National Guard was used to assist first responders and local law enforcement personnel with crowd control and civil disturbance missions, staff traffic control points, and visitor screening. Vastly different, after the earthquakes in Haiti in January 2010, the National Guard helped construct new homes, schools, and medical clinics. Winter storm emergencies in 2010 found guardsmen delivering food and water to shelters in Oklahoma, operating Humvees and heavy equipment with first responders in **Virginia**, and repairing downed power lines that were coated with ice in **Oklahoma** and **Arkansas**.

Governors have the authority to deploy the National Guard as a resource during times of need within the state. Consequently, they must understand the roles and responsibilities of the National Guard as a key partner in homeland security and emergency management efforts. Specifically, governors need to know the answers to these questions.

- What is the statutory role of the governor regarding the National Guard?
- What are legal considerations for military assistance to civilian authorities?
- What is the difference between homeland security and homeland defense?
- How is the National Guard deployed and funded?
- How does the military support states?
- How can state and federal military response activities be integrated effectively?

What Is the Statutory Role of the Governor Regarding the National Guard?

Under Article I of the U.S. Constitution, authority over the state militia (the National Guard) originates with states. States have further codified the roles and responsibilities of the governor as commander in chief through their constitutions.

Governors generally are granted the authority to deploy the National Guard to execute state law, suppress or prevent insurrection or lawless violence, and repel invasion. For example, in **Oregon**, "the governor shall be commander in chief of the military and naval forces of this [s]tate, and may call out such forces to execute the laws, to suppress insurrection, or to repel invasion."[41] In **Alabama**, "the governor shall be commander in chief of the militia and volunteer forces of this state, except when they shall be called into the service of the United States, and he may call out the same to execute the laws, suppress insurrection,

and repel invasion, but need not command in person unless directed to do so by resolution of the legislature; and when acting in the service of the United States, he shall appoint his staff, and the legislature shall fix his rank."[42]

What Are Legal Considerations for Military Assistance to Civilian Authorities?

To stem the potential for abuse or misuse of military forces, legal safeguards have been established to regulate the use of the military in providing assistance to civilian authorities. The most significant of these safeguards are the Posse Comitatus Act and the Insurrection Act.

The **Posse Comitatus Act of 1878** prohibits the use of the federal military, including National Guard units operating under federal authority, to enforce civil laws unless authorized to do so by the U.S. Constitution or federal law. The limitations on federal forces spelled out in the legislation apply only to direct application of federal military forces. Supportive and technical assistance, such as use of facilities, vessels, aircraft, and technical aid, are not restricted under the act. Nor is the use of the National Guard on state active duty status limited by its provisions.

In addition, federal legislation has been enacted to allow the military some law enforcement authority in limited circumstances.

- The military may provide assistance in drug interdiction at the request of federal or state law enforcement agencies.[43]
- Military personnel may conduct searches and arrest those involved in prohibited transactions of nuclear materials if the U.S. attorney general and secretary of defense jointly determine that the situation poses a serious threat.[44]
- At the U.S. attorney general's request, during the threat of an attack using chemical or biological weapons, the military may provide equipment necessary to detect and dispose of those weapons.[45]
- The governor of a state where a major disaster has occurred may request that the President direct military personnel to assist in emergency work to preserve life and property.[46]
- The Secret Service may request military assistance to protect the President from assault, manslaughter, or murder.[47]
- If requested by the Federal Bureau of Investigation, the military may assist in investigations of the assassination, kidnapping, or assault of a Cabinet member, a member of Congress, or a Supreme Court justice.[48]

The **Insurrection Act** recognizes that primary responsibility for protecting life and property and maintaining law and order in the civilian community is vested in state and local governments, but it authorizes the President to direct the armed forces to enforce the law to suppress insurrections and domestic violence.[49] Under these circumstances, federal military forces may be used to restore order, prevent looting, and engage in other law enforcement activities.

Since 2007, several attempts have been made to amend the Insurrection Act or otherwise expand federal authorities governing the use of National Guard and reserve forces during domestic disaster response. The John Warner Defense Authorization Act of 2007 amended the Insurrection Act to allow the President to federalize National Guard troops to "restore public order as a result of a national disaster, epidemic, or serious public health emergency."[50] The provision met with strong opposition from governors due to concerns that the President could federalize the National Guard at a time when guardsmen are most needed by the state, and it was repealed the following year.

Since then, however, the Department of Defense has sought several times to expand federal authorities to use other military forces to assist in domestic disaster response. Without clarity regarding when such forces would be used and under whose command authority, governors have remained concerned about these efforts because they could result in competing chains of command that interfere with lifesaving missions. This could lead to confusion in mission execution and the dilution of governors' control over situations with which they are more familiar and better capable of handling than a federal military commander.

To address governors' concerns, Congress called for the establishment of the **Council of Governors** to enable governors and the Department of Defense to discuss how the federal military supports civil authorities during times

of crisis. The Council of Governors consists of 10 governors who meet periodically with the secretaries of defense and homeland security as well as other senior federal officials. The Council of Governors provides a forum to discuss issues such as achieving a unified command for all military forces (state and federal) when operating domestically, coordinating military emergency response forces, and meeting the personnel, training, and equipment needs of the National Guard.

What Is the Difference Between Homeland Security and Homeland Defense?

The terms "homeland security" and "homeland defense" are defined this way:

Homeland defense is the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats, as directed by the President. The Department of Defense and the National Guard Bureau (see role of the National Guard Bureau on this page) are responsible for homeland defense.[51]

Homeland security is the concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from terrorist attacks that do occur.[52] Also, DHS has included a focus on addressing the full range of potential catastrophic events, including man-made and natural disasters (all hazards), due to their implications for homeland security.[53] The Department of Homeland Security is the lead federal agency for homeland security.

The **Idaho** Bureau of Homeland Security is one of the three divisions within the Idaho Military Division. The bureau's mission is "[to] save life and to limit human suffering, injury to wildlife, and damage to natural resources, private and public property, the environment, and the economy as a result of the harmful effects of natural and man-caused disasters, from all hazards, including terrorism and the use of weapons of mass destruction, in support of local governments and communities."[54]

The National Guard straddles both these missions. In some states, the adjutant general, who serves as the state's most senior military official and oversees state homeland defense resources, is also appointed as the homeland security advisor or emergency manager. For example, in **Washington**, the state's homeland security apparatus is embedded in the Washington Military Department. The office of the direc-

The National Guard Bureau (NGB) is a joint activity of the Department of Defense. The Chief of the National Guard Bureau serves as a principal advisor to the Secretary of Defense. The mission of the NGB is to participate with the Army and the Air Force staff in the formulation, development, and coordination of all programs, policies, concepts, and plans pertaining to or affecting the National Guard and to assist the states in the organization, maintenance, and operation of their National Guard units so as to provide trained and equipped units capable of immediate expansion to war strength in time of war or emergency. As part of its homeland defense mission, the NGB identifies 10 essential core capabilities for the National Guard to ensure readiness to assist in the response to a natural or man-made disaster. These capabilities include: a Joint Force Headquarters for command and control, a Civil Support Team for chemical, biological, and radiological detection, engineering assets, communications, ground transportation, aviation, medical capability, security forces, logistics, and maintenance capability.

tor is responsible for strategic planning, homeland security, and policy-related interaction with the executive and legislative branches of local and state governments and the federal government.

As a federal asset, the National Guard also plays an important role in defense missions at home and abroad and has played a critical role in the wars in Afghanistan and Iraq. At one point, more than 40 percent of the units involved in the Iraq War were National Guard members, and the Air National Guard continues to fly missions under North American Aerospace Defense Command control in defense of North American air space.

How Is the National Guard Deployed and Funded?

The National Guard can be deployed in disaster situations through several mechanisms. These include deploying on state active duty, deploying under Title 32 status, and deploying under Title 10 status. Each mechanism has benefits and drawbacks related to roles and funding.

In state active duty status and under Title 32 status, governors are clearly in command and control of the National Guard in their respective state or territory. National Guard troops in a Title 10 status have been used primarily to deploy in times of war and national crises. Some experts believe the National Guard would be more effective under state active duty status or Title 32 status when performing domestic missions.

State Active Duty

When deployed on state active duty status, the governor retains command and control of all National Guard forces inside his or her state. The governor can activate National Guard personnel to state active duty in response to natural or man-made disasters or for homeland defense missions. State active duty is based on state statute and policy, and the state is responsible for all costs relating to the deployment. A key aspect of state active duty status is that the Posse Comitatus restrictions on National Guard activities do not apply.

Title 32 Full-Time National Guard Duty

Full-time National Guard duty means training or other duty, other than inactive duty, performed by a member of the National Guard. Title 32 allows the governor, with the approval of the President or the secretary of defense, to order a guard member to duty for operational homeland defense activities. The key to a Title 32 deployment is that it provides the governor with the ability to place a soldier in a full-duty status under command and control of the state but directly funded with federal dollars. This status, even though funded directly by the federal government, is

not subject to the Posse Comitatus restrictions and enables a governor to use the National Guard in a law enforcement capacity.

Title 10 Active Duty

When in Title 10 status, the National Guard is under the command and control of the President, and the federal government is responsible for all associated costs of the deployment. The President can federalize National Guard troops under Title 10 when the state (the legislature or the governor, if the legislature cannot be convened) requests, through the U.S. attorney general, federal military assistance under 10 U.S.C. Chapter 15 in the event state and local police forces, including the National Guard operating under state control, are unable to adequately respond to a civil disturbance or other serious law enforcement emergency. The President may also use the military in a state to enforce federal law or protect constitutional rights. Under Title 10 authority, the President may federalize and deploy all or part of any state's National Guard.

The main limitation on National Guard members operating under a Title 10 deployment is that the forces would be limited by Posse Comitatus restrictions to providing support functions such as logistics or communications. In times of disaster, particularly in a catastrophic event, the military's police units are in high demand to maintain law and order in the disaster zone. Under Title 10, National Guard forces could not perform those functions.

How Does the Military Support States?

During the response to a domestic incident, the governor may use the National Guard to assist in response operations, in support of the local incident commander and/or the state's emergency management organization. Pursuant to the National Response Framework, which lays out the roles and responsibilities of federal, state, and local governments as well as private and nonprofit entities during an incident response, the governor may request federal assistance through the Federal Emergency Management Agency (FEMA). FEMA coordinates all requests from a governor for federal assistance and will coordinate with the Department of Defense (DoD) as it determines how best to fulfill requests for military assistance.

When additional federal military support is requested by a governor and approved by the Department of Defense, the U.S. Northern Command (USNORTHCOM) provides command and control of DoD homeland defense efforts and coordinates defense support to civil authorities. Civil support missions include domestic disaster relief operations that occur during fires, floods, hurricanes, earthquakes, and counterdrug operations. They also include managing the consequences of a terrorist attack that involves a weapon of mass destruction. In providing civil support, USNORTHCOM generally operates through its subordinate joint task forces. An emergency must exceed the capabilities of local, state, and federal agencies before USNORTHCOM becomes involved. In most cases, support will be limited, localized, and specific.‡

One of the standing joint task forces operating under USNORTHCOM is the Joint Task Force Civil Support (JTF-CS), the only military organization dedicated to planning and integrating DoD forces for consequence management to support civil authorities during disasters. Composed of active, reserve, and National Guard members from the Army, Navy, Air Force, Marines, and Coast Guard, as well as civilian personnel, the JTF-CS is charged with saving lives, preventing injury, and providing temporary critical life support during a chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE) situation in the United States or its territories and possessions. The task force is commanded by a federalized Army National Guard general officer.

Additional resources available to states include several National Guard and other federal military support teams capable of providing support in the event of a CBRNE incident. One such resource is the weapons of mass destruction **civil support teams** (CSTs). The teams are federally funded, specially trained National Guard units that can augment local and regional terrorism response capabilities. CSTs can provide rapid analysis of chemical or radiological hazards and identify biological agents at an incident involving weapons of mass destruction. The CST is broken down into six sections: command, operations, survey, medical, communications, and logistics/administration. Each state and territory has at least one CST composed of 22 full-time soldiers and airmen with technical training by agencies that include the National Fire Academy, Department of Defense, Department of Energy, and Environmental Protection Agency.

‡One exception to this construct is counter-drug operations in which Joint Task Force North (JTF-N) provides direct support to U.S. Customs and Border Protection within DHS and works directly with states' National Guard in performing its mission on behalf of USNORTHCOM.

In addition to CSTs, the governor may also use National Guard **CBRNE enhanced response force packages** (CERFPs). CERFPs are regional task forces composed of 186 personnel that build on the capabilities of CSTs to provide search and rescue, patient and mass casualty decontamination, and emergency medical services to support civilian response agencies. The 17 CERFPs can be deployed to an incident scene within six hours and may be used under state active duty, Title 32, or Title 10 authorities.

The Quadrennial Defense Review released in February 2010 also directed the establishment of 10 regional **homeland response forces** (HRFs) to provide additional resources in the event of a large-scale incident that overwhelms other response capabilities. The HRFs are intended to provide lifesaving capabilities within 48 hours of a CBRNE event. Each FEMA region will have an assigned HRF composed of 566 National Guard members. Once established, each HRF will be capable of responding to an event within six hours to provide capabilities such as CBRNE assessment, search and rescue, decontamination, emergency medical services, security, logistics support, and support for command-and-control operations. These forces will be available and under the control of the governor.

Similar federal response forces, called CBRNE **consequence management response forces** (CCMRFs), may also be called on for assistance. In contrast to CSTs, CERFPs, and HRFs, however, CCMRFs are a Title 10 federal capability. One CCMRF is composed of 5,200 personnel who can deploy to an incident scene within 24 to 48 hours to provide the same capabilities as an HRF. Two additional CCMRFs can deploy to an incident scene within 96 hours to provide more limited command-and-control support.

How Can State and Federal Military Response Activities Be Integrated Effectively?

Integrating federal military forces with those of the state is critical to an effective and efficient response. Several strategies have been pursued to accomplish this goal, including joint exercises.

A recent development in integrated command and control is the dual-status command concept. With the consent of the governor and the authorization of the President, a dual-status commander may be appointed to command both Title 10 federal forces and National Guard forces operating in a Title 32 status or on state active duty. This structure provides both the federal and state chains of command with a common operating picture and common mission-tasking authority. In practice, the dual-status commander can either be a Title 10 federal active duty officer or a Title 32 or state active duty National Guard officer. The dual-status commander concept has been used at national special security events, including the 2009 presidential inauguration, the G-20 summit in Pittsburgh, and the Democratic and Republican national conventions.

CHAPTER 10.

Mutual Aid

Key Concepts

- Mutual aid between and among states is critical to supplement emergency response capabilities, capitalize on economies of scale, and avoid exhausting resources during a disaster or an emergency.
- Strong intrastate mutual aid agreements should be implemented to support local responders during response and recovery.
- The Emergency Management Assistance Compact provides the governance structure and mechanism for rapid interstate mutual aid, facilitates recognition of out-of-state medical licenses, clarifies reimbursement processes, and addresses liability claims.

Disasters and emergencies can quickly exhaust or overwhelm the resources of a single jurisdiction at either the local or state level. As a result, municipalities and states have developed mutual aid agreements to supplement one another's response capabilities with additional personnel, equipment, and expertise. Mutual aid agreements also are a necessary component of an effective response to incidents that cross political and jurisdictional boundaries.

At the local level, where fire and police department personnel support their colleagues in neighboring municipalities on a routine basis, mutual aid agreements are well established and well tested. These agreements specify the type of assistance to be provided under specific circumstances, describe the triggers and mechanisms for obtaining assistance, and provide a mechanism for ensuring member jurisdictions are compensated for the assistance they provide. Interstate mutual aid agreements address these same issues, but state differences in workers' compensation and liability laws and in licensing procedures and standards for some professionals, complicate matters.

Governors need to ensure their state has robust intrastate and interstate mutual aid agreements to support jurisdictions as they respond to natural disasters, criminal acts, and acts of terrorism. Most states have a solid history of participating in mutual aid agreements with neighboring states, and governors should be aware of existing agreements in which their state participates and the legal foundation of those agreements. The Emergency Management Assistance Compact is a mutual aid agreement to which most states subscribe. Yet governors should not discount other interstate mutual aid agreements or public-private partnerships for mutual aid.

Intrastate Mutual Aid

When confronted with a large-scale emergency or potential disaster, governors first look within their borders to determine whether assets and resources are available to support the jurisdictions involved in the immediate response. Most jurisdictions have standing agreements with their neighbors to share assets and resources on a routine and emergency basis. Moving equipment and personnel from one part of the state to another, however, can be more complicated because agreements about cost reimbursement may not be in place.

In the wake of the September 11 terrorist attacks, the Department of Homeland Security contracted with the National Emergency Management Association (NEMA) to develop model intrastate mutual aid legislation for states to consider as they develop or refine statewide mutual aid agreements.[55] The model law, published in 2004, addresses issues such as:

- Member party responsibilities;
- Implementation;
- Limitations;
- License, certificate, and permit portability;
- Reimbursement;
- Development of guidelines and procedures;
- Workers' compensation; and
- Immunity.

In 2001, several states already had, or have since developed, statewide mutual aid agreements. In April 2002, for example, **Iowa** introduced a voluntary statewide mutual aid program known as the Iowa Mutual Aid Compact (IMAC). Modeled on the national Emergency Management Assistance Compact, IMAC establishes a system through which political subdivisions can help one another during disasters that have been declared by local officials or the governor. **Kansas** has a similar statewide mutual aid system that was created in the 2006 Kansas Intrastate Mutual Aid Act. The act provides for a system of intrastate mutual aid among participating political subdivisions in cases of declared disasters as well as during drills and exercises in preparation for such disasters.

In **Illinois**, meanwhile, the fire service developed and implemented a mutual aid system that began in the northern part of the state but has since expanded to all of Illinois, southern Wisconsin, and parts of Indiana. The Mutual Aid Box Alarm System (MABAS) involves hundreds of fire departments and provides an orderly system for dispatching fire and emergency medical services equipment and personnel to fires, accidents, or other incidents. Equipment is moved among participating jurisdictions according to predetermined lists, known as "box cards." Each box card covers specific equipment for specific types of incidents in specific areas. The system is managed through geographic divisions, through which local fire departments can access assistance. From its inception, MABAS included procedures for ensuring the integration of assisting personnel and equipment into the local command structure.

Ohio has a web-based application to identify law enforcement and fire personnel and equipment statewide. The database can be searched before an incident to locate resources for the planning or purchasing process. During an incident, an agency can call a predetermined call center for any amount of resources. The database identifies the closest resources, electronically notifies the agency, and sends essential information, including maps. Requesting agencies can monitor the website and view real-time response of mutual aid.

Interstate Mutual Aid

When incidents overwhelm the response capabilities of a state, governors may need to look beyond state borders for assistance. Mutual aid agreements exist on a state-to-state basis in the areas of law enforcement, drug interdiction, and wildfire suppression. Interstate mutual aid in the area of disaster response and recovery now generally comes through the Emergency Management Assistance Compact. This congressionally approved, nationwide compact is operationally controlled by the states through their respective state emergency management agency.

Role of the Emergency Management Assistance Compact

In August and September 2005, equipment, supplies, and personnel flowed from across the nation into **Alabama**, **Louisiana**, **Mississippi**, and **Texas** in the wake of Hurricane Katrina and Hurricane Rita. This influx of assistance was largely the result of the Emergency Management Assistance Compact (EMAC), which provides the structure and mechanisms for the rapid movement of equipment, supplies, and personnel across state lines.

EMAC addresses most challenges to interstate mutual aid, including these:

The acceptance of out-of-state medical licenses. EMAC states that when a person holds a license, certificate, or other permit issued by any state party to the compact, that person shall be deemed licensed, certified, or permitted by the state requesting assistance, subject to limitations and conditions prescribed by the governor of the state requesting that assistance.[56]

The recovery of costs incurred by states providing assistance. EMAC provides that any state providing assistance to another state under the compact will be reimbursed by the state receiving the assistance for costs related to the provision of that assistance.[57]

Legal liability claims that arise from the activities of out-of-state workers. EMAC states that officers or employees of a party state rendering aid in another state pursuant to the compact are considered agents of the requesting state for tort liability and immunity purposes.[58]

Workers' compensation payments in the event those out-of-state workers are injured or killed while responding to the disasters or emergencies. EMAC states that each party state shall provide for the payment of compensation and death benefits to injured members of the emergency forces of that state and representatives of deceased members of those emergency forces in the same manner and on the same terms as if the injury or death were sustained within their own state.[59]

In short, EMAC provides for "mutual assistance between states . . . in managing any emergency or disaster that is duly declared by the governor of the affected state(s), whether arising from natural disaster, technological hazard, man-made disaster, civil emergency aspects of resource shortages, community disorders, insurgency, or enemy attack."[60]

EMAC dates back to Hurricane Andrew in 1992. In the wake of that storm, former Florida Governor Lawton Chiles initiated a mutual aid compact among states in the southeast United States. Participating governors amended the agreement to open participation to all states, creating the Emergency Management Assistance Compact. The 104th Congress ratified the interstate agreement in 1996 with the passage of House Resolution 193 (PL 104-321). In 2006, Hawaii became the 50th state to join the compact,

How EMAC Works and the Benefits of Membership

The Emergency Management Assistance Compact is administered by the National Emergency Management Association (NEMA), which provides the day-to-day support and technical backbone for the compact. During emergencies, NEMA staff work directly with EMAC members to ensure requests for assistance are fielded quickly and effectively in order to maximize relief efforts.

The trigger for assistance under EMAC is a declaration of emergency by the governor of the affected state. Once that declaration is made, the EMAC assistance process can be set into motion. The process involves several steps.

- An authorized representative of the affected state contacts the EMAC National Coordinating Group.
- The affected state requests the deployment of an A-Team to facilitate assistance.[61]
- The A-Team works with the state to determine needs and sends an EMAC broadcast requesting assistance from member states.
- The A-Team helps the state determine costs and availability of resources.
- States complete requisitions and negotiation of costs.
- Resources are sent to the requesting state.
- Upon arriving home, the resource providers submit their reimbursement package to the assisting state emergency management agency, which completes an audit of the reimbursement package and then seeks reimbursement from the requesting state.

Participation in EMAC does not reduce federal disaster assistance to states, and participating states receive several benefits as a result of their membership in the compact. In fact, EMAC:

- Supplements federal assistance;
- Replaces federal assistance when it is not available or when a state is ineligible for funds;
- Enhances cost-effectiveness;
- Establishes standard operating procedures;
- Provides the expertise of member states;
- Guarantees reimbursement to states that provide eligible assistance; and
- Authorizes the use of the National Guard for humanitarian purposes.

EMAC is structured to afford governors the authority to pull resources into a disaster zone, rather than allow other states or organizations to flood an affected area with resources, personnel, and donations. This enables governors to maintain control over the types and sources of assistance provided and to maximize the integration of out-of-state resources into in-state incident command systems. EMAC requires states receiving assistance to accept responsibility for cost reimbursement and for liability claims, so the ability of receiving state governors to manage outside assistance is critical.

which also counts Guam, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia among its members.

To join EMAC, states were required to pass legislation approving the compact as written. This ensures that states receiving assistance under the terms of the compact are legally responsible for reimbursing assisting states and are liable for out-of-state personnel. This significantly reduces the confusion and anxiety sometimes associated with interstate mutual aid. For more information, see How EMAC Works and Benefits of Membership on page 49.

Concerns About the Emergency Management Assistance Compact

The scope and scale of destruction wrought by a major hurricane or similar disaster can seem unprecedented. For example, the scale of response to Hurricane Katrina in 2005 involved resources from across the nation. EMAC assistance in Louisiana and Mississippi included 67,006 personnel—20,085 civilian and 46,921 National Guard—and cost an estimated $845 million.[62] The complexity of the response and the number of EMAC missions fielded—estimated at more than 1,900—highlighted issues that governors should be aware of as they contemplate receiving or providing EMAC assistance during a disaster or an emergency.

Reimbursement is limited to approved EMAC missions. EMAC sets out the terms and conditions under which states will be reimbursed for costs they incur in providing assistance to another member state. In general, states providing assistance must closely track their costs and submit those costs to the receiving state, which compensates them with funding. The EMAC reimbursement process is not tied to FEMA or other federal reimbursement processes. However, if the impacted state receives a presidential disaster or emergency declaration, it may be eligible for cost reimbursement under the federal Stafford Act.

Only activities carried out under an EMAC requisition agreement signed by the requesting state and the assisting state are eligible for reimbursement. Costs incurred for activities that are outside the scope of that agreement or by response teams that "self-deploy" into a disaster zone outside the EMAC framework are not reimbursable under the terms of the compact.

Detailed record keeping and auditing are essential. The sheer number of EMAC missions carried out during the response to Hurricane Katrina illustrates the need for accurate record keeping by both receiving and assisting states. Detailed and accurate receipts, employee timesheets, and other financial documents will ease the reimbursement process, particularly in large-scale, costly events such as Hurricane Katrina. State finance and administration officers monitored the post-Katrina reimbursement process very closely, auditing reimbursement claims and rejecting those for which adequate documentation did not exist.

State and local officials should be educated about EMAC. Out-of-state teams were able to reach affected areas of the Gulf Coast efficiently through EMAC deployments. However, their integration with response crews already on the ground was complicated by the fact that many local officials, and some federal officials, were unfamiliar with EMAC and questioned or rejected the credentials of the EMAC-deployed teams. The absence of reliable communications systems in the disaster zone meant the state emergency operations center often was unaware of the problem and could not intervene on behalf of the EMAC teams.

Education at all levels of government is essential for the continued success of EMAC. Local emergency management officials, local law enforcement officials, the National Guard leadership, and federal emergency response personnel must be made aware of EMAC, its provisions, its benefits, and its limitations so out-of-state resources can quickly and efficiently be brought to bear during disasters.

Other Interstate Mutual Aid Agreements

EMAC has emerged as the gold standard in state-to-state mutual aid since its inception in the wake of Hurricane Andrew, but it is not the only vehicle for cross-border cooperation. The compact recognizes the likelihood of other arrangements and states that EMAC membership does not "preclude any state entering into supplementary agreements with another state or affect any other agreements already in force between states." Those supplementary agreements, the compact adds, could include provisions for "evacuation and reception of injured and other persons and the exchange of medical, fire, police, public utility, reconnaissance, welfare, transportation and communications personnel, and equipment and supplies."

Several other interstate mutual aid compacts or arrangements already exist, including the following.

Ratified by Congress in July 1998, the **Pacific Northwest Emergency Management Arrangement** is an interstate and international emergency management

compact among Alaska, Idaho, Oregon, Washington, and the Canadian provinces of British Columbia and the Yukon Territory.[63]

Although not an interstate compact, the **Mid-America Alliance** is a multistate framework for public health mutual assistance during situations that stress a state's resources but do not initiate a governor-declared state of emergency. Member states include Colorado, Iowa, Kansas, Missouri, Montana, Nebraska, North Dakota, South Dakota, Utah, and Wyoming. The alliance aims to establish a system by which member states can share services, resources, and information to efficiently address the needs of citizens during a public health emergency.[64]

Ratified in 2007, members of the **International Emergency Management Assistance Compact** include Quebec, Newfoundland, New Brunswick, Nova Scotia, Prince Edward Island, Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The compact established protocols to share personnel and equipment in a major emergency.[65]

Three states—Maine, New Hampshire, and Vermont—have taken the concept of the Metropolitan Medical Response System (MMRS) and applied it to a multistate region to create the **Northern New England Metropolitan Medical Response System**. MMRS is a DHS program that encourages metropolitan areas to develop a cross-jurisdictional and interagency capacity to prepare for and respond to health emergencies in their region. The three-state Northern New England MMRS aims to ensure that resources and responses of the region are coordinated to handle care locally; education, training, and exercising for the region are cooperative and coordinated; and the region can manage any surge from an event in Boston or New York.[66]

Public-Private Mutual Aid Partnerships

Partnering effectively with the private sector to improve disaster preparedness and response has only recently begun to receive attention, despite the private sector having significant involvement in disaster response. That involvement has included engaging in volunteer and donation management activities, providing emergency and long-term medical care, and reporting and disseminating information.

Recognizing that most infrastructure is privately held, the **Colorado** Emergency Preparedness Partnership brings local, state, federal, nonprofit, and private-sector stakeholders together to collaborate on emergency management issues in the state. The partnership also focuses on building communications and collaboration among the parties. It holds cross-disciplinary exercises to correct gaps in public-private response to an incident.

The **Illinois** Private Sector Alliance, an initiative of the Illinois Office of Homeland Security and the Illinois Terrorism Task Force, promotes a culture of information sharing and partnership between public safety agencies and the private sector. The alliance focuses on two key project areas: infrastructure security awareness and the mutual aid response network. The network leverages existing private-sector resources for use during an emergency by providing a clearinghouse for mutual aid agreements with state private-sector partners.

CHAPTER 11.

Interoperable Communications

Key Concepts

- Interoperability enables first responders to communicate during times of disaster. Unfortunately, despite advances since September 11, interoperability remains an ongoing concern among homeland security advisors, public safety officials, and first responders.
- The governor should appoint a statewide interoperability coordinator (SWIC) to coordinate all state public safety communications grants and activities. Likewise, statewide interoperable communications governing boards (SIGBs) should be given the authority to act and enforce statewide interoperable communications policy and plans. Many SWICs and SIGBs were created by executive orders, so new governors may want to ensure these boards and positions continue to exist following the gubernatorial transition.
- Interoperability can be enhanced through coordinated funding strategies, clearly defined state governance structures, standardization of operations, purchase of new technologies, and training.

Interoperability refers to seamless communication among emergency responders using differing systems, products, or protocols. Wireless communication interoperability is the specific ability of emergency responders to use voice and data communication in real time, without delay. For example, police, fire, and emergency medical services responding to an incident are deemed interoperable when they can all communicate with one another using different wireless communication systems. Interoperability makes it possible for first responders from any jurisdiction to communicate with those from another jurisdiction at the scene of incidents. It also enables emergency planners and personnel to coordinate their efforts in advance of major events, such as state fairs, large college sports games, or presidential visits to a state.[67]

Although governors cannot single-handedly achieve seamless communication among emergency responders, they can take these steps toward a unified effort:

- Account for recent developments in interoperability;
- Address the challenges to interoperability;
- Commit to statewide interoperability;
- Identify sustainable funding for interoperability; and
- Promote communications exercises.

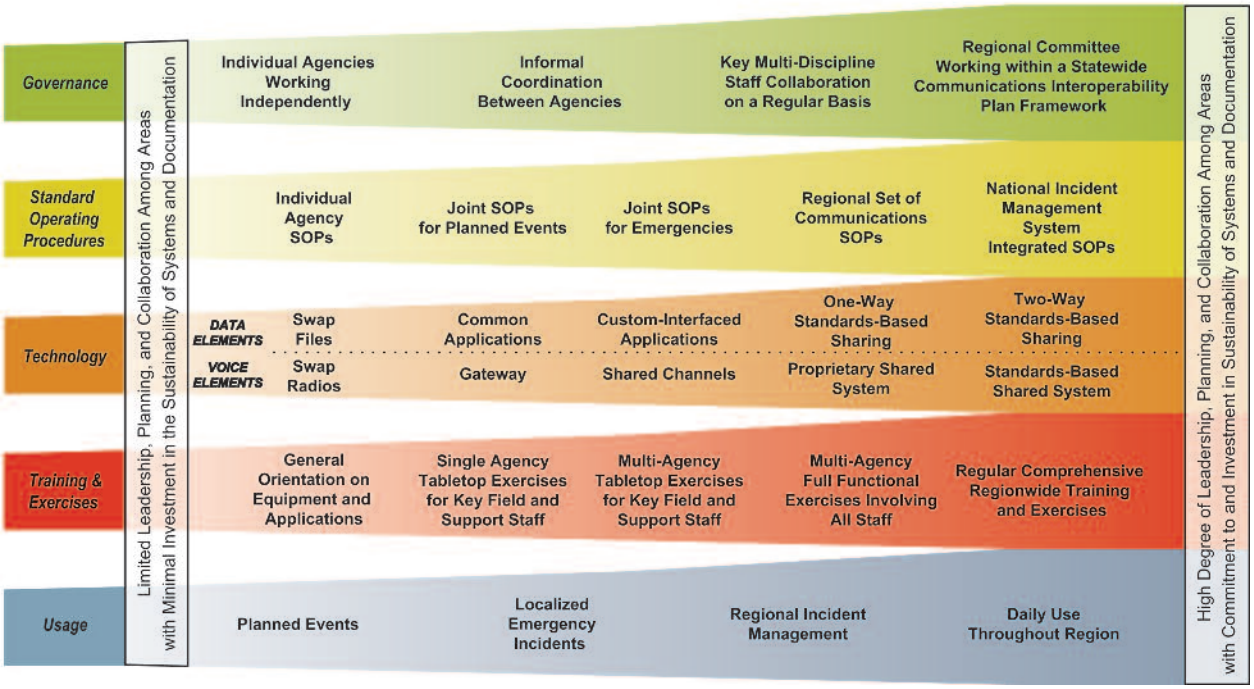
Account for Recent Developments in Interoperability

Since 2006, several developments have transpired to improve interoperable communications. Most notably, the Interoperability Continuum, developed by state and local practitioners and released through the SAFECOM Program of the U.S. Department of Homeland Security (DHS), emerged as a tool to assist decisionmakers in advancing interoperability.

The continuum demonstrates how states can advance interoperable communications by focusing their efforts on five key components: governance, standard operating procedures, technology, training and exercises, and usage (see Interoperability Continuum chart on page 53). States use the continuum to gauge annual progress toward interoperable communications capability by tracking their progress across each component. For example, developing governance models in a state requires a movement from independent agencies developing their own governance structures toward coordination of protocols among agencies. Progress through each component culminates in a highly developed interoperable communications capability that will be of use to the state.

All states were required to submit a statewide communications interoperability plan (SCIP) to the DHS Office of Emergency Communications by December 2007 to qualify for funding assistance under the Public Safety Interoperable Communications grant. This one-time grant provided upwards of $1 billion to states to develop their interoperable communications. Through this funding, all states, territories, and the District of Columbia developed a statewide communications interoperability plan using

Interoperability Continuum



Source: U.S. Department of Homeland Security, SAFECOM, "Interoperability Continuum: A Tool for Improving Public Safety and Interoperability," (Washington, DC: U.S. Department of Homeland Security, September 21, 2010).

consistent criteria based on the Interoperability Continuum. The SCIP addresses all aspects of the statewide strategy and implementation needed to achieve interoperability and highlights areas that are deficient.

In July 2008, DHS released the National Emergency Communications Plan (NECP), developed in collaboration with state, local, and tribal stakeholders. NECP provides a national roadmap that incorporates statewide plans for advancing interoperability from the user perspective. It also provides guidance to all first responders on interoperability issues and fosters development along the Interoperability Continuum.

Address the Challenges to Interoperability

States have made significant progress by creating plans consistent with the criteria they helped develop, but additional work is needed to achieve full interoperability across the nation. Governors can provide the vision and leadership necessary to create statewide interoperable public safety communications. They can build support at the federal, state, and local levels for the investments and coordination needed to achieve interoperability. Several policy actions are important to promote statewide interoperability:

- Strengthen governance by gaining commitments from all disciplines in the state through a statewide interoperability coordinator;
- Lay the foundation for sustainable long-term funding by planning and budgeting for ongoing updates to systems, procedures, and documentation; and
- Develop routine exercises for interoperable communications.

Commit to Statewide Interoperability

Interoperability requires the commitment of leadership from the public safety community. Leadership buy-in fosters agency-wide support and acceptance of new interoperability methods. A statewide interoperability governing body (SIGB) is a useful coordinating tool to gain commitment and buy-in. Most states use a SIGB, or a state interoperability executive committee, to administer interoperability programs in state government. This multidisciplinary committee—created by formal legislation or executive order—brings diverse opinions and expertise to state interoperability efforts. For example, **Arkansas** formed the Arkansas Wireless Information Network to gain leadership commitments from state emergency management, county and local courts, local fire chiefs, sheriffs and police chief associations, and state information technology and finance departments to develop and oversee a statewide public safety radio system.[68]

In 2007, **Minnesota** Governor Tim Pawlenty signed an executive order establishing the statewide radio board (SRB) as Minnesota's statewide interoperability executive committee. SRB established an Interoperability Committee with state, regional, local, tribal, and federal representation to address broader issues of public safety communications interoperability within the state, among states, and along the Canadian border.[69]

The governor or SIGB should name a statewide interoperability coordinator (SWIC) who is responsible for the coordination, communication, and promotion of interoperability efforts throughout the state. The roles and responsibilities of the SWIC will vary by state, but typically they include program management, outreach to stakeholders, grants management and policy development, and development of metrics to assess interoperability progress. Although the ultimate goal of the SWIC is full interoperability on a statewide scale, considerable achievements have occurred during the interim, including working to meet the goals of the NECP.

Identify Sustainable Funding for Interoperability

States are taking a comprehensive approach to funding interoperable communications projects. Instead of piecemeal funding of interoperable communications through agencies or jurisdictions, states are integrating state and federal funding streams. They also are developing novel ways to fund interoperability. Some states have used 911 service fees to pay the debt service on bonds used to construct the statewide system and to provide funding for the statewide interoperability program and the operation and maintenance costs of the system.

To ensure continued revenue for interoperability maintenance, **Indiana**'s Project Hoosier SAFE-T is funded by a $1.25 surcharge on all department of motor vehicles transactions. To maximize the impact of limited federal, state, and local funding, **Arizona** encourages regional partnerships to leverage funds while aligning individual agency and community priorities with statewide needs.

Promote Communications Exercises

Radio equipment is useless to the first responder unless accompanied by regular exercises. Exercises maintain equipment, expose vulnerabilities in planning, and increase the knowledge, skills, and abilities of end users to effectively use interoperable technology. An optimal exercise program includes orientations, tabletop exercises for single and multiple agencies, functional exercises of a particular task, routine comprehensive regional training, and full-scale exercises.

CHAPTER 12.

Major Disaster and Emergency Declarations

Key Concepts

- All requests to the President for supplemental federal assistance under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act) must be made by the governor of the affected state. The governor's request should be based on the finding that the disaster is of such severity and magnitude that effective response is beyond the capabilities of the state and local government.
- The National Response Framework (NRF) details how government at all levels should respond to incidents of various magnitudes. NRF provides greater flexibility than its predecessor, enabling continuous development and refinement of all-hazards emergency operations plans.
- In catastrophic situations, including acts of terrorism, governors should expect significant involvement of high-level federal officials from various agencies.

Most incidents in a state do not reach sufficient magnitude to merit a presidential disaster or emergency declaration. However, when state and local resources are insufficient to respond to and recover from a situation, a governor may ask the President to declare a disaster or emergency.

The amount and extent of federal assistance, as well as the state's share of the response and recovery costs, are different for major disaster declarations and emergency declarations. A **presidential disaster declaration** sets in motion long-term federal recovery assistance programs—some of which are matched by state programs—to help disaster survivors, businesses, and public entities. A **presidential emergency declaration** provides emergency federal assistance for measures undertaken for conducting lifesaving measures.

Congressional appropriations determine the amount of federal assistance available. Under a federal disaster declaration, states are required to cover no more than 25 percent of the eligible response and recovery costs. For an emergency, the amount of federal assistance is initially limited to $5 million per declaration. When the $5 million limitation is exceeded, the President is required to report to Congress on the nature and extent of emergency assistance requirements and shall propose additional legislation, if necessary. The state's share of the costs for an emergency declaration may be no more than 25 percent of the eligible costs.

The National Response Framework (NRF) details how government at all levels should respond to incidents of various magnitudes. NRF provides greater flexibility than its predecessor, enabling continuous development and refinement of all-hazards emergency operations plans (see Role of the National Response Framework on page 56).

When an incident occurs in a state, members of the media and the public will closely examine the governor's immediate reaction, including how well he or she interacts with the federal government. Governors are more likely to be viewed as leading a positive state response if they:

- Understand differences in disaster and emergency definitions;
- Take appropriate actions prior to requesting a presidential declaration;
- Request a major disaster declaration, if needed;
- Request an emergency declaration, if needed; and
- Know what federal resources can be deployed after declaration of a disaster or an emergency.

Understand Differences in Disaster and Emergency Definitions

The Robert T. Stafford Disaster Relief and Emergency As-

Role of the National Response Framework

The National Response Framework (NRF) is a guide that details how federal, state, and local governments will respond to incidents of all sizes, from routine accidents to catastrophes. NRF builds on and supersedes the National Response Plan (NRP), which was published in 2004. NRF provides more flexibility than its predecessor and enables ongoing development and refinement of all-hazards emergency operations plans. NRF defines and outlines key response principles, identifies roles and responsibilities of agencies at various levels of government, and describes how communities, states, the federal government, and the private sector should apply those principles for a coordinated, effective response.

Although the principles stated in NRF apply to an incident of any size, the document serves as the outline for how the federal government will respond to an incident that results in a presidential declaration of a major disaster or an emergency. NRF provides the mechanism for coordinating delivery of federal assistance and resources to augment the efforts of state and local governments overwhelmed by a major disaster or an emergency; supports implementation of the Stafford Act and individual agency statutory authorities; and supplements other federal emergency operations plans developed to address specific hazards.

sistance Act, generally known as the Stafford Act, authorizes the President to provide financial and other forms of assistance to eligible state and local governments, certain private nonprofit organizations that provide essential government services, and individuals to support response, recovery, and mitigation efforts following presidentially declared major disasters and emergencies. The Stafford Act describes the declaration process, the types and extent of assistance that may be provided, and assistance-eligibility requirements.

The Stafford Act defines a major **disaster** as "any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this [a]ct to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby."[70]

Less severe than a major disaster, the Stafford Act defines an **emergency** as "any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States."[71]

Take Appropriate Actions Prior to Requesting a Presidential Declaration

As a prerequisite to disaster assistance under the Stafford Act, the governor must take appropriate response action under state law and carry out the state's emergency plan. If the governor is considering asking the President to declare a major disaster or an emergency, state emergency management officials in cooperation with local officials, should:

- Survey the affected areas to determine the extent of private and public damage;
- Request and conduct joint preliminary damage assessments with FEMA officials;
- Estimate the types and extent of federal disaster assistance required;
- Consult with the FEMA regional administrator on eligibility for federal disaster assistance; and
- Inform the FEMA regional office if the governor intends to request a declaration from the President.

Request a Major Disaster Declaration, If Needed

The FEMA regional office will deploy a team of federal officials to assist the state in determining if a request to the President is warranted. Only the governor has the authority to initiate a request for a presidential disaster declaration. This request is made through the FEMA regional administrator, in accordance with the Stafford Act and its implementing regulations. The governor bases the request on a finding that the situation is of such severity and magnitude that an effective response is beyond state, local, and tribal government capabilities and that federal assistance is necessary to supplement the efforts and available resources from the state.

The request for a disaster declaration should include:

- Confirmation that the governor has taken appropriate action under state law and carried out the state emergency plan;
- Information on the extent and nature of state resources that have been or will be used to address the consequences of the disaster;
- A certification by the governor that state and local governments will assume all applicable nonfederal costs required by the Stafford Act;
- A preliminary estimate of the types and amounts of supplementary federal assistance required; and
- Designation of the state coordination officer for purposes of coordinating response and recovery operations on behalf of the governor.

The completed request should be addressed to the President and sent to the FEMA regional administrator within 30 days of the incident, who will evaluate the damage and requirements for federal assistance and make a recommendation to the administrator of FEMA. The administrator of FEMA will then recommend a course of action to the President. The governor, appropriate members of Congress, and federal agencies are immediately notified of a presidential declaration.

Request an Emergency Declaration, If Needed

For events that occur or threaten to occur that do not qualify as a major disaster, the governor may request an emergency declaration to obtain federal assistance to save lives; protect property, public health, and safety; or lessen or avert the threat of a catastrophe. This request is made through the FEMA regional administrator, in accordance with the Stafford Act and its implementing regulations. The process for requesting an emergency declaration is similar to the process for requesting a major disaster declaration, except the time in which to submit an emergency declaration request generally is shorter. The request must be submitted within five days after the need for assistance becomes apparent, but no longer than 30 days after the incident occurs.

The governor's request should contain specific information describing state and local efforts and resources used to alleviate the situation. The request should also include information on the extent and type of federal assistance that is necessary. States are encouraged to consult with the FEMA regional office when preparing their request. The governor has the right to appeal if the request for a declaration is denied or if the request for approval of certain types of assistance or designation of certain affected areas is denied.

As detailed in the Stafford Act, a declaration of emergency allows federal agencies assisting state and local governments to use federal equipment, supplies, facilities, and personnel to:

- Lend or donate food or medicine;
- Remove debris;
- Engage in search and rescue activities;
- Provide emergency medical care and emergency shelter;
- Assist in the movement of supplies and persons (e.g., clearance of roads and construction of temporary bridges);
- Provide temporary facilities for schools;
- Demolish unsafe structures; and
- Disseminate public information.

Know What Federal Resources Can Be Deployed After a Declaration

Following a presidential disaster declaration, a wide array of federal assets can be deployed as needed. FEMA may deploy incident management assistance teams (IMATs), which are interagency, regionally based response teams that provide a forward federal presence to improve response to serious incidents. IMATs support efforts to meet state and local needs, possess the capability to provide initial situational awareness for federal decisionmakers, and support the establishment of federal and state coordination efforts.

FEMA can deploy still other initial response and coordination tools in conjunction with declared emergencies and disasters, including these.

- **Hurricane liaison team.** This small team is designed to enhance hurricane disaster response by facilitating information exchange among the National Oceanic and Atmospheric Administration's National Hurricane Center, and federal, state, and local government officials.
- **Urban search and rescue (US&R) task forces.** The National US&R Response System is a framework for structuring local emergency services personnel into integrated response task forces.
- **Mobile emergency response support.** The primary function of this support is to provide mobile telecommunications capabilities and life support, operational support, and power-generation support, and logistics required for the onsite management of response activities.

The federal government maintains diverse resources and capabilities that can be made available at the governor's request. When an incident occurs that exceeds or is anticipated to exceed state resources, the federal government may provide resources and capabilities to support the state response. These include, for example:

- Initial response resources, including food, water, and emergency generators;
- Emergency services to clear debris, open critical transportation routes, and provide mass shelter and feeding;
- Loans and grants to repair or replace damaged housing and personal property for uninsured or under-insured individuals;
- Grants to repair or replace roads and public buildings (incorporating, to the extent practical, hazard-reduction structural and nonstructural measures);
- Technical assistance to identify and implement mitigation opportunities to reduce future losses; and
- Crisis counseling, tax relief, legal services, unemployment insurance, and job placement.

During catastrophic situations, including major acts of terrorism, the participation of federal agencies will be greater than in smaller events, which may only include FEMA. In catastrophic incidents, governors should expect the White House and Congress to take a direct interest in response and recovery activities. In the event of a catastrophic incident, the governor may request an expedited declaration.

CHAPTER 13.

Public and Media Communications

Key Concepts

- Governors should clearly define roles and responsibilities for themselves, their chief of staff, their communications director, and other key staff during a disaster or an emergency.
- The most important role of the governor is to set realistic expectations among survivors and provide comfort through words and actions. The chief of staff can serve as the "enforcer" of state government's efforts to convey a single message to the media during a disaster or an emergency.
- During an incident, the governor's communications director should compile and disseminate consistent and accurate information to the public through established media outlets. Social media networks should also be considered for communicating important information to state residents.

An effective public communications strategy is essential to any incident response and should be developed as a key component of any emergency response plan. Absent adequate preparation and coordination during an event by the governor's chief of staff, communications director, and agency public information officers, rumors can spread and facts can be misrepresented, resulting in confusion, a lack of trust, and a possible loss of control over the situation. The public communications strategy should be tailored to the type of incident (i.e., a natural disaster, a criminal act, or an act of terrorism).

An incident that is the result of a criminal act or act of terrorism makes communicating to the public more complex because of concerns about jeopardizing an ongoing investigation. Homeland security advisors assist the governor with counterterrorism efforts, including intelligence gathering. They should be at the center of the discussion when determining how to communicate sensitive information to the public.

Media coverage of disasters has led to increased public expectations of government response. The press is eager to report what the government is doing—and not doing—to deal with the situation. Disasters and emergencies provide dramatic live images for the media and evoke strong emotions from the public. Consequently, governors need a strategy for managing those emotions and expectations. The strategy should include:

- Making a quick, initial statement within 30 minutes of an incident (a delay of more than 30 minutes could cause the media to rely on other sources of information);
- Establishing a joint information center with involved agencies;
- Clearly establishing who speaks about what and when;
- Establishing a regular schedule of statements;
- Monitoring the media closely;
- Correcting erroneous reports; and
- Preparing for "who's to blame" questions.

Essential to the successful implementation of this strategy is deciding on the roles of the governor, chief of staff, and communications director. In addition, governors should consider how they want to use the state's joint information center and social media technologies to communicate effectively about a disaster or an emergency.

Governor's Role in Effective Communications

Governors have unique access to the media and should use that access to provide information to the public through scheduled press briefings, televised appearances, and radio announcements.

Initial messages should express compassion and be designed to assure the public that:

- The seriousness of the situation is recognized;
- Someone is in charge; and
- All reasonable steps are being taken to respond.

Governors should ensure that lines of communication with the press and public remain open so questions receive prompt responses and inaccurate information can be corrected before it spreads. It is equally important for a governor or his or her representatives to communicate with victims and their families. If survivors do not know where to turn for help, they become frustrated. Telling people specifically where to get help is among the most important information a governor can provide.

The decision to visit a disaster site should be made deliberately in consultation with the homeland security and emergency management team. The governor's presence can go a long way to calming and reassuring the community during and after a disaster. Survivors, victims' families, and other citizens will look to the governor for leadership and reassurance. However, 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. A governor's presence can also set unrealistic expectations that government programs or assistance may be forthcoming when, in fact, they will not. The most important role of the governor is to set realistic expectations among disaster survivors and to provide comfort through both words and actions.

A governor's actions during the early stages of a disaster often will set the tone for the state's response (see The First 72 Hours . . . on page 61). All disasters are local, so the governor will want to involve and coordinate with local officials. However, incidents that are the result of a criminal or terrorist act will require a delicate balance of coordination with local governments, media outlets, and law enforcement agencies.

Chief of Staff's Role in Effective Communications

Often the chief of staff serves as a secondary media contact for the governor's office, especially during emergency situations. As an extension of the governor, the chief of staff is well positioned to meet this occasional need.

A more important media role for the chief of staff is to serve as the "enforcer" of state government efforts to convey a single message to the media during a disaster or an emergency. Although this role typically is performed by the communications staff during small or moderately sized incidents, larger incidents may require additional assistance. In this event, the chief of staff can help ensure cabinet officials and other members of the governor's staff know the correct media protocols and messages during a disaster or an emergency.

Communications Director's Role in Effective Communications

The governor's communications staff spends most of their time accentuating the positive and ensuring reporters see the best of state government. When incidents happen, staff can be unprepared for the ensuing challenges. Communications directors should take time to read the state's emergency plan, learn the established procedures, and familiarize themselves with the roles assigned to state officials in responding to disasters or emergencies.

During a disaster or an emergency, the governor's communications director maintains critical lines of communication among the governor's office and emergency personnel, survivors, the press, state and local officials, and the federal government, all of whom want to be first in line for the latest information. Communications directors have the enormous challenge of compiling and disseminating consistent, accurate information.

The First 72 Hours . . .

Consider this description of actions that governors should consider during the first 72 hours of an event such as landfall of a hurricane.

Day 1. During the first day of an emergency, the governor should make an announcement, in person or through a press release, stating that information is being collected and the state is working with the affected local jurisdictions. The announcement should indicate that the governor has deep compassion and empathy for those affected and is in charge of the situation, that there is a unified plan in action, and that information on further developments will be forthcoming. Compiling and disseminating consistent, accurate information can be an enormous challenge. To avoid communicating misleading or incomplete information, the governor should not provide a detailed assessment until adequate data have been collected.

Day 2. 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 state emergency operations center, incident command post, or disaster site. The governor's representative should not make specific promises for recovery assistance. Statements should be carefully framed to indicate that state and federal aid, if appropriate, are available to those who qualify. The governor's communications director should begin to think about a coordinated message with FEMA's regional office regarding federal aid.

Although questions can be expected from reporters about how this emergency compares with others of its type, experience shows that accurate comparisons are difficult, if not impossible. Comparisons should be avoided, especially at the beginning of a disaster. If safe and appropriate, the governor should consider visiting the site affected. The governor's presence at the scene can graphically demonstrate his or her concern and the seriousness with which he or she is treating the event. It may also bolster the spirits of citizens affected by the disaster. Local officials, as well as technical experts such as the homeland security advisor or personnel from the state's emergency management office and relevant state agencies, should join the governor. These experts can handle technical questions concerning long-term damages and state aid. The governor needs to be cognizant of not creating the perception of an overly staged press conference that could come across as self-serving.

Day 3 and Thereafter. The governor's involvement and presence should not end suddenly with his or her return to the state capital. Those affected by the disaster need to know the emergency is still a top priority and the governor is doing everything possible to provide assistance. A daily press release should indicate onsite personnel are keeping the governor apprised of the situation. These releases should be coordinated with the homeland security organization's and/or state emergency management agency's press officer, so all offices speak with one voice.

The governor and his or her staff should remember, however, that every disaster and emergency situation is unique. Flexibility is an important concern, and the governor should determine what action to take on a case-by-case basis rather than strictly adhere to a prescribed response approach.

The homeland security advisor or state emergency management agency director should brief the governor continually on the status of state response and recovery efforts. Long after the emergency occurs, disaster assistance will be a key concern of press covering the affected area.

The governor will also be questioned about the status of federal recovery efforts. However, a governor should avoid answering questions about specific cases, such as why a particular business has not received a loan from the Small Business Administration or other federal assistance. Governors should reinforce the federal, state, and local response partnership when communicating with survivors.

A communications director should do several things before a disaster strikes or an emergency occurs:

- Set up models for the types of communication to be sent during a disaster or an emergency, identify who will serve as spokespeople for state government, and establish a process for clearing any communication with the media in a timely manner;
- Read the state emergency management plan;
- Sit down with homeland security and emergency management officials to learn their roles and establish a contact person in each organization;
- Meet with the state emergency management agency's and/or homeland security office's public information officer (PIO) and other key state personnel involved in communications to establish a relationship and information-release protocol;
- Access the joint information center to develop a system for disseminating information to agency PIOs and the press and clarify 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 public expectations are realistic when the governor asks the President to declare a disaster or an emergency;
- Ensure members of the governor's staff have pagers or other backup means of communicating to maintain critical communication links in the event telephone lines are down and cell phones become jammed;
- Understand the roles of the Red Cross, Salvation Army, and other volunteer emergency assistance groups and identify an appropriate governor's staff liaison to those organizations; and
- Create or update a website where the public can access the most up-to-date information on emergency preparedness and citizen capabilities.

Joint Information Center's Role in Effective Communications

After the President has declared a disaster or an emergency, a joint information center (JIC) should be established to coordinate the print and electronic dissemination of information about response and recovery programs and the state's long-term prevention and mitigation strategy. Public information officers representing federal, state, and local agencies providing response or recovery services should be part of the JIC to ensure messages are coordinated. The state homeland security's and/or emergency management office's PIO plays an integral role in the JIC and is an invaluable resource to the governor's communications director. Volunteer organizations should also be included in the JIC.

JIC objectives are to develop and implement public relations and media strategies to instill confidence within the affected community that the state is using all possible resources and is working in partnership with federal, state, and local organizations to restore essential services and help survivors recover. JIC also promotes a positive understanding of response, recovery, and mitigation programs; provides equal access to timely and accurate information about disaster response, recovery, and mitigation programs; and manages expectations so disaster victims have a clear understanding of the disaster response, recovery, and mitigation services available to them and the limitations of those services.

Use of Social Media Technologies in Effective Communications

The rapid development of communications and social networking technology has provided additional opportunities for governors and emergency officials to communicate with the public on a regular basis. Technologies such as microblogging (Twitter), social networking (Facebook, Myspace, etc.), and high-volume text messaging enable instantaneous communication with large audiences.

Although these technologies contain less information than a website, they can facilitate rapid response to an incident and provide information to large audiences when access to traditional media sources is limited. Communications offices should have a "Web 2.0" plan that addresses the strategic use of these additional communications tools in the event of a disaster or an emergency. Often, state and allied agencies already have robust social media networks they use on a daily basis. By identifying these resources ahead of time, they can become an immediate dissemination source for links, media advisories, and news releases already being distributed through traditional methods.


RECOVER

CHAPTER 14.

Federal Assistance Available to States, Individuals, and Businesses

Key Concepts

- Federal public assistance programs typically pay for 75 percent of approved project costs, including repair or restoration of facilities to their predisaster condition, in accordance with applicable codes, specifications, and standards.
- For small public assistance projects, payment of the federal share of the estimated total is made upon approval of the project, and no further accounting to the Federal Emergency Management Agency is required. For large public assistance projects, payment is made on the basis of actual costs of the project after completion, though interim payments may be made.
- Disaster assistance also is available to individuals, with major types including disaster unemployment assistance, disaster housing assistance, legal services assistance, and the National Flood Insurance Program. Businesses and farmers also qualify for some federal assistance programs.

State and local governments share responsibility for protecting their citizens from disasters and emergencies and for helping them recover when either strikes. In some cases, however, the scale of an incident exhausts the capabilities of state and local governments. In these situations, federal assistance often is available to states, individuals, and businesses in the forms of resources, personnel, and loans.

As soon as possible after the President declares a major disaster or an emergency, the state should submit for approval by the Federal Emergency Management Agency (FEMA) regional administrator a single assistance application for all incident-related projects. The state serves as the program grantee and has management and financial responsibilities. A team of federal, state, and local officials should inspect the damage area. Federal inspectors prepare project worksheets with recommended scopes of work and estimated project costs in accordance with FEMA eligibility criteria.

Federal regulations allow for repair or restoration of facilities to their predisaster/preemergency condition, in accordance with applicable codes, specifications, and standards. Following the applicant's briefing, and after identifying public or private nonprofit facility damages, state or local representatives attend an initial meeting with a FEMA representative—generally the public assistance coordinator (PAC). At this meeting, damages are discussed, needs are assessed, and a plan of action is put into place. The PAC reviews what is expected of the state and provides detailed instructions on how to apply for and receive federal assistance. This meeting also is the appropriate time and place for state officials to raise questions or voice concerns about how the public assistance process works.

Federal assistance is available to state and local governments and individuals. In addition, farmers, ranchers, and businesses qualify for targeted assistance. Finally, additional programs provide still other assistance (see Assistance Available from Other Federal Programs on page 68).

Assistance Available to State and Local Governments

Public assistance, oriented to public entities, can fund the repair, restoration, reconstruction, or replacement of a public facility or infrastructure that is damaged or destroyed. Eligible recipients include state governments, local governments, any other political subdivision of the state, Indian tribes or authorized tribal organizations, and Alaska Native villages. Private nonprofit organizations, such as education organizations; nonprofit utilities; emergency, medical, rehabilitation, and temporary or permanent custodial care facilities (including those for the elderly and those for people with disabilities); and other facilities that provide essential services of a governmental nature to the public may also be eligible for assistance.

State agency, local government, and nonprofit organization officials must submit requests for public assistance to the state public assistance officer—a state official situated in the emergency operations center—within 30 days of the date of a presidential declaration. Applicants may combine damaged sites into work projects. Projects are considered small if they fall below an inflation-adjusted threshold.

Applicants may complete their own small projects and document their damages on a project worksheet. If the applicant is unable to complete the worksheet, federal representatives are available to develop the worksheet for the applicant. For large projects, a federal representative will work with the applicant and the state to develop the worksheet. Large projects fall into the following categories: debris removal, emergency protective measures, road systems and bridges, water control facilities, public buildings and contents, public utilities, and parks, recreational, and other.

For insurable structures—primarily buildings—within special flood hazard areas (SFHAs), FEMA reduces its assistance by the amount of insurance settlement fees that could have been obtained under a standard National Flood Insurance Program policy. For structures located outside a SFHA, FEMA reduces the amount of assistance by any insurance proceeds.

FEMA reviews and approves project worksheets and obligates the federal share of the costs—which cannot be less than 75 percent of the total—to the state. The state then distributes funds to the local recipients. For small public assistance projects, payment of the federal share of the estimated total is made upon approval of the project, and no further accounting to FEMA is required. For large public assistance projects—currently defined as $63,200 or higher—payment is made on the basis of actual costs after the project is completed, though interim payments may be made. Once FEMA obligates funds to the state, further management of the assistance, including disbursement to local governments and nonprofit organizations, is the responsibility of the state. FEMA continues to monitor the recovery process to ensure the timely delivery of eligible assistance and compliance with applicable laws and regulations.

Following a major disaster declaration, state and local governments may obtain assistance to pay part of the costs of rebuilding a community's damaged infrastructure. Federal public assistance programs typically pay for 75 percent of the approved project costs.

Assistance Available to Individuals

After the President has declared a major disaster or emergency, FEMA, in coordination with the affected state, will tell citizens how to apply for various forms of federal assistance, such as crisis counseling, housing assistance, legal assistance, tax relief, unemployment assistance, and veterans' assistance.

In some cases, FEMA, in coordination with the state, will establish disaster recovery centers (DRCs) in heavily affected communities. DRCs provide a place where applicants can speak with FEMA representatives in person and obtain information about applying for assistance following a presidential declaration. States have the opportunity to staff DRCs with representatives of various state agencies that want to provide greater access to their programs and services. The state also has a major role in managing donated goods and services.

Crisis Counseling

The Crisis Counseling Assistance and Training Program, authorized by the Stafford Act, is designed to provide supplemental funding to states for short-term crisis counsel-

ing services to people affected by presidentially declared disasters or emergencies. Two separate parts of the CCP can be funded: immediate services programs and regular services programs. A state may request either or both parts.

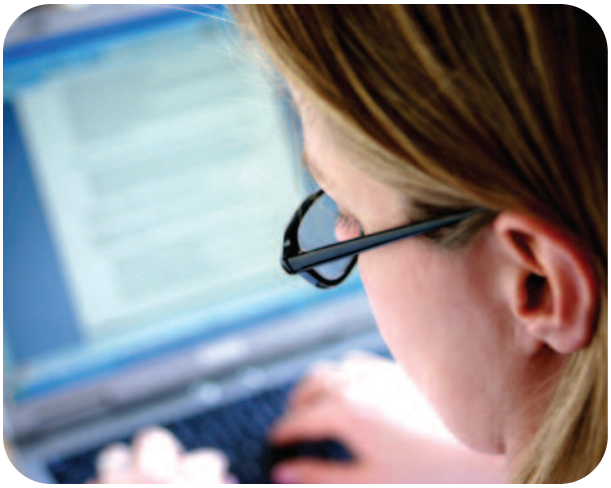
The immediate services program aims to enable the state or local agency to respond to the immediate mental health needs of victims. Immediate services include screening, diagnostic, and counseling techniques as well as outreach services such as public information and community networking. The regular services program provides up to nine months of crisis counseling, community outreach, consultation, and education services to people affected by disasters and emergencies. To be eligible for crisis counseling services funded by this program, applicants must be residents of the designated area or must have been located in the area when the incident occurred.

Housing Assistance

Housing assistance is available to individuals in the affected area whose primary residence has been damaged or destroyed and whose losses are not covered by insurance. This assistance provides for temporary housing, repair, placement, and permanent housing construction.

Legal Services

Through an agreement with FEMA, the Young Lawyers Division of the American Bar Association provides free legal advice to low-income individuals whose cases will not produce a fee. The American Bar Association turns over cases that may generate fees to the local lawyer referral service.



Tax Relief

The Internal Revenue Service (IRS) provides assistance to people claiming casualty losses as a result of the incident. The federal tax agency can also expedite refunds to eligible taxpayers located in a declared disaster or emergency area. Depending on the circumstances, the IRS may grant additional time to file returns and pay taxes.

Unemployment Assistance

Weekly benefit payments for up to 26 weeks are available to those out of work because of a disaster or an emergency. Recipients include the self-employed, farmworkers, farm and ranch owners, and others not covered by regular unemployment insurance programs. This assistance is available through state unemployment offices.

Veterans' Assistance

Veterans' assistance includes death benefits, pensions, insurance settlements, and adjustments to home mortgages held by the U.S. Department of Veterans' Affairs (DVA) if a DVA-insured home has been damaged.

Assistance Available to Farmers, Ranchers, and Businesses

The Small Business Administration and the U.S. Department of Agriculture's Farm Service Agency also provide assistance to aid individuals, farmers, ranchers, and businesses in repairing or replacing uninsured property that was damaged in a disaster or an emergency.

Small Business Administration

The Small Business Administration (SBA) offers two primary kinds of disaster loan programs to help business owners recover from a disaster or an emergency: business physical disaster loans and economic injury disaster loans.

Business physical disaster loans allow up to 100 percent of the uninsured, SBA-verified loss—not to exceed $1.5 million—to repair or replace damaged business property, including inventory and supplies. Within this limit, the loan may be increased by up to 20 percent for the purchase of mitigating devices for damaged real property.

Economic injury disaster loans (EIDLs) enable small businesses and small agricultural cooperatives to meet necessary financial obligations that could have been met had

Assistance Available from Other Federal Programs

Additional assistance is available from other federal programs, including fire management assistance, flood protection, health and human services assistance, repairs to roads and bridges, and search and rescue assistance.

Fire Management Assistance

The Stafford Act authorizes the President to provide assistance, including grants, equipment, supplies, and personnel, to a state for the suppression of a forest or grassland fire, on public or private lands, that threatens to become a major disaster. The governor or the governor's authorized representative must request this assistance through the FEMA regional administrator. The request must include detailed information on the nature of the threat and the federal assistance needed.

Flood Protection

The U.S. Army Corps of Engineers is authorized to assist in flood fighting and rescue operations and to protect, repair, and restore certain flood control works that are threatened, damaged, or destroyed by a flood. The corps may assist states for a 10-day period, subject to specific criteria. Homeowners can also purchase insurance for flood damage within any community participating in the National Flood Insurance Program. The insurance covers damage that is not covered under typical insurance policies for homeowners.

Health and Human Services Assistance

The U.S. Department of Health and Human Services may provide assistance to state and local human services agencies and state vocational rehabilitation agencies. The Food and Drug Administration may work with state and local governments to establish public health controls by decontaminating or condemning contaminated food and drugs.

Repairs to Roads and Bridges

The U.S. Department of Transportation's Federal Highway Administration can provide assistance to restore roads and bridges that are part of the federal aid system. The Federal Highway Administration provides tools, guidance, capacity building, and good practices that aid local and state transportation departments and their partners in their efforts to improve transportation network efficiency and public/responder safety when a nonrecurring event interrupts or overwhelms transportation operations. Events can range from traffic incidents to disaster or emergency transportation operations.

Search and Rescue Assistance

U.S. Coast Guard or armed forces units may assist in search-and-rescue operations, evacuate disaster victims, and transport supplies and equipment.

a disaster or an emergency not occurred. EIDLs are working capital loans and are made only to provide relief from economic injury caused directly by the disaster or emergency and to permit individuals to maintain a reasonable working-capital position during the period affected by the disaster or emergency.

EIDL assistance is provided only to businesses that cannot obtain credit elsewhere, and it is limited to a maximum of $1.5 million (together with any business physical disaster loan for damage from the same disaster). However, the actual amount of the loan will be based on the economic injury to the business and its financial needs. The interest rate on

EIDLs may not exceed 4 percent per year, and the term of these loans may not exceed 30 years. The actual term will be based on the ability of the business to repay the loan.

U.S. Department of Agriculture's Farm Service Agency

The Farm Service Agency, an agency of the U. S. Department of Agriculture (USDA), provides various loans to farming and ranching operations that have suffered loss due to a disaster. Farming and ranching operations may apply for loans in counties named as primary or secondary locations under one of these categories: presidential major disaster declaration, USDA secretarial disaster designation, Farm Service Agency administrator's physical loss notification, and quarantine designation.

The Emergency Conservation Program (ECP) helps agricultural producers rehabilitate eligible farmlands damaged by natural disaster. ECP cost-share assistance may be available to agricultural producers for all designated natural disasters. To be eligible, an applicant must have suffered a natural disaster that created new conservation problems that, untreated, would impair or endanger the land; materially affect the land's productive capacity; represent unusual damage that, except for wind erosion, is not of a type likely to recur frequently in the same area; or are so costly to repair that federal assistance is or will be required to return the land to productive agricultural use. Conservation problems that existed before the natural disaster are not eligible for cost-sharing assistance. ECP funds may be used for debris removal, fence restoration, restoration of conservation structures, or water conservation measures, including providing water to livestock in periods of severe drought.

The **Farm Service Agency** also provides low-interest emergency loan assistance to eligible farmers and ranchers to help cover production and physical losses in locations that fall under one of the four declaration categories. Administrators may also authorize loan assistance to cover only physical losses. Emergency loans are available to qualifying ranchers and farmers who are established operators of family farms; are citizens or permanent residents of the United States; have adequate training or experience in managing and operating a farm or ranch; have suffered a qualifying physical loss or a production loss of at least 30 percent in any essential farm or ranch enterprise; cannot obtain commercial credit; can provide collateral to secure the loan; and can demonstrate repayment ability.

Emergency loan funds may be used to restore or replace essential physical property; pay all or part of production costs associated with the disaster year; pay essential family living expenses; reorganize the farming operation; and refinance debts. The loan limit is 100 percent of the actual physical loss, with a maximum indebtedness under this program of $500,000.

The **Crop Disaster Program** (CDP) covers crops for which crop insurance is not available and crops insured by catastrophic or "buy-in" insurance. It provides assistance for farmers who grow such crops, limiting their losses from natural disaster and helping to manage their business risk. CDP payments are limited to $80,000 per person. Producers with incomes of greater than $2.5 million, as defined by the Food Security Act of 1985, are not eligible.

CHAPTER 15.

Long-Term Recovery Strategies

Key Concepts

- Governors can strengthen and rebuild disaster- or emergency-affected communities in their state by providing leadership, resources, and a plan for the long term.
- Long-term recovery is an expansive process that begins immediately with response to an incident and continues with proactive, forward-looking preparation and mitigation strategies aimed at the inevitable next disaster or emergency.
- The governor's office can be a central point of coordination for localities to access state resources and assistance. It can also manage the local recovery effort and act as a liaison to request and manage federal assistance funding.
- A federal long-term community recovery team, which can support local strategic planning and goals for states, can be activated through a gubernatorial request to the Federal Emergency Management Agency (FEMA) federal coordinating officer.

Once the response to a disaster or an emergency begins to wane, communities begin the long-term recovery process. The main responsibility for long-term recovery ultimately lies with the local government and community, with support from the state government. The challenge is keeping state, federal, and local governments and the private sector focused and energized to see through a recovery period that may take many years. The long-term recovery of a community will likely occur well past a governor's term in office. Smart planning, leadership, and coordination of state resources at the beginning of the recovery phase will greatly improve the chances of the community making a recovery from the disaster or emergency and being more resilient to future incidents.

Governors appreciate the importance of healthy communities and can take proactive steps to ensure the long-term recovery of their state. Specifically, they can:

- Create a plan for long-term recovery;
- Coordinate state support to assist local recovery efforts;
- Recognize the federal government's role in long-term recovery; and
- Understand the prospects for long-term recovery.

Create a Plan for Long-Term Recovery

Recovery from a disaster or an emergency comes in phases. The immediate recovery phase will meet basic human needs for food, water, and shelter. As the critical period of response and short-term recovery passes and basic needs are met, citizens will try to reestablish routines, reopen workplaces, clean up their own properties, and rebuild their community. The chronic physical, economic, and social costs of disaster to an affected area may be significant. Businesses will assess damages, either rebuilding or closing indefinitely. Volunteer organizations and spontaneous volunteers will engage in support and assistance. Government agencies will begin to plan for long-term recovery.[72]

A strategic plan and vision are essential to come to terms with the numerous and varied technical challenges facing an affected community. Individuals, families, and communities may require more specialized assistance to recover than is available through uncoordinated volunteer efforts, such as care for citizens with special needs or chronic medical conditions and efforts to address homelessness caused by the disaster or emergency. The restoration of infrastructure, historic landmarks, and community services will also require specialized assistance. To address these long-term challenges, a community will require assistance from the state, local, and federal governments, nonprofit organizations, the private sector, and individuals. Strong leadership during the early phase of response and recovery will help communities rebound.

Currently, no enabling legislation exists to provide federal grants to states for long-term recovery efforts.[73] In 2009, the U.S. Department of Homeland Security and the U.S. Department of Housing and Urban Development co-chaired a long-term recovery working group and released a draft National Disaster Recovery Framework (NDRF).[74] NDRF will serve as a companion guide to the National Response Framework and will provide federal guidance for long-term disaster recovery.

Coordinate State Support to Assist Local Recovery Efforts

Just as disaster preparation, protection, and response are primarily local functions, so, too, will the long-term recovery of a community be led by local government. At the local level, governors can expect communities to make investments in permanent disaster-resistant housing units, downtown revitalization programs, buy-outs of flood-prone properties for public open space, and improvements to infrastructure. Affected communities will lean on state government for state assistance in recovery. A broad range of state government agencies besides the state administrative agency may be involved in assisting local communities recover, including:[75]

- Economic development;
- Natural resources;
- Emergency management;
- Homeland security;
- Governor's office;
- Transportation;
- Housing;
- Health;
- Community development;
- Historic preservation; and
- Agriculture.

Governors can provide a central point of coordination for localities to access state resources and assistance. **Iowa** Governor Chet Culver established the Rebuild Iowa Office and the Rebuild Iowa Advisory Commission after severe flooding in 2008. The office was tasked with coordinating all state recovery activities; developing short-term priorities and long-term plans for redevelopment; identifying funding and innovating financing opportunities; establishing priorities and guidelines for those funds; setting timelines and benchmarks; providing a means for public and stakeholder input; and providing guidance for the entire long-term recovery process.

After hurricanes destroyed much of Louisiana in 2005, former Governor Kathleen Blanco issued an executive order establishing the **Louisiana** Recovery Authority to guide the state's long-term recovery efforts. The authority had five main focus areas:

- Securing funding and other resources needed for the recovery;
- Establishing principles and policies for redevelopment;
- Leading long-term community and regional planning efforts;
- Ensuring transparency and accountability in the investment of recovery funds; and
- Communicating progress, status, and needs of the recovery to officials, community advocates, and the public.

Recognize the Federal Government's Role in Long-Term Recovery

In 2009, the Department of Homeland Security identified response and recovery as one of its five priority missions.[76] Under the National Response Framework, federal activity for long-term recovery is housed in the FEMA Emergency Support Function 14 (ESF 14). The federal Long-Term Community Recovery (LTCR) team collaborates with states to promote the successful recovery of communities by facilitating local strategic planning and goals, coordinating federal agencies with state efforts, identifying past practices in long-term recovery, and fostering optimal recovery.[77]

To activate the federal ESF 14 LTCR team, the governor files a request with the FEMA federal coordinating officer. Ideally, the state will organize itself to support community recovery, with technical assistance from the LTCR team. For example, governors in Indiana, Iowa, Texas, and Wisconsin created state recovery task forces or governor's commissions to help manage resources for recovery.[78]

After the 2008 floods, **Iowa's** LTCR team coordinated with the Rebuild Iowa Office to create a state interagency coordination team. The team brought state and federal agencies together to meet with local community leadership to develop a community-driven long-term recovery plan. The team also worked with the U.S. Environmental Protection Agency to use available Green Communities and Smart Growth grants to rebuild local communities through interagency agreements.[79]

Understand the Prospects for Long-Term Recovery

No definitive finish line exists for when a community is fully "recovered" from an incident. Social, economic, and cultural damage may linger long after the return of the local economy and infrastructure. However, empowering communities early in the recovery phase, with clear goals and objectives and a good understanding of the kinds of support on which they can rely will put them on a stronger path of rebuilding. Many elements of the long-term recovery process will lead to community discussions and planning on how to prepare for future events, bringing full circle the emergency management rubric—prepare, prevent, respond, and recover.

Notes

[1] Alaska Division of Homeland Security and Emergency Management website. http://www.ak-prepared.com/homelandsecurity/ (accessed September 30, 2010).

[2] Indiana Department of Homeland Security Mission website: http://www.in.gov/dhs/2358.htm (accessed September 30, 2010).

[3] State of Minnesota, Division of Homeland Security & Emergency Management, All Hazard Mitigation Plan April 21, 2008, page 14

[4] State of Virginia, Office of Commonwealth Preparedness, Office of Governor Robert McDonnell website: http://www.commonwealthpreparedness.virginia.gov/index.cfm (accessed September 30, 2010)

[5] DHS, "National Homeland Security Strategy" page 3. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed September 19, 2010)

[6] U.S. Department of Homeland Security; National Strategy for Homeland Security, 2007. Page 1. See http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed September 30, 2010)

[7] U.S. Department of Defense, DoD 101: "An Introductory Overview of the Department of Defense," http://www.defense.gov/pubs/dod101/dod101.html (accessed September 19, 2010).

[8] US Department of Homeland Security, National Response Framework, Glossary, (http://www.fema.gov/emergency/nrf/index.htm, accessed September 30, 2010).

[9] U.S. Department of Homeland Security (DHS), "DHS Announces Nearly $1.8 Billion in Fiscal Year 2009 Preparedness Grants," Press Release, June 16, 2009, http://www.dhs.gov/ynews/releases/pr_1245074657821.shtm (accessed September 19, 2010).

[10] U.S. Department of Justice, Office of Justice Programs, "Fiscal Year 2010 OJP Program Plan" http://www.ojp.usdoj.gov/ProgramPlan/introduction.htm (accessed September 19, 2010).

[11] Federal Emergency Management Agency (FEMA), "National Incident Management System," December 2008, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf. (accessed September 3, 2010)

[12] FEMA's Homeland Security Exercise and Evaluation Program, "About HSEEP," https://hseep.dhs.gov/pages/1001_About.aspx (accessed September 3, 2010).

[13] California Emergency Management Agency, "Golden Guardian Exercise Program," http://www.calema.ca.gov/WebPage/oesWebsite.nsf/content/AEC4591D507E40F388257648006488 2D?OpenDocument (accessed September 3, 2010).

[14] Office of the Alabama Emergency Management Agency, "Alabama Mutual Aid Teams to Participate in Full Scale Exercise," Press Release, May 26, 2009, http://ema.alabama.gov/filelibrary/PressRelease/NR%20AMAS%20Exercise_Tusc%20052709.pdf (accessed September 3, 2010).

[15] Jonathan B. Tucker, *Scourge: The Once and Future Threat of Smallpox* (New York: Grove Press, 2001).

[16] Telephone Interview with Robert Mauskopf, Virginia Department of Health, and Rue White, Virginia Department of Human Resources. July 28th, 2008.

[17] Governor's Food Safety Council, Pennsylvania Executive Order 2008-09, Doc. No. 10-3, August 26, 2009, http://www.pabulletin.com/secure/data/vol40/40-1/3.html (accessed September 3, 2010).

[18] Alabama Department of Homeland Security, "Virtual Alabama Program Fact Sheet," http://www.dhs.alabama.gov/virtual_alabama/pdf_files/VirAL_Fact_Sheet.pdf (accessed September 3, 2010).

[19] Esri, "Virtual USA Emergency Initiative," ArcNews (spring 2010), http://www.esri.com/news/arcnews/spring10articles/virtual-usa.html (accessed September 3, 2010).

[20] U.S. Department of Homeland Security, "Daily Open Source Infrastructure Report," March 31, 2009, http://www.globalsecurity.org/security/library/news/2009/03/dhs_daily_report_2009-03-31.pdf (accessed September 3, 2010).

[21] Louisiana's Get a Game Plan, "Louisiana Governor's Office of Homeland Security and Emergency Preparedness," http://www.getagameplan.org/ (accessed on September 21, 2010).

[22] North Carolina Citizen Corps, "Shelter in Place: Family Preparedness Tips for Staying at Home," http://readync.org/index.cfm?espanol=0&topic=35&on=Shelter-in-Place (accessed September 3, 2010).

[23] State of Oklahoma, Oklahoma Department of Emergency Management: "McReady Program" http://www.ok.gov/mcready/ (accessed September 3, 2010).

[24] Louisiana Homeland Security and Emergency Preparedness, "2009 Louisiana Hurricane Preparedness Sales Tax Holiday," Press Release, May 26, 2009, http://gohsep.la.gov/newsrelated/eptaxfree052609.htm (accessed September 3, 2010).

[25] Virginia Department of Taxation, "May Sales Tax Holiday: Hurricane and Emergency Preparedness Equipment," http://www.tax.virginia.gov/site.cfm?alias=HurricanePreparednessEquipmentHoliday (accessed September 3, 2010).

[26] U.S. Department of Homeland Security, "State and Local Fusion Centers," (September 2009) http://www.dhs.gov/files/programs/gc_1156877184684.shtm (accessed September 22, 2010).

[27] U.S. Department of Justice, Office of Justice Programs, "Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines" (September 2008)

www.it.ojp.gov/documents/baselinecapabilitiesa.pdf (accessed September 3, 2010).

[28] Paul Wormeli and Andrea Walter, "Disaster Preparedness & Recovery: The Evolution of the National Information Exchange Model," *Emergency Management Magazine*, August 2009.

[29] "Further Strengthening the Sharing of Terrorism Information to Protect Americans," Executive Order 13388, Federal Register (October 2005), http://edocket.access.gpo.gov/2005/pdf/05-21571.pdf (accessed September 3, 2010).

[30] US Department of Homeland Security, "National Response Framework," (January 2008), page 19. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed September 19, 2010).

[31] Ibid.

[32] The White House Presidential Decision Directive, National Security Council, "Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed September 3, 2010).

[33] John Moteff, *Critical Infrastructure: The National Asset Database*, (Washington, DC Congressional Research Service, 2007, page 1.

[34] State of New Jersey, "ADMINISTRATIVE ORDER NO. 2005-05" (2005) www.njwec.org/PDF/TCPA%20AO%20Final%20Signed.pdf (accessed September 3, 2010).

[35] The Infrastructure Security Partnership, "About Us" http://www.tisp.org/index.cfm?pid=10213 (accessed September 19, 2010).

[36] U.S. Department of Homeland Security, *Critical Infrastructure Identification, Prioritization, and Protection, Homeland Security Presidential Directive* 7, The White House (December 17, 2003).

[37] The Homeland Security Act of 2002. Public Law 107–296, (2002).

[38] State of Maryland, Office of Governor Martin O'Malley, "Governor Martin O'Malley Releases Plan to Make Maryland Nation's Epicenter for Cyber Security," Press Release January 11, 2010. http://www.governor.maryland.gov/pressreleases/100111.asp (accessed October 18, 2010).

[39] State of Wisconsin, Homeland Security Council: "2010 Report on Homeland Security," September 2010, page 20, http://emergencymanagement.wi.gov/news/publications/2010_Annual_Report.pdf (accessed October 18, 2010).

[40] The White House, National Security Council: *Comprehensive National Cyber Security Initiative* (2009) http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed (September 19, 2010).

[41] State of Oregon. "Constitution of Oregon - 2009 Edition," (2009): Section 9, http://www.leg.state.or.us/orcons/orcons.html (accessed September 3, 2010).

[42] State of Alabama. "Constitution of the State of Alabama," (1901): Section 131, http://alisondb.legislature.state.al.us/acas/ACASLogin.asp (accessed September 3, 2010).

[43] Maintenance and operation of equipment, 10 USC § 374, Office of the Law Revision Counsel, U.S. House of Representatives.

[44] Prohibited transactions involving nuclear materials, 18 USC § 831, Office of the Law Revision Counsel, U.S. House of Representatives.

[45] Emergency situations involving chemical or biological weapons of mass destruction, 10 USC § 382, Office of the Law Revision Counsel, U.S. House of Representatives.

[46] Support and services for eligible organizations and activities outside Department of Defense, 10 USC § 2012, Office of the Law Revision Counsel, U.S. House of Representatives.

[47] Powers, authorities, and duties of United States Secret Service, 18 USC § 3056, Office of the Law Revision Counsel, U.S. House of Representatives.

[48] Congressional, Cabinet, and Supreme Court assassination, kidnapping, and assault, 18 USC § 351, Office of the Law Revision Counsel, U.S. House of Representatives.

[49] Federal aid for state governments, 10 U.S.C. §§ 331-335, Office of the Law Revision Counsel, U.S. House of Representatives.

[50] John Warner National Defense Authorization Act for Fiscal Year 2007, 109th Cong., 2d sess., 2006, http://www.rules.house.gov/109_2nd/text/hr5122cr/1092nd5122cr_1.pdf (accessed September 3, 2010).

[51] U.S. Department of Defense, DoD 101: "An Introductory Overview of the Department of Defense," http://www.defense.gov/pubs/dod101/dod101.html (accessed September 19, 2010).

[52] DHS, "National Homeland Security Strategy" page 3. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed September 19, 2010)

[53] U.S. Department of Homeland Security; National Strategy for Homeland Security, 2007. Page 1. See http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed September 30, 2010)

[54] Idaho Bureau of Homeland Security, "About Us," http://www.bhs.idaho.gov/pages/AboutUs.aspx (accessed September 3, 2010).

[55] National Emergency Management Association, Emergency Management Assistance Compact, "Model Mutual Aid Legislation" http://www.emacweb.org/?150 (accessed September 19, 2010).

[56] National Emergency Management Association, "Article V-Licenses and Permits," Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (accessed September 3, 2010).

[57] National Emergency Management Association, "Article IX-Reimbursement," Emergency Management Assistance

Compact, http://www.emacweb.org/?1838 (accessed September 3, 2010).

[58] National Emergency Management Association, "Article VI-Liability," Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (accessed September 3, 2010).

[59] National Emergency Management Association, "Article VIII-Compensation," Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (accessed September 3, 2010).

[60] National Emergency Management Association, "Article I-Purpose and Authorities," Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (accessed September 3, 2010).

[61] Federal Emergency Management Agency, "Emergency Management Assistance Compact: Overview for National Response Framework," http://www.fema.gov/pdf/emergency/nrf/EMACoverviewForNRF.pdf (accessed September 3, 2010).

[62] National Emergency Management Association, "EMAC Overview," June 14, 2007, 38, http://www.emacweb.org/?323#search=%22EMAC%20Katrina%20response%22 (accessed September 3, 2010).

[63] Pacific Coast Collaborative, Regional Best Practices: http://www.pacificcoastcollaborative.org/priorities/emergency/Pages/emergency.aspx (accessed September 22, 2010)

[64] Mid America Alliance, Mission Statement: http://www.unmc.edu/apps/midamerica/index.cfm?L1_ID=1&CONREF=1 (accessed September 19, 2010).

[65] State of Maine, Maine Emergency Management Agency, http://www.maine.gov/MEMA/response/mema_response_iemac.shtml (accessed September 19, 2010).

[66] Northern New England Metropolitan Medical Response System, http://www.nnemmrs.org/ (accessed September 19, 2010).

[67] U.S. Department of Homeland Security, "Interoperability," SAFECOM, http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm (accessed September 3, 2010).

[68] Arkansas Department of Information, "Arkansas Wireless Information Network," http://www.awin.arkansas.gov/index.htm (accessed September 3, 2010).

[69] State of Minnesota, "Final Report to the NGA Center on the Interoperable Communications Policy Academy," presented January 28, 2008.

[70] Federal Emergency Management Agency, "Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288) as amended," http://www.fema.gov/about/stafact.shtm (accessed September 3, 2010).

[71] Federal Emergency Management Agency, "Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288) as amended," http://www.fema.gov/about/stafact.shtm (accessed September 3, 2010).

[72] Federal Emergency Management Agency, "Long Term Community Recovery Planning Process: A Self-Help Guide," 2005, http://www.fema.gov/txt/rebuild/ltrc/selfhelp.txt (accessed September 3, 2010).

[73] Claire B. Rubin, "Long Term Recovery from Disasters—The Neglected Component of Emergency Management," *Journal of Homeland Security and Emergency Management,* vol. 6, no. 1 (2009).

[74] Federal Emergency Management Agency, "National Disaster Recovery Framework," http://www.fema.gov/pdf/recoveryframework/omb_ndrf.pdf (accessed September 3, 2010).

[75] Ibid.

[76] U.S. Department of Homeland Security, "Secretary Napolitano Announces Fiscal Year 2010 Budget Request," Press Release, May 7, 2009, http://www.dhs.gov/ynews/releases/pr_1241715252729.shtm (accessed September 3, 2010).

[77] Ibid.

[78] Federal Emergency Management Agency, "Long Term Community Recovery Planning Process: A Self-Help Guide.

[79] U.S. Department of Homeland Security, "The Road to Recovery 2008: Emergency Support Function 14 Long-Term Community Recovery," August 2009, http://www.fema.gov/pdf/rebuild/ltrc/2008_report.pdf (accessed September 3, 2010).

NGA CENTER DIVISIONS

The NGA Center is organized into five divisions with some collaborative projects across all divisions.

- **Economic, Human Services & Workforce** focuses on best practices, policy options, and service delivery improvements across a range of current and emerging issues, including economic development and innovation, workforce development, employment services, research and development policies, and human services for children, youth, low-income families, and people with disabilities.

- **Education** provides information on best practices in early childhood, elementary, secondary, and postsecondary education. Specific issues include common core state standards and assessments; teacher effectiveness; high school redesign; science, technology, engineering and math (STEM) education; postsecondary education attainment, productivity, and accountability; extra learning opportunities; and school readiness.

- **Environment, Energy & Transportation** identifies best practices and provides technical assistance on issues including clean energy for the electricity and transportation sectors, energy and infrastructure financing, green economic development, transportation and land use planning, and clean up and stewardship of nuclear weapons sites.

- **Health** covers a broad range of health financing, service delivery, and coverage issues, including state options under federal health reform, quality initiatives, cost-containment policies, health information technology, state public health initiatives, and Medicaid.

- **Homeland Security & Public Safety** supports governors' homeland security and criminal justice policy advisors. This work includes supporting the Governors Homeland Security Advisors Council (GHSAC) and providing technical assistance to a network of governors' criminal justice policy advisors. Issues include emergency preparedness, interoperability, cyber-crime and cyber-security, intelligence coordination, emergency management, sentencing and corrections, forensics, and justice information technology.

John Thomasian, Director
NGA Center for Best Practices
444 N. Capitol Street, Suite 267
Washington, DC 20001
202.624.5300
www.nga.org/center