A GOVERNOR'S GUIDE TO HOMELAND SECURITY

NGA
NATIONAL GOVERNORS ASSOCIATION

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

NGA Center for Best Practices
Homeland Security & Public Safety Division

FEBRUARY 2019

NGA
NATIONAL GOVERNORS ASSOCIATION

Acknowledgements

A Governor's Guide to Homeland Security was produced by the Homeland Security & Public Safety Division of the National Governors Association Center for Best Practices (NGA Center) including Maggie Brunner, Reza Zomorrodian, David Forscey, Michael Garcia, Mary Catherine Ott, and Jeff McLeod. Former NGA staff who also contributed include Alisha Powell, Allison Cullin, Carmen Ferro, David Henry, Thomas MacLellan, Heather Hogsett, Christopher Logan, Will Ware, Taryn Hunter, and John Thomasian.

The authors appreciate the valuable insights from: Trina Sheets, National Emergency Management Association; Major General Timothy Lowenberg, former Adjutant General, State of Washington; William Pelgrin, former director, Multi-State Information Sharing & Analysis Center, Alberto Martinez, National Fusion Center Association; Nikki Cassingham, Statewide Interoperability Coordinator, State of Oklahoma; Arthur House, Chief Cybersecurity Risk Officer, State of Connecticut; Joe Galvin, Statewide Interoperability Coordinator, State of Illinois; Karen Jackson, President, Apogee Strategic Partners and former Secretary of Technology, State of Virginia; and Michael Sprayberry, North Carolina Emergency Management.

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 and Church Street Editorial for editing support, and Middour & Nolan Design for designing the report.

NGA would like to dedicate this publication to Major General Timothy Lowenberg, former Adjutant General, State of Washington. MG Lowenberg was a founding member of the Governors Homeland Security Advisors Council. NGA Honored MG Lowenberg with the passage of a resolution at the 2018 Winter Meeting as a "model of service over self throughout his long service to the nation."

Contents

PART I: PREPARE

PART II: PREVENT

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 well as catastrophes on the scale of Hurricane Maria 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 2010 guide provides recent state examples and the latest information on evidence-based practices and the changing landscape of homeland security and emergency management.

The suggestions for gubernatorial and state actions draw heavily from the experiences of governors, homeland security advisors, and other state officials nationwide. The goal of this guide is to help governors and other state executives effectively manage homeland security incidents of all types and sizes to ensure the safety and security of citizens and their communities.

FIRE
FIRE
FIRE
FI

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 Las Vegas Shooting of October 1, 2017; western state wildfires that have raged through California, Oregon, and Washington; and Hurricanes Irma and Maria demonstrate the diverse events for 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 (HSA) is one of the most important gubernatorial decisions.** After the governor, the 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. There are many different ways to organize a state's homeland security functions, 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 are the state fusion centers. 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 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 HSA, have proper security clearances and adequately coordinate with and utilize the capabilities of the fusion center. 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 the vast majority 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, such as 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, important principals include the governor's chief of staff and communications director, the HSA, 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 noted[*],"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, Governor Greg Abbott created the Governor's Commission to Rebuild Texas in response to the devastation of Hurricane Harvey in 2017. New Jersey Governor Phil Murphy also established a Commission on Puerto Rico Relief via executive order to work with state and federal agencies to ensure expedited benefits to displaced Puerto Ricans and identify other ways to help with the island's recovery.

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 authorities, 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 (HSA);
- 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 coordinating the various aspects of a state's homeland security enterprise. 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 tenure.

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

Louisiana: The Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) is responsible for coordinating the state's efforts throughout the emergency management cycle to prepare for, prevent, respond to, recover from and mitigate to lessen the effects of man-made or natural disasters.[1]

Indiana: The Indiana Department of Homeland Security works 24/7 to protect the people, property and prosperity of Indiana.[2]

Minnesota: The Minnesota Homeland Security and Emergency Management (HSEM) Division is a component of the state's Department of Public Safety, and it's mission is to help Minnesota prevent, prepare for, and recover from natural and human-caused disasters. The HSEM team develops and maintains partnerships; collects and shares information; plans, trains and educates; coordinates response resources; and provides technical and financial assistance.[3]

West Virginia: The mission of the West Virginia Division of Homeland Security and Emergency Management (DHSEM) is to ensure the protection of life and property by providing coordination, guidance, support and assistance to local emergency managers and first responders.[4]

As these examples show, governors must support an all-hazards approach (see definitions of homeland security, homeland defense, and emergency management on the next 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 an HSA 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 the state's main point of contact in the event of a disaster. 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 HSA is a member of the NGA Governors Homeland Security Advisors Council (GHSAC). The GHSAC, founded in 2006, provides an organizational structure through which the HSA from each state, territory, and the District of Columbia can discuss homeland security issues, share information and expertise, build connections with their peers in other states, and keep governors informed of the federal, state, and local issues that affect homeland security policy and practice.

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 U.S. Department of Homeland Security (DHS), 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] DHS 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 HSA, who should have the authority to make critical decisions regarding policies, procedures, and communications. Governors need to appoint a strategic and collaborative HSA 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 HSA. 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 entity, 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 HSA. 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?
- Do they have a background in cybersecurity, and/or are they proficient in their understanding of cyber risk and how best to manage it?

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 2018 survey of state HSAs conducted by the NGA Center, 55 percent serve in a cabinet-level role reporting directly to the governor. Additionally, 86 percent serve in multiple capacities, including HSA 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 non-cabinet-level agency but reports directly to the governor.

The state HSA 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 HSAs from the states, territories, and commonwealths. The council provides a unified voice for states on national homeland security policy, keeps governors abreast of the current threat environment, and informs the work of the NGA Center for Best Practices by sharing ideas and best practices, identifying emerging issues, and analyzing federal impacts on state interests.

Council members maintain frequent communication via conference calls and biannual meetings where they receive briefings from federal executives, discuss common challenges and emerging threats, learn about model state initiatives and best practices, and identify collective priorities. GHSAC leadership comprise four committees: Special & Emerging Issues, Catastrophic Planning & Emergency Communications, Information Sharing & Analysis, and Cybersecurity & Critical Infrastructure Protection. These committees identify issue-specific priorities for the larger body and carry out activities in support of those priorities.

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 can 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 HSA.

Types of State Homeland Security Organizations

State homeland security organizations have evolved since the early 2000s. In most states, the 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 thirteen 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 thirty-three 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 ten 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 priorities, 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 HSA 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 2014 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 2014, 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 2016 **Cyber Storm V Final Report**[9] 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.

Last updated in June 2016, the **National Response Framework** (NRF)[10] establishes a comprehensive, all-hazards approach to domestic incident response. The 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 (NIMS), which provides a consistent template for managing incidents.

The **National Infrastructure Protection Plan,** released in 2008 and most recently updated in 2013, 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 2014 **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 (NIMS)**[11], last updated in 2017, 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**[12] 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, 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 U.S. Department of Homeland Security (DHS), through the Federal Emergency Management Agency (FEMA), oversees the Homeland Security Grant Program (HSGP). HSGP provides state, local, tribe, and territorial governments with funds to support activities designed to improve preparedness against the threats and hazards posing the greatest risk to the nation. The National Preparedness Goal (NPG) defines what preparedness means for the nation when responding to threats and hazards. Additionally, the NPG identifies 32 core capabilities that are necessary to address those risks, and HSPG funding helps to build and sustain them. Activities grant applicants must conduct to develop and maintain those capabilities must fall into one of the following categories: planning, organization, equipment, training and/or exercises.

HSGP is a grant made up of three components:

- State Homeland Security Program (SHSP)
- Urban Area Security Initiative (UASI)
- Operation Stonegarden (OPSG)

There are several additional standing requirements that states and territories must meet to receive FEMA grants.

Grant	Purpose	Eligibility	Allocation	Requirements
SHSP	Build capabilities to improve preparedness at the state and local levels	All fifty-six states, territories, and the District of Columbia	Based on minimum amounts as legislatively mandated and DHS risk methodology	Twenty-five percent of the grant must go to law enforcement for terrorism prevention activities Eighty percent must go to local governments
UASI	Enhances regional preparedness for high-risk, major metropolitan and urban areas from acts of terrorism	Only the 100 most populous areas are eligible to apply. (However, the number of urban areas funded changes every year.)	Based on a risk of terrorism to the most populous areas	Twenty-five percent of the grant must go to law enforcement for terrorism prevention activities Eighty percent must go to local governments
OPSG	Supports coordination	States and territories with international water borders; local and tribal government entities bordering Canada or Mexico	Based on the security risk to the border; determination made by U.S. Customs and Border Protection	100 percent must go to local jurisdictions

First, each state must adopt and implement the National Incident Management System (NIMS), which governs the management of incident response. States also must participate in the Emergency Management Assistance Compact (EMAC). EMAC is the interstate compact that governs state-to-state assistance in the event of a gubernatorially declared emergency. (Chapter 9 on mutual aid will discuss EMAC in more detail.) Additionally, each state must complete the Threat Hazard Identification Risk Assessment (THIRA) and Stakeholder Preparedness Report (SPR) to receive their grants. The THIRA is a risk assessment process that jurisdictions complete every three years to determine the threats and hazards they face, the associated impact, and the capabilities needed to address identified risks. The SPR is a self-assessment completed annually to assess a jurisdiction's capabilities to address gaps identified in the THIRA.

States also must develop an investment justification (IJ) that identifies the capability areas in which they want to invest. The IJ also describes the specific projects that support that investment. Grant applicants must describe in the IJ how those projects will support terrorism preparedness, closing capability gaps, and how they will engage the whole community in those efforts. Additionally, applicants must explain how the investments will prevent terrorism; prepare jurisdictions for all threats and hazards while connecting it to terrorism; protect individuals and infrastructure; and develop rapid response in the aftermath of a terrorist attack or other catastrophic event.

State Management of Grants

Each governor must designate an entity to serve as the state administrative agent/agency (SAA). Only the SAA can apply for federal grants, including those intended for local government agencies. The SAA is responsible for carrying out the administrative requirements of federal grants, including submission of the grant application and progress reports, allocating funding to sub-applicants appropriately, and ensuring the completion of deliverables.

The SAA also is responsible for ensuring that all relevant stakeholders are included in the homeland security grant process. FEMA requires that all states receiving funds through the HSGP have a Senior Advisory Committee (SAC). The SAC is an advisory body made up of stakeholders from across government and disciplines to help integrate preparedness efforts across the whole community. The SAC provides recommendations to the SAA about the type of activities that the FEMA grants should support. Additionally, the HSAC helps ensure all activities reflect the state's unique risks, hazards and identified capability gaps.

In many states, the SAA and the homeland security agency are the same. In others, another state entity provides oversight of federal grants. Regardless of grant organizational structure, the HSA must have a significant input into how federal homeland security grant funds are allocated.

Related Federal Grants

FEMA also provides several other grants that assist with preparedness. Although many of these grant programs do not directly fund state, local, tribal or territorial activities, they have an impact on state preparedness. Therefore, governors and HSAs should have an awareness of them and how they can help enhance preparedness.

- **The Emergency Management Performance Grant Program (EMPG)** provides states, locals, territories and tribal nations with funds to develop a system of emergency preparedness that can respond to all hazards. Eligible applicants include all states, territories and the District of Columbia. EMPG requires a 50 percent match—either cash or in-kind—by grant recipients to the federal contribution.

- The **Port Security Grant Program** supports maritime transportation infrastructure security activities.[13] Eligible applicants are port authorities, facility operators, and state and local government agencies.

- The **Transit Security Grant Program** aims to protect public transportation systems from terrorism and enhance mass transit's overall resilience. Eligible applicants are publicly-owned operators of public transit, including bus, ferries, and passenger rail.

- The **Intercity Bus Security Grant Program** provides funding for infrastructure hardening and security enhancements to bus transit operators in the highest-risk metropolitan areas. Eligible applicants are operators of fixed-route intercity and charter buses.

- The **Intercity Passenger Rail Security Grant Program** supports security activities for the Amtrak rail system against acts of terrorism and is designed to enhance its overall resilience. Amtrak is the only eligible applicant for this grant program.

- The **Nonprofit Security Grant Program** provides target hardening and other physical security enhancements to nonprofit organizations that are at high risk of a terrorist attack.[14] Although nonprofits are the intended recipient of the grant, the SAA must apply on their behalf.

- The **Tribal Homeland Security Grant Program** supports the building and sustainment of core capabilities for tribal governments. Eligible applicants are federally-recognized tribal nations.

In addition to FEMA, the U.S. Departments of Justice, Health and Human Services, and Centers for Disease Control and Prevention provide grant funds that could support preparedness activities. These additional funding sources are maintained by non-homeland security agencies.

- The **Edward Byrne Memorial Justice Assistance Grant** provides criminal justice funding to states and locals for multiple activities including programs for law enforcement; prevention and education; and planning, evaluation and technology.[15]

- The **Public Health Emergency Preparedness** cooperative agreement funds health departments to enhance their capabilities to respond to a myriad of public health threats, including infectious diseases, natural disasters, and biological, chemical, nuclear, and radiological events.[16]

- The **Hospital Preparedness Program** aims to enhance the health care system's ability to plan for and respond to medical surge needs.[17]

State Investments in Homeland Security

State and local governments also invest their own funds to support and complement federal investments. A recent study conducted by the National Emergency Management Association and the National Homeland Security Consortium determined that states and local government see a return on investment of $1.70 for every dollar in federal grants they receive.[18] One example of direct state financial support is funding fusion center operations.

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, implementation, 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:

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 former Governor Arnold Schwarzenegger, provides a useful model of an integrated statewide exercise program.[19] 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. This program has continued under Governor Jerry Brown and has seen its implementation conducted across various emergency planning exercises. For example, in 2013 the California Golden Guardian Exercise activated as a series that continued for 18 months had 20 planning meetings and 11 unique exercises.[20] This series of exercises included collaboration with partners like FEMA Region IX, state agencies outside of the California Governor's Office of Emergency Services, and non-governmental partners.

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.[21]

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?

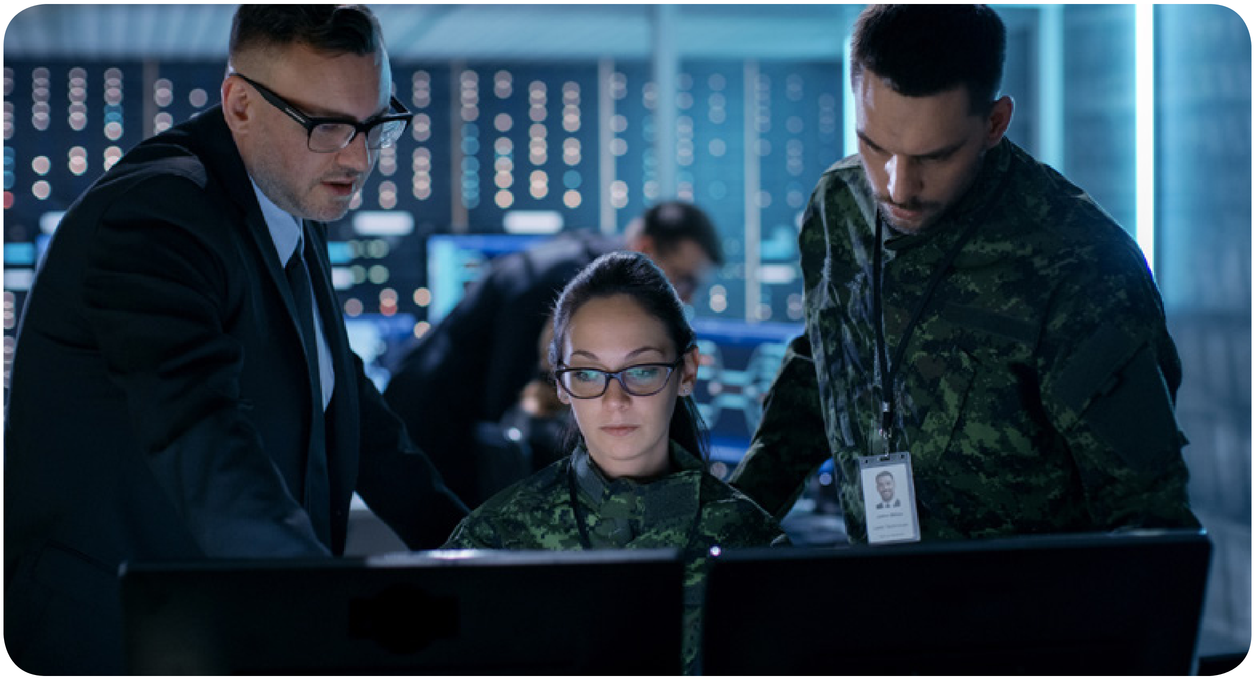
The Naval Postgraduate School, Center for Homeland Defense and Security, offers seminars to help states develop the capabilities to respond to incidents and bolster multi-agency cooperation. The seminars are conducted by mobile education teams composed of nationally recognized experts in various areas 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.

Major National Homeland Security Exercises and Resources

Various national homeland security exercises are conducted that could present opportunities for state agencies to partner on or that could be conducted at a state level to test state agency readiness for those events. Some of these exercises include:

Cyber Storm: Securing Cyber Space

The Department of Homeland Security hosts Cyber Storm on a biennial basis. It is currently the most comprehensive cybersecurity exercise practiced at the federal level. The



origins of Cyber Storm started with a congressional mandate in order to test and strengthen cyber readiness in both the public and private sectors. Some the activities in Cyber Storm events have included the following:[22]

- A review of various organizations and agencies and their readiness for cyber attacks and capabilities to prevent them;
- Interagency coordination activities to respond and prevent cyber attacks and ensure they meet national policy and best practice standards;
- Information sharing capabilities and gaps for partners working to prevent and respond to cyber attacks; and
- Ways to share sensitive information across sectors without compromising this information.

The most recent Cyber Storm event occurred in Spring of 2018.

The National Exercise Program

The National Exercise Program (NEP)[23] was derived from the National Preparedness Goal, which emphasizes:

“A secure and resilient nation with capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”

As a result of this goal, the NEP aims to achieve it by having exercises that aim to build, sustain, and deliver core capabilities for sustainment and improvement.

The NEP works to validate the identified core responsibilities for the preparedness mission areas of prevention, protection, mitigation, response, and recovery. The NEP incorporates a multitude of practices to accomplish these core capabilities. Exercises nominated in the NEP include policy discussions, workshops, tabletop exercises, and drills. The NEP functions on a two-year cycle and is anchored to the Principle Objectives, a common set of strategic objectives, with all the NEP’s exercises coming together in a final biennial National Level Exercise.

Homeland Security Exercise and Evaluation Program (HSEEP)

The Homeland Security Exercise and Evaluation Program (HSEEP) lays out a set of overarching principles to approach homeland security exercise, program management, development of programs, evaluation, and planning. The HSEEP provides frameworks for program managers to help design and develop their own exercises to meet the priorities and goals of their organization or agency. The mechanisms of the HSEEP are based on the National Preparedness Goal, strategy literature, threat identification and risk assessment, and real world events. The principles in the HSEEP that would help to guide a common approach to designing and creating exercises include:

- Guided by elected and appointed officials
- Capability-based
- Progressive planning approach
- Whole community integration
- Informed by risk
- Common methodology

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. In short, the health of the public is routinely at risk. Yet because public health threats are not singular events (e.g., a subway bombing) and are diffused over the entire population, maintaining concern for public health can be 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.

In December 2013, an outbreak of the Ebola virus erupted in West Africa. The U.S. Centers for Disease Control & Prevention (CDC) diagnosed the first case of Ebola in the United States in September of 2014, carried into Texas by a traveler from West Africa. By 2016, eleven people had been treated for Ebola in the United States.[24] While government officials were able to put isolation procedures in place that prevented the spread of the disease, this example demonstrates the unpredictable and potentially dire consequences of a public health threat.

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 and a "terrorist handbook" were discovered in a **Nevada** hotel room, demonstrate the ongoing threat of bioterrorism. In 2018, outbreaks of E. coli occurred across 36 states. As a result of this outbreak close to 210 people were infected and 96 people were hospitalized.[25] This outbreak ultimately resulted in the death of five people and was traced back to Yuma, Arizona, where it had entered the water supply of major romaine lettuce processors. This incident demonstrates the danger of foodborne illnesses that occur naturally or through human 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, Ebola virus, tuberculosis, hepatitis, and smallpox;
- Latent environmental contaminants that can poison large numbers of people, such as lead;
- Foodborne 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 (NIMS). Moreover, in some cases, such as the H1N1 influenza or Ebola outbreaks, 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 experts. The terrorist attacks of September 11, Hurricane Katrina, and the ongoing, nationwide opioid epidemic underscore that all incidents require a collaborative response to fully care for victims and survivors. Often, public health's role and responsibilities in incident response are 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 CDC and DHS 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 guides 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.[26]

In **Arkansas,** the New Madrid seismic zone puts Arkansas and neighboring states at risk for a major earthquake. Poison control centers can be critical in an earthquake response, for example, in case of water contamination. Arkansas developed a plan for neighboring states to support its poison control centers during a catastrophic disaster. This plan utilized a partnership with the Arkansas Poison Control Center and the Emergency Management Assistance Compact, a mutual aid agreement between states and territories. Other states have since adopted a similar model to support one another's poison control centers during a major emergency.[27]

In May 2017, **Massachusetts** conducted an exercise that tested the ability of state health programs to detect health threats, disseminate information, conduct laboratory testing, and distribute medical countermeasures during a full-scale response. Through this exercise, Massachusetts learned the value of engaging healthcare partners to strengthen surveillance activities. It also demonstrated the state's success in mobilizing the communications systems that would be used during a real event to share information, addressing a gap discovered during the H1N1 influenza pandemic.

In **Missouri,** local health departments establish dedicated medication-dispensing sites within each jurisdiction and train partners from all sectors on how to provide life-saving medication to employees, family members, and customers during a public health emergency. There were 916 dispensing sites in Missouri as of October 2017. In a statewide emergency, this dispensing operation could reduce the burden on local health departments by as much as 25 percent while helping ensure that people have fast access to lifesaving medicine.

To address the threat of foodborne illnesses, many states and their departments of agriculture participate in the CDC's Council to Improve Foodborne Outbreak Response (CIFOR).[28] CIFOR is made up of national associations of state public health officials and federal agencies that work collaboratively to optimize processes to control, investigate, and prevent foodborne disease outbreaks. In addition to state and federal representation, members of the food industry are also present to provide their expertise and assistance to the council.

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.

Many states have elected to participate in the Health Information Exchange (HIE), which includes the mobilization of health care information electronically across different groups in a community, hospital systems, and regions. In 2010 the Office of the National Coordinator (ONC) for Health Information Technology funded the launch of the State Health Information Exchange (HIE) Cooperative Agreement Pact and granted 56 awards to launch these exchange networks across states and territories. The funding was used by awardees for:

- The creation and implementation of up-to-date privacy and security requirements for HIE;
- Coordination with Medicaid and state public health programs to establish an integrated approach;
- Monitoring and tracking of meaningful use HIE capabilities; and
- Ensuring consistency with national standards.

While the use of the HIE Cooperative Agreement Pact has risen from 36 percent in 2010 to 79 percent in 2014, this increase was prompted by a small group of states. Still, the HIE Cooperative Agreement Pact remains an avenue for states to have an integrated approach in terms of their state's public health records management and for streamlining efficiency in the sharing of critical data between health systems. **New Jersey**'s Department of Health began developing an HIE in 2018 to allow their health networks to improve interoperability and to guide better-informed clinical decision making. This decision was spurred by other states' success, and **Michigan** in particular, in adopting an HIE network and joining the pact.

In 2017, the ONC continued to push states toward greater integration under the HIE Cooperative Agreement Pact. Improved operability, reduced redundant connections, and the availability of data for disease surveillance systems are all benefits that states can achieve through its adoption. The ONC identified the following obstacles that continue to limit the HIE Cooperative Pact's adoption:

- Existing reporting infrastructure designed to facilitate public health reporting for care providers;
- HIE's technical solution may not supply public health agencies with the level of data required for certain public health functions; and
- Limited resources.

States that want to be a part of the HIE Cooperative Pact can mitigate these limitations through flexible standardized technical solutions and policies that enable public health data reporting through the HIE. More affordable options for states from health IT providers and developers that could also mitigate the resource and financial costs.

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. The Ebola outbreak in 2014 demonstrated a lack of preparedness on the part of various public health entities to cope with the development and spread of Ebola in real time.[29] This was in part a symptom of a greater issue within the context of public health preparedness, which includes a lack of available funding that can be tapped immediately once an outbreak occurs, and a general reliance on federal support in cases of disease outbreaks like Ebola on the part of states. Relying on federal funding for such events, however, may not be the best strategy for state governments and health institutions, given declining federal support for public health preparedness. For example, funding levels for the Public Health Emergency Preparedness cooperative agreement has declined by 70 percent since its peak in 2006.

While in most states federal funds are critical to ensuring a cooperative, coordinated, and robust response, the overreliance on these funds can be dangerous and can delay the response to an outbreak, similar to that of Ebola in 2014 or Zika in 2015. During the Ebola outbreak only three hospitals were initially equipped to handle patients in need of intensive care in the United States. While this number rose to 50 after the outbreak, the delay in having this capability present before the outbreak occurred, especially if the magnitude of the outbreak had been greater, could have severly impacted hospitals' ability to save lives.

To help offset the unpredictability of federal funds to support public health emergencies, states will need to sustain their health infrastructure and support preparedness programs continuously with other sources of funding. A crucial need also exists to establish a public health emergency fund at the state level that can be tapped when an outbreak occurs to help shift the reliance solely from congressionally appropriated funds and allow for more effective responses. 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 is necessary to develop a coordinated response system.

During the 2014 Ebola outbreak, strong partnerships between the private and public sectors helped facilitate a robust response.[30] The CDC released a diverse list of academic and hospital system partners, professional public health organizations, and corporate private partners that all assisted and provided material support for the response between 2014 and 2016, as the CDC worked to contain and neutralize remaining localized outbreaks. Additionally, to accelerate future response efforts to emerging public health emergencies—using the Ebola outbreak as a case study—Congress passed a law[31] in 2015 authorizing the U.S. government to provide subsidies to pharmaceutical companies to expedite the manufacture of the Ebola vaccine and bring it to clinical trials.

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 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 2015, the Federal Emergency Management Agency (FEMA) conducted a survey of 5,008 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 demographics.

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. States at risk for catastrophic disasters, such as those in the Cascadia Subduction Zone, are now actively encouraging citizens to prepare for two weeks without assistance.

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, spare batteries, and, if possible, solar chargers or generators to provide electricity to power communication devices.
- 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.
- Exposure to the basics of amateur (HAM) radio is highly recommended for citizens because in the case of many disasters phones lines, cell towers, and commercial radio may be down.

Findings of FEMA's 2015 National Survey

The 2015 FEMA National Household Survey measured household and individual preparedness, including by targeting citizens in areas prone to hurricanes, tornados, earthquakes, winter storms, floods, and wildfires. The survey found:

- 18 percent of respondents attended a preparedness training or meeting during the prior year;
- 39 percent sought preparedness information during the prior year; and
- On average, 68 percent had enough supplies to last three days.

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, Individual and Community Preparedness Division. "National Household Survey, 2018." https://www.fema.gov/media-library/assets/documents/94717 (accessed October 23, 2018)

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 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 is 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 which 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.

Oregon, a state with a long history of natural disasters, created a two-page checklist for recording financial information that individuals frequently need after a disaster, but which is often left behind or destroyed. The checklist includes reminders to safeguard, among other things:

- Account numbers;
- Personal identification records;
- Copies of critical financial records;
- Computer files; and
- An inventory of belongings.

The checklist contains blank spaces for citizens to record critical records in one place prior to a disaster, allowing victims to evacuate quickly with a copy of essential information.[32]

The Ready **North Carolina** program maintains a comprehensive website with information on potential threats, planning, recovering, and rebuilding. The site features a series of YouTube videos (with sign language interpreters) showing how citizens can make a plan, put together a preparedness toolkit, evacuate, and sign up for emergency alerts. The state's preparedness website also includes information on post-disaster needs like applying for FEMA assistance and safety tips for cleaning up devastated homes.[33]

Oklahoma's McReady program is a public-private partnership designed to prepare families for emergencies

Sample Family Communications Plan

- ✔ Write down phone numbers and email addresses for everyone in the household, and ensure every member has a copy.
- ✔ Discuss emergency response plans for schools and places of work. Ensure that household members with phones are signed up for alerts and warnings from their school, workplace, and/or local government.
- ✔ Identify an out-of-town individual who can act as a central point of contact to help the household reconnect.
- ✔ Subscribe to alert services. Many communities have systems that will send instant text alerts or e-mails to communicate information about bad weather, road closings, local emergencies, and more.
- ✔ Decide on safe, familiar places indoors, nearby, outside the neighborhood, or out-of-town to go for protection or to reunite. Ensure such locations are accessible to all household members.

Source: U.S. Department of Homeland Security, http://www.ready.gov/make-a-plan (accessed October 23, 2018).

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 videos are shown in schools throughout the state and officials with the National Weather Service hold weather radio programming events as part of the program.[34]

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 **Florida, Louisiana, Texas,** and **Virginia**[35] 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. In October 2017, **Pennsylvania** Governor Tom Wolf held a five-day Governor's Emergency Preparedness Summit.

PREVENT

CHAPTER 6.

State and Major Urban Area Fusion Centers

Key Concepts

- State and major urban area fusion centers bring together information and personnel from various agencies and levels of government to develop crucial homeland security and public safety intelligence. Currently, 79 fusion centers are operating across the nation serving as a national asset to protect the homeland.
- Governors and homeland security advisors (HSAs) 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 state or major urban area fusion centers 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 and major urban area 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 coordination 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:[36]

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, 79 fusion centers are operating nationwide. All 50 states now have at least one state-designated fusion center; the remaining 29 fusion centers reside in major cities and three territories. States with more than one fusion center must designate a primary fusion center for their state. The state-designated fusion center has a number of unique coordinating and reporting responsibilities related to the FEMA grant program.

In 2016, the total cost of operating the nationwide network of fusion centers was $322 million. State funds covered 35 percent, localities provided 25 percent, and federal dollars made up 35 percent (19 percent from DHS grants and 16 percent from direct federal expenditures).

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 an 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 counterterrorism program at the state level. Many fusion centers include state National Guard personnel and have co-located with the FBI's Joint Terrorism Task Forces, FBI Field Intelligence Groups, and High Intensity Drug Trafficking Area Investigative Support Centers (HIDTA-ISCs).

Source: U.S. Department of Homeland Security, "State and Major Urban Areas Fusion Centers," revised August 31, 2018, http://www.dhs.gov/state-and-major-urban-areas-fusion-centers (accessed October 22, 2018).

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 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. DHS is responsible for nationwide implementation of suspicious activity reporting. The FBI is responsible for the implementation and management of the SAR Data Repository that captures reported SAR.

Furthermore, as fusion centers have evolved and their practices have become more streamlined, co-location of fusion centers with partner agencies has become the standard. Co-location improves opportunities for synchronization with partner agencies and greater collaboration in counterterrorism activities, law enforcement efforts, critical infrastructure protection, and other public safety objectives. As of 2016, 100 percent of fusion centers report that they are co-located with a partner agency in the federal or state, local, tribal, territorial (SLTT) jurisdiction.

Lastly, as the management of fusion centers has evolved along with their operational capabilities, governance structures for fusion centers have also started to become more streamlined and consistent across the country. As of 2016, 69 percent maintain a formal governance body that manages fusion center operations and provides oversight for them. Fifteen fusion center (19 percent) have alternatives to a formal governance body.

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.[37]

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.[38] 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 and major urban area 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)[39] 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. Participants include federal agencies, states, municipalities, and other local government entities, with a significant number of users from the law enforcement community. HSIN enables multiple jurisdictions, disciplines, and emergency operation centers to receive and share the same intelligence and tactical information with each other. 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.

The Law Enforcement Enterprise Portal (LEEP) is an electronic gateway that provides law enforcement agencies, intelligence partners, and criminal justice groups with a centralized access system to different resources and services through a single sign-on mechanism. Ultimately, the aim of sharing these resources can strengthen the development of cases for investigators and enhance information sharing among agencies. Resources included on LEEP are:[40]

- Virtual Command Center
- Special Interest Group
- VCC Trax
- Active Shooter
- Internet Crimes Complaint Center (IC3)
- Malware Investigator

Understand Intelligence and Information-Sharing Challenges

While these initiatives have improved information sharing, 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;
- Inconsistencies in criminal justice and financial crimes information access;
- Privacy concerns; and
- Homeland security advisor 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 Recognition

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.

Inconsistencies in Criminal Justice and Financial Crimes Information Access

Designated fusion centers need consistent access to criminal justice and financial crimes information. However, some designated fusion centers that operate under the control of emergency management departments are denied access to vital criminal justice information sources. Additionally, financial crimes information is not consistently shared across the fusion center network.

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 governor's homeland security advisor (HSA) 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, HSAs need to be aware of all intelligence and counter terrorism efforts occurring at the fusion center level.

Learn from Other State Fusion Centers

The **New Jersey State Police** opened New Jersey's first Regional Operations and Intelligence Center (ROIC)[41] and fusion center in the wake of 9/11. The ROIC focuses on command and control on a 24/7 basis. Its mandate is broader than that of traditional homeland security because it also includes traffic control, anti-gang initiatives, and community policing. The goal of the ROIC in New Jersey is to be an active presence in the Information Sharing Environment, increase the public safety of the region and the nation, mitigate the threat of injury to members of the public and health care communities, mitigate the risk of property damage, protect individual privacy and civil rights/civil liberties, protect the integrity of the criminal justice system, and promote cooperation between the community and law enforcement.

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 Administration (DEA), and the Department of Homeland Security (DHS). 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 federal government has identified 17 sectors of critical infrastructure spanning agriculture, energy, and telecommunications. Protecting critical infrastructure and ensuring continuity of operations demands close cooperation with the private sector, which owns and/or operates the vast majority of critical assets.
- Essential steps to protecting critical infrastructure include conducting vulnerability assessments and prioritizing assets, understanding how different sectors depend on one another, and coordinating with the private sector and other states.
- 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 are essential to a nationwide security strategy. Critical infrastructure involves physical or virtual assets whose incapacitation would cause a debilitating impact on the state and/or the entire nation. Identifying the key critical infrastructure and resources in a state is a first step, and preserving these assets from potential disaster is a critical component of a governor's homeland security strategy.

Nationally, 17 sectors of critical infrastructure have been designated by presidential directive: chemical facilities; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare; information technology; civilian nuclear facilities; transportation; water and wastewater systems; and election systems.[42]

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 are physical and cyber-based systems that are essential to the minimum operations of the economy and government.[43] An estimated 85 percent of the nation's critical infrastructure is 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."[44]

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 their vulnerabilities.

State legislatures have taken a variety of approaches to ensuring critical infrastructure protection. Below are some examples of state actions.

In 2014, **New York** passed a law to empower the Division of Homeland Security and Emergency Services to prioritize further protections for critical infrastructure, including commercial aviation, petroleum and natural gas fuel transmission facilities and pipelines.[45] It required, among other things, that the commissioner of the Division of Homeland Security and Emergency Services conduct a review and analysis of any other measures being taken by the state or its partners to protect critical infrastructure. The law went further to allow the commissioner of the Division of Homeland Security to physically inspect and audit sites and to require commercial owners of sites to provide access to the Division of Homeland Security for these inspections.

In 2018, **Iowa** passed a bill that would provide criminal convictions and large fines for the sabotage of pipelines, telecommunication facilities, water treatment plants, and other critical infrastructure.[46] It created the crime of "critical infrastructure sabotage" as a Class B felony, punishable by up to 25 years in prison and a fine ranging between $85,000 to $100,000.

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.[47] 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, 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 Critical Infrastructure and Key Resources (CIKR), 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 (PNWER) 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. Examples of actions that the PNWER has taken on include:

Regional Critical Infrastructure Protection Work Group – The PNWER conducts quarterly conference calls with critical infrastructure protection managers from their member jurisdictions, allowing them to have an open forum to discuss broader challenges to critical infrastructure protection.[48]

Northwest Warning Alert and Response – This regional communication tool is available for cross-sector critical infrastructure communications. The tool is web-based and provides information from trusted sources to help protect critical infrastructure. It is capable of providing early warning messages and two-way situational awareness before and during a disaster with impacts on critical infrastructure.

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 ensuring 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.[49] 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 the Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience.[50] The aim of PPD-21 is to advance the national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. To accomplish this, PPD-21 directs the federal government to work with critical infrastructure owners and operators to take steps to manage risk and to strengthen the nation's existing critical infrastructure.

This collaborative work aims to reduce existing vulnerabilities, minimize potential consequences, identify and disrupt threats, and accelerate response and recovery associated with critical infrastructure. PPD-21 goes further in its efforts in outlining what qualifies as critical infrastructure by specifically highlighting energy and communications systems due to the enabling functions they provide across all critical infrastructure sectors. PPD-21 expedites Homeland Security Presidential Directive 7 (HSPD-7) which designated lead federal agencies, known as sector-specific agencies that must collaborate with the private sector to develop information-sharing and analysis mechanisms. PPD-21 highlights three strategic imperatives:

- Refining and clarifying the functional relationships across the federal government to advance the national unity of efforts to strengthen critical infrastructure
- Enabling effective information exchange by identifying baseline data system requirements
- Implementing an integration and analysis function to inform planning and operations decisions for critical infrastructure

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."[51] The department published an updated version of this comprehensive plan, known as the National Infrastructure Protection Plan (NIPP), in 2013. NIPP provides a unifying structure that aligns multiple efforts to protect state critical infrastructure and key resources.

The **State, Local, Tribal, and Territorial Government Coordinating Council** (SLTTGCC) works to strengthen the sector partnership structure by gathering geographically varied experts from a broad pool of critical infrastructure areas to ensure that state, local, tribal, and territorial officials have an active role in national critical infrastructure security and resilience. The mission of the SLTTGCC includes:

- Senior-level, cross-jurisdictional strategic coordination in partnership with DHS;
- Planning, revision, updates, and implementation of the National Infrastructure Protection Plan (NIPP), Sector-Specific Plans (SSP);
- Coordinating strategic issue management among state, local, tribal, and territorial partners and federal partners;
- Coordinating with DHS to support efforts to develop plans, implement, and execute the nation's critical infrastructure protection mission; and
- Providing the Department of Homeland Security with information on state, local, tribal, and territorial critical infrastructure protection initiatives, activities, and best practices.

The **National Infrastructure Protection Plan (NIPP) 2013** aims to guide the national effort to manage risks to the country's critical infrastructure by collectively identifying national priorities, goals, mitigating risks, measuring progress, and adapting based on feedback. Success can only be achieved by having a broad array of expertise, capabilities, experiences, and building partnerships. 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 GCCs 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 GCC.

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 a vast array of computer systems that manage sensitive data and control critical government functions, including emergency communications, transportation networks, and the distribution of public benefits. Governors and much of state government are also essential partners for municipal governments, educational institutions and companies—large and small—that provide vital services such as financial data, electricity, and medical services.
- Governors constantly face the threat of a high consequence cyberattack. In an interdependent economy, seemingly minor incidents have the potential to cascade into crises. Financial markets cannot operate without electricity, and power plants require natural gas, the price of which depends on financial markets. An attack against a single sector could have broader implications and require comprehensive preparation for management and recovery.
- Cyberattacks are inevitable. State security offices monitor constant probing by attackers searching for any gaps in state defenses. Every state agency must prepare for breaches by formalizing plans that allow them to recover data and restore services quickly. Close collaboration with private partners will enhance resiliency.
- Focus on governance first, and technology second. Governors should create a formal body to ensure that: (1) appropriate agencies can agree on, and implement, a statewide cybersecurity strategy and action plan; (2) the state has and can exercise a cyber disruption response and recovery plan; and (3) cybersecurity leaders have the authority to enforce cybersecurity plans and manage recovery operations.
- Consider appointing a chief cybersecurity advisor who can execute a statewide cybersecurity strategy. Whereas a chief information security officer (see below) focuses on defending state-owned networks, a cybersecurity advisor can build partnerships to advance cybersecurity for the entire state.

Public safety is a foundational tenet of gubernatorial leadership, and all states have law enforcement agencies, fire protective services, and emergency response systems to anticipate and respond to public safety emergencies. During the past few years, cyber threats have grown in scope and sophistication and require a comprehensive public safety umbrella. Citizens and state officials rely on computer networks for virtually every aspect of modern life and government. Securing those networks is now an indispensable element of safeguarding the public welfare.

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

- Learn about cyber risks;
- Develop a cybersecurity strategy and action plan;
- Manage statewide coordination between state agencies, municipal governments, private business, education and civic organizations; and
- Recognize the federal government's role, use federal resources, and accommodate the limited assistance federal authorities can provide.

Learn More About the Risks

Computers usually connect to one another, share information, and control processes remotely. Many software and hardware systems are designed for easy access. When combined with the globalized architecture of the Internet, openness makes computer systems attractive for criminals, hacktivists, and foreign adversaries who want to steal confidential information, damage or destroy computer systems, or disrupt information flows.

Any organization that relies on computerized information systems is vulnerable to these attackers, and states offer an especially attractive target. State agencies collect and store massive amounts of personal and financial data. They also own, operate, and regulate critical infrastructure. Yet, by their nature, many state information systems are difficult to defend against outside attackers. States must maintain online portals that allow citizens to complete tax forms, apply for licenses, register to vote, pay traffc violations, file annual reports, renew vehicle registration, and request permits. Attackers exploit these types of public-facing resources on a regular basis. Many state agencies manage their information systems through third party contractors. When those vendors practice lax security, they provide a pathway for attackers into state systems. Not all attackers are external. Insiders enjoy privileged access that can allow them to cause serious damage without needing to bypass any security measures.

Attackers, whether external or internal, have different motivations. Some want citizens' financial or health data so they can sell it on the black market, steal identities, and/or commit fraud. Others are activists seeking to publicize wrongdoing or embarrassing secrets. Disgruntled employees may decide to settle a personal vendetta via cyberattack. Foreign intelligence operatives use cyber intrusions to search for a greater understanding of U.S. politics, intellectual property, classified documents, or information that they can use to compromise federal, state, or local officials.

Cyber threats facing states are not hypothetical. To date, thousands of state information systems have fallen victim to cyberattacks. Some have been relatively benign, such as defacing a state agency's web page. Others have been more damaging. In one case, hackers altered a tax commission website to download malicious software (malware) onto the computer of any visitor. This attack allowed hackers to take control of those computers.

Other breaches have accessed and copied large datasets containing highly sensitive financial information. Direct and indirect costs from these breaches run into the millions of dollars. More dangerous attacks have disabled systems that run emergency communications, health services, or transportation nodes. States must protect these systems while also planning for the worst; should an attack on critical services succeed, response and recovery must be swift and comprehensive.

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.

Develop a Cybersecurity Governance Structure

In the face of growing risks from cyberattacks, technology companies have made significant investments to develop software and hardware defenses. Today, many of those solutions allow state agencies to reduce the likelihood of a security incident and to restrict potential damage. The primary challenge for state government is not technology; it is the governance processes that ensure state agencies use the technology correctly, and plan for when that technology fails. States need a unified approach that encompasses non-traditional security partners such as health and human services, department of transportation, or universities, that can craft, implement, and enforce statewide cybersecurity strategies and response procedures.

STEP 1: Conduct a Statewide Risk Assessment

A risk assessment will establish the baseline risk confronting state operations and/or the state more generally, e.g., private businesses, schools, and municipalities. The assessment will identify vulnerabilities to assets, internal and external threats to those assets, consequences if those threats attack vulnerabilities, and resources available to mitigate the vulnerabilities and respond to attacks. It should also identify the comprehensive list of cybersecurity standards and guidelines that already apply to state agencies or other organizations.

STEP 2: Choose a Mechanism for Creating a Governance Body

A cybersecurity governance body may be a committee, commission, council, or working group. It may be created by an executive order, legislation, policy, or simple ad-hoc convening. Depending on the state, different mechanisms carry various advantages and disadvantages. Accounting for political realities, sunset rules, public records statutes, and budgetary requirements will result in more realistic timelines and encourage sensitive discussion among members of the governance body and their outside partners.

STEP 3: Establish the Purpose and Structure of the Governance Body

Information technology and cybersecurity projects risk failure without concrete, coherent objectives. Will a state cybersecurity body focus on securing state networks alone, or will it study how the state can assist private sector cybersecurity as well? Will it simply offer recommendations, or craft and operationalize cybersecurity standards that agencies must follow? If the body will be issuing funding recommendations, organizers might want to include legislative representation. In the latter case, a governor should issue an executive order or seek legislation that authorizes the body and/or its members to mandate specific actions.

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 55 states, territories, 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.

Establish an Enterprise Cybersecurity Program

An established governance body can define the legal authorities, procurement policies, administrative procedures, and interagency collaboration needed to adopt basic cybersecurity measures across all state agencies. Specifically, it can:

- Define the roles and responsibilities of key cybersecurity personnel and ensure the necessary authority exists for those personnel to fulfill their duties and reflect the state's essential cybersecurity priorities;
- Monitor for vulnerabilities, intrusions, and security breaches;
- Log network activity to track threats and repeated attempts to gain access;
- Develop statewide policies for baseline cyber security procedures;
- Create user-friendly incident reporting;
- Encourage data encryption;
- Provide cybersecurity education and training for state employees and contractors in conjunction with the Multi-State Information Sharing and Analysis Center (see breakout box: Role of the Multi-State Information Sharing and Analysis Center on this page);

- Generate a statewide culture of cybersecurity awareness and cybersecurity hygiene under the governor's leadership.

Plan a Statewide Approach to Cybersecurity

Leaders should consider how the cyber threat affects non-state assets, and integrate public and private activities accordingly. A high consequence cyberattack against private assets, such as telecommunications systems, electrical grids, gas and oil pipelines, and transportation networks, could cause serious harm to state interests. These sectors of infrastructure are interdependent, and a successful attack on one sector could have a cascading effect on several others. A reliable supply of energy, for example, is essential to the operation of hospitals, transportation systems, 9-1-1 dispatch centers, and water and wastewater treatment facilities.

The public expects state officials to engage in planning and preparation commensurate with other types of potential disasters or emergencies. A collaborative process can help ensure comprehensive planning and preparation. Most infrastructure is owned by the private sector, and efforts to mandate cybersecurity standards for private companies are controversial. Governors should direct their state homeland security advisor (HSA), state chief information officer (or chief information security officer), and state energy offcials to:

- Employ cybersecurity governance bodies to engage with private sector entities that have cybersecurity expertise and determine how state agencies and non-state experts can collaborate;
- Employ cybersecurity governance bodies to engage with private entities that lack cybersecurity expertise and determine their preparedness gaps to tailor state cybersecurity assistance;
- Draft, formalize, and test a statewide cyber disruption response plan that includes procedures for assisting (and requesting assistance from) private entities in the event of a high consequence disruption;
- Participate in federal and private-sector cybersecurity initiatives to build partnerships and learn about new tools and practices.

Effective, exercised relations between private-sector infrastructure owners and state and local governments are crucial to detecting security incidents and responding to cyberattacks.

Understand the Federal Government's Role and Disruption Response

The federal government has a critical role in state cybersecurity. Federal authorities offer a wealth of knowledge and resources to detect, prevent, and investigate cyberattacks. The National Cybersecurity & Communications Integration Center, operated by the U.S. Department of Homeland Security, acts as a national fusion center focused on protecting the nation's critical infrastructure against cyberattacks. DHS cybersecurity advisors spread across the country offer a wide variety of free services to assist states and localities in finding cyber vulnerabilities and conducting cyber exercises. Additionally, the Federal Bureau of Investigation works closely with state and local law enforcement to notify state agencies of security incidents and investigate significant computer crimes. These agencies can share their uniquely sophisticated understanding of foreign cyber threats to help state officials design more effective cybersecurity measures. Governors should direct their cybersecurity leaders and/or cybersecurity governance bodies to leverage the myriad federal resources that often go untapped.

However, if defensive measures fail and a high consequence cyberattack strikes a city or region, states cannot assume that federal authorities will bear the brunt of response efforts. While Washington has attempted to assign clear roles and responsibilities through Presidential Policy Directive 41 (PPD-41) and the National Cyber Incident Response Plan (NCIRP), no one has integrated these procedures with state-level cyber emergency plans.

Governors should direct their advisors to prepare to respond to serious cyber incidents on their own. Planning should include the creation of a cyber disruption response plan that accounts for the full range of available assets, from private businesses to the National Guard, and considers interdependencies between different critical infrastructure sectors: state agencies, local government, utilities, telecommunications firms, transportation nodes, and financial institutions. Once plans are formalized, state officials should invite relevant stakeholders (including federal officials) to a cyber response exercise that tests planning assumptions. These rehearsals present opportunities to clarify the federal role and integrate state operations with federal procedures.

RESPOND

CHAPTER 9.

National Guard and Military Assistance

Key Concepts

- Governors have at their disposal a crucial 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, natural disaster, 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, Stafford 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 and the funding sources.
- In 2010, the Council of Governors was established to provide a bi-partisan forum for 10 governors—five Democratic governors, and five Republican governors—and key federal officials to discuss unity of effort among state and federal military forces, response to catastrophic disasters, cybersecurity, and other key issues regarding National Guard missions and resources.

National Guard capabilities can be deployed to meet various needs before, during, or after an emergency or a significant event. During a presidential inauguration, for example, the National Guard can be used to assist first responders and local law enforcement personnel with crowd control and civil disturbance missions, strategic traffic control points, and visitor screening. Under vastly different circumstances, the National Guard responded to hurricanes Irma, Harvey, and Maria where a total of approximately 45,000 guardsmen and woman supported recovery efforts. Simultaneously, the National Guard supported wildland firefighting efforts across several states.

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, disaster response, 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**,[52] "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." 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;

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 or Title 32 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.[54]
- 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.[55]
- 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.[56]
- 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.[57]
- The Secret Service may request military assistance to protect the president from assault, manslaughter, or murder.[58]
- 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.[59]

and when acting in the service of the United States, he shall appoint his staff, and the legislature shall fix his rank."[53]

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 **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.[60] 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."[61] 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. Created by the National Defense Authorization Act and formally established by Executive Order 13528 in 2010, the Council of Governors consists of 10 governors appointed by the president—five from each party—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; cybersecurity information sharing; 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.[62]

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.[63] 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.[64] The Department of Homeland Security is the lead federal agency for homeland security.

At the state level, homeland security may be incorporated into a defense agency, for example 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."[65]

The National Guard straddles both the homeland defense and homeland security 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

The National Guard Bureau (NGB) is a joint activity of the Department of Defense. The Chief of the National Guard Bureau is a member of the Joint Chiefs of Staff and serves as a principal advisor to the Secretary of Defense and the president on the non-federalized National Guard. 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. It also assists the states in the organization, maintenance, and operation of their National Guard units and provides trained and equipped units capable of immediate expansion to war strength in a time of war or emergency. As part of its homeland defense mission, the NGB identifies ten 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.

manager. For example, in **Washington** state, homeland security apparatus is embedded in the Washington Military Department. The office of the director 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.[66]

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 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. The key to a Title 32 deployment is that it places a soldier and airmen in a full-duty status under command and control of the governor but 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, or as 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** (NORTHCOM) 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, NORTHCOM generally operates through its subordinate joint task forces. An emergency must exceed the capabilities of local, state, and federal agencies before NORTHCOM becomes involved. In most cases, support will be limited, localized, and specific. Through the Secretary of Defense, at the direction of the president, NORTHCOM can provide defense support to civil authorities if requested by state, local, tribal, and federal officials as part of the National Response Framework.‡

One of the standing joint task forces operating under NORTHCOM 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 assisting 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 who have technical training by agencies that include the National Fire Academy, Department of Defense, Department of Energy, and the Environmental Protection Agency.

In addition to CSTs, the governor may also use National Guard **CBRNE enhanced response force packages**

‡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.

(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 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 and are usually assembled within 6 to 12 hours after being alerted. Each FEMA region has an assigned HRF composed of 583 National Guard members. Each HRF can respond 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 are available and under the control of the governor and are a mechanism for interested employment under an emergency management assistance compact (EMAC) control support.

Cyber Security and the National Guard

The National Guard is also well qualified to help support state cybersecurity efforts given its citizen-soldier construct. Across several states, many guardsmen and women serve in critical cyber fields in their civilian jobs, which can translate into critical cyber defense skills.

National Guard cyber protection teams help to boost state and federal cyber defense capabilities. These teams operate on a part-time basis in support of their respective states and governors. When mobilized in a federal status, the teams can provide surge support to the Department of Defense defensive cyberspace operations.

Army and Air National Guard cyber forces are projected to grow to 59 units in 38 states by the end of 2018. These units are trained to joint standards established by U.S. Cyber Command. Additionally, the Army Guard has 54 Defensive Cyberspace Operations Elements in each of the 50 states, three territories and the District of Columbia to provide the first line of defense for our military networks.

How Can State and Federal Military Response Activities Be Integrated Effectively? The Dual Status Commander.

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.

With the consent of the governor and authorization of the president, through a memorandum of agreement, 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 and usually at a major disaster occurrence.

Frameworks for Government Response to Emergencies

The National Incident Management System (NIMS)

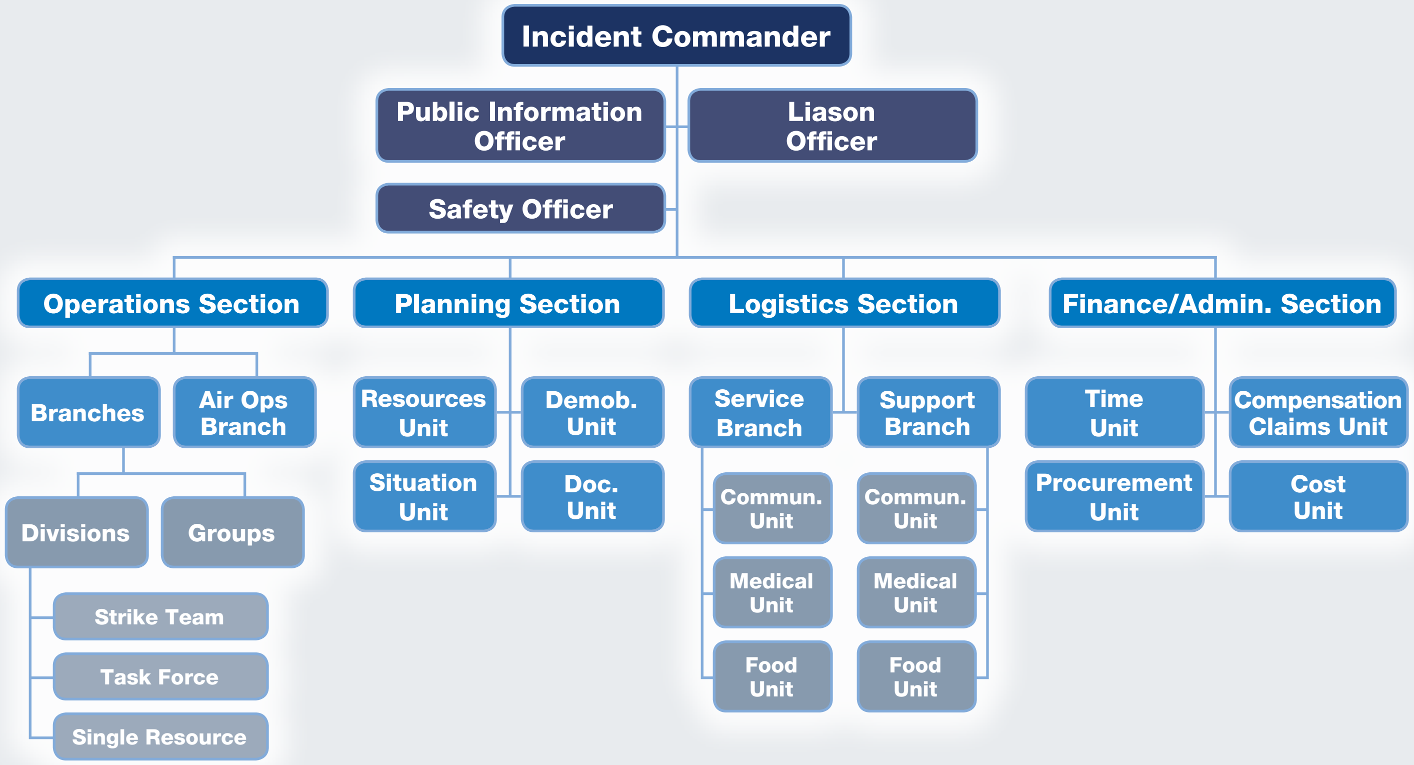
The National Incident Management Systems (NIMS) helps manage any critical incident or event that involves coordination across multiple jurisdictions or job disciplines. Homeland Security Presidential Directive-5 (Feb. 28, 2003) directed the Department of Homeland Security to create NIMS to provide a national approach to prepare for, respond to, and recover from domestic incidents.[67] It applies not only to emergency managers, but all state, territorial, tribal, and local governments; private partners such as critical infrastructure owners; and non-government organizations involved in emergency management. NIMS components include:

- **Resource Management,** including preparedness and mutual aid;
- **Command and Coordination,** including the use of the Incident Command System (ICS) and Emergency Operations Centers (EOCs); and
- **Communications and Information Management,** including interoperability.

The Department of Homeland Security has made NIMS adoption a requirement for states to obtain FEMA preparedness grants. NIMS has companion frameworks, including the National Response Framework (NRF) and National Disasters Recovery Framework (NDRF) that establish common platforms for specific components of incident management.

The Incident Command System (ICS)

One core component of NIMS is the Incident Command System (ICS), which provides the structure by which personnel involved in a response must organize. ICS is a common approach to the command, control, and coordination of a response that creates the standardization across jurisdictions and agencies so important for large-scale events or critical incidents. Originally created for the fire services discipline, ICS has now been adopted by all first responders, emergency managers, and other entities involved in response nationwide. The following chart demonstrates the different roles and functions within ICS.[68]



Emergency Support Functions (ESFs)

Within different functions of ICS (Command, Operations, Planning, Logistics, and Finance/Administration), there are also fifteen different Emergency Support Functions (ESFs) or activities necessary for a comprehensive response.[69] The ESFs are:

1. Transportation
2. Communications
3. Public Work and Engineering
4. Firefighting
5. Emergency Management
6. Mass Care, Housing, and Human Services
7. Logistics Management and Resource Support
8. Public Health and Medical Services
9. Search and Rescue
10. Oil and Hazardous Materials Response
11. Agriculture and Natural Resources
12. Energy
13. Public Safety and Security
14. Long-Term Community Recovery (see the National Disaster Response Framework)
15. External Affairs

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 (EMAC) 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, liability laws, 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 (EMAC)** is a mutual aid agreement to which all 50 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands 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.[70] 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 (EMAC), 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.

California, established the California Disaster and Civil Defense Master Mutual Aid Agreement in 1950 to allow the various departments, political subdivision, municipal corporations, public agencies, and the state of California to effectively share resources in response to a disaster. The agreement was developed in accordance with the California Disaster Act and required all parties to this agreement to abide by later intrastate agreements and federal mutual aid agreements California would enter. A timely example of the continued need for this agreement was its activation to help battle the severe wildfires burning across California in 2017. The California Governor's Office of Emergency Services (CAL OES) activated the statewide mutual aid agreement to provide better logistical and resource support to firefighters across the state.

Maine has a statewide mutual aid agreement that provides avenues for local governments and the state government to assist one another during an emergency event. In 2009, Maine passed the Authorizing Statewide Mutual Aid Among First Responder Agencies Act, allowing local first responder agencies to provide emergency services to one another at the request of another town without any additional agreement in place. In 2014, new changes have been made to this agreement to specify that anyone directed by MEMA or local emergency management agencies in an emergency are considered state employees. Fire protection has also been added to the agreement to allow the governor to mobilize mutual aid to assist with fire emergencies.

Interstate Mutual Aid

When incidents overwhelm a states's response capabilities, 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 EMAC. 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

2017 was a historic hurricane season and required out-of-state assistance from other jurisdictions. The combined cost of Hurricane Harvey, Irma, and Maria is estimated to be roughly 385 billion dollars. It affected multiple states and territories including Texas, Florida, Georgia, Louisiana, Puerto Rico, and the U.S. Virgin Islands. EMAC was instrumental in ensuring that states were able to get the resources and personnel they needed. Through EMAC, 16,600 personnel were deployed from across the United States to support areas impacted by Harvey, Irma, and Maria.

Between August 2017 and July 2018, roughly 19,200 personnel deployed to emergencies ranging from wildfires to mass shootings. EMAC addresses most challenges to interstate mutual aid, including the following:

The acceptance of out-of-state professional medical licenses. EMAC stipulates 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.[71]

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.[72]

Legal liability claims that arise from the activities of out-of-state workers. EMAC states that officers or employees of a state rendering aid in another state pursuant to the compact are considered agents of the requesting state for tort liability and immunity purposes.[73]

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.[74]

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."[75]

How EMAC Works and the Benefits of Membership

The Emergency Management Assistance Compact (EMAC) 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 utilizes their internal Advance Teams (A-Teams) or requests the deployment of an A-Team to facilitate assistance.
- The A-Team works with the state to fill resource requests identified by the affected state and determines costs and availability of resources from Assisting States.
- 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.

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, which also counts Guam, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia among its members.[76]

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 53.)

Considerations with 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 while 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 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**.[77]

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.[78]

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.[79]

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.[80]

California, Nevada, and **Oregon** have created a regional sharing agreement known as the **"California, Nevada, and Oregon Chempack Sharing Procedures"**. This set of procedures is focused around the Centers for Disease Control and Prevention (CDC) established Chempack Project, with the goal of assisting states with the Federal Strategic National Stockpile of drugs and medical supplies to protect communities against harmful effects of chemical agents that can attack the human nervous system. These three states have elected to join the Chempack and have thus signed a memorandum of agreement with the CDC that outlines both federal and state roles. If adopted by all states in the region, it would help harmonize sharing and assistance procedures among them if an event were to occur.

The Great Lakes Border Health Initiative Public Health Data Sharing Agreement is another example of an interstate aid and cooperation agreement signed by **Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania, Wisconsin,** and the Canadian province of **Ontario.** The purpose of this agreement is to facilitate the sharing of public health data pertaining to individuals and populations to all signatories in an effort to prevent, detect, or respond to a major public health event impacting the region. The primary mechanism to facilitate this sharing is the requirement for each signatory to provide copies of their respective statutes related to public health events, infectious disease agents, and other relevant materials to one another to help guide what health data would be shared amongst the member states.

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.
- Governors 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.

Public safety depends on the entire emergency communications ecosystem: alerts & warnings, 9-1-1, public safety broadband, and land mobile radio. These tools are the primary means through which citizens and first responders verbally communicate with each other and get access to critical information.

Within a state, a multitude of agencies with responsibility for protecting the public safety independently select the various communication systems they will use. This decentralized approach can pose particular challenges for homeland security. Natural and manmade disasters may cross over county and state lines or require a response

What Is the Emergency Communications Ecosystem?[81]

Alerts and Warnings: "Alerts and Warnings" include notification systems used to issue alerts, warnings, and incident-related information, primarily from government agencies over privately-owned communications networks and services to individuals, private sector entities, and nongovernmental organizations. IPAWS, the Integrated Alert and Warning System, is used by state authorities and can integrate local systems that use Common Alerting Protocol (CAP), to push out alerts to the public using the Emergency Alert System (EAS).

9-1-1 and Next Generation 9-1-1: Traditional 9-1-1 uses analog technology and only allows for voice transmissions between the caller and 9-1-1 dispatch center. Next Generation 9-1-1 (NG9-1-1) is an Internet Protocol-based system that allows voice, photos, videos, text messages and other data to flow seamlessly from the caller to the 9-1-1 dispatcher and onto public safety personnel and first responders.

Land Mobile Radio: Land mobile radio (LMR) is a land-based wireless narrowband communications system commonly used by federal, state, local, tribal and territorial emergency responders; public works agencies; and the military to support voice and some low-speed data communications.

Public Safety Broadband (i.e., FirstNet): Broadband is a means to transfer voice and data information (cellular phone calls, access to databases, videos, photos) over cellular-based infrastructure networks.

Who are the stakeholders?

Statewide Interoperability Executive Committee (SIEC) and Statewide Interoperability Governing Body (SIGB): An SIEC or SIGB provides a statewide, unified approach across multiple disciplines and jurisdictions to address system implementation and upgrades, funding, and overall support for communications interoperability.[82] SIECs and SIGBs have predominately been responsible for LMR systems and have recently added public safety broadband as a responsibility.

State 9-1-1 Boards: A state 9-1-1 board collects and disseminates 9-1-1 fees to local 9-1-1 boards and sets statewide, strategic goals.

9-1-1 Administrator: A state's 911 administrator supports the statewide implementation and maintenance of 911 services, identifying and recommending the minimum standards for emergency phone systems.[83]

Statewide Interoperability Coordinators (SWIC): The SWIC's primary function is to plan and implement the statewide interoperability program—historically confined to just LMR systems—and to support the SIEC/SIGB.[84]

FirstNet State Point of Contact (SPOC): A governor's designated point of contact for coordinating the decisions around FirstNet. In December 2017, all governors elected to opt in to FirstNet. Since then, states have maintained the SPOC position, eliminated the role, or transferred its responsibilities to ensure oversight of the FirstNet implementation in the state.

that exceeds the capacity of a single department. Large-scale incidents often demand multiple agencies to work together harmoniously, making coordination essential. An inability for first responders to communicate can lengthen response times, reduce their ability to assess situations, make the coordination of mutual aid more difficult, and create confusion at the scene of an incident.

As states continue to strengthen their homeland security posture, many recognize the need to enhance the interoperability of their emergency communications ecosystem. First responders require tools that are not only operable during critical incidents but also allow them to communicate across carriers, devices, agencies, jurisdictions, systems, and most importantly allow our citizens to send and receive information critical for decision making.

Challenges

Two overarching challenges impede the functionality and interoperability of emergency communications: (1) insufficient funding to maintain infrastructure and adopt new technology, and (2) inadequate coordination among state agencies, localities, and tribes.

Insufficient Funding

With a wide variety of competing public safety priorities, it can be challenging for states to secure sufficient funding for emergency communications. Existing emergency communications tools may be perfectly sufficient for first responders' everyday needs but may require significant investment to improve the ecosystem's functionality during a critical incident or large-scale event. For a layman, there may also be misconceptions about legacy infrastructure's capabilities and how emerging technology either complements or supplants that infrastructure. For instance, the general public may not understand the necessity of maintaining an LMR system due to the inability of broadband networks using smart phones to provide mission critical push-to-talk capabilities. Further, the ancillary costs of emergency communications—hiring more full-time employees, contracting for data storage, and migrating a legacy system to an IP-based system—may be less obvious.

Inadequate Coordination

Various governance bodies, such as statewide interoperability executive committees (SIECs) or 9-1-1 boards, are responsible for coordinating components within their portion of the emergency communications ecosystem. These governance bodies, however, may not have a formal relationship. For instance, authorizing

language for an SIEC may not include the state 9-1-1 administrator as an SIEC member. Further, in some states, alerts and warnings may not be integrated into any governance body. This lack of coordination across the emergency communication ecosystem may contribute to misalignment of strategic goals and funding priorities or hinder the ability of a state to address significant challenges, such as securing the ecosystem against cyber threats.

Promising Practices

Governors and their cabinet members can overcome these challenges by: (1) informing and building relationships with key stakeholders to provide accurate information on emergency communications' capabilities and capacities; (2) securing financial support for existing and emerging technologies; and (3) leveraging a multi-stakeholder governance body to coordinate state and local efforts.

Inform and Build Relationships

Governors and their cabinet members should engage local stakeholders and legislators to build relationships and provide accurate information on the emergency communication ecosystem's capabilities. Governors' offices should review their SIEC's authorizing language to ensure local and legislative representation is adequate. Similarly, governors' offices can task the SIEC chair, who may be a cabinet member, to review the SIEC roster and meeting attendance to assess if new members are required to adequately represent and inform their respective localities.

Second, governors can propose legislation or issue an executive order mandating the SIEC submit a report card to the legislature and the executive branch on the status of emergency communications. This can help foster accountability and educate state leaders on capabilities and funding limitations.

Third, cabinet members can invite legislators and other stakeholders to site visits or tabletop exercises to highlight the need for improved emergency communications and their role in disaster response. For example, visiting public safety answering points (PSAPs)—the locations that receive 9-1-1 calls and dispatch responding officials—can vividly illustrate data exchange between caller and dispatcher, as well as the quality of radio transmissions.

Secure financial support for existing and emerging technologies

Governors and their cabinet members should request that their SIECs and other related bodies inventory the investments made into emergency communications, their current funding sources, and the cost to purchase new technology or sustain existing infrastructure. Governors' offices can then use this information to prioritize funding requests with the legislature. Second, cabinet members should discuss how emergency communications can support other priorities, such as school safety and domestic violence, to further explain the need to fund these systems to legislators. It should be seen as an investment in public safety and not seen as an expense. Lastly, if a cabinet member chairs the state's SIEC, they should propose that the SIEC assist in streamlining local and state agency funding requests for the legislature and governor.

Leverage a multi-stakeholder governance body to coordinate state and local efforts

Governors need to ensure that SIECs, 9-1-1 boards, and other governing bodies have institutionalized relationships to provide and receive information, solicit input on funding priorities, develop policies and procedures, and set goals for the future. Governors should review SIECs and other governance bodies' executive orders or authorizing legislation to ensure relevant stakeholders are represented on the appropriate governance bodies. The review should also determine whether the bodies have the appropriate authorities to carry out their prescribed missions. For instance, governors may want to maintain the SPOC position, which may require funding a full-time employee without federal assistance, or transfer the SPOC's roles and responsibilities to the SIEC or SIGB. This will enable governors to ensure FirstNet implementation is successful according to the state's plan detailing the buildout and maintenance of the Nationwide Public Safety Broadband Network (NPSBN). Lastly, governors should consider creating full-time positions to manage, coordinate, and share information on emergency communications with their office.

Maintaining an active, multi-stakeholder governance body that can effectively disseminate information is key to emergency communications. Governors and their offices play an important role in advancing public safety through ensuring effective emergency communications governance.

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. The 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 60).

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 Assistance 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

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. The NRF builds on and supersedes the National Response Plan (NRP), which was published in 2004. The NRF provides more flexibility than its predecessor and enables ongoing development and refinement of all-hazards emergency operations plans. The 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.

In June of 2016, the Department of Homeland Security released the third edition of the NRF. The NRF still serves as a guide for how the nation would respond to all types of disasters and emergencies, and it describes the principles, roles and responsibilities, and coordinating structure for delivering core capabilities in an emergency or disaster event. The NRF identifies response mission areas and a range of incidents that the nation should be prepared to respond to, and it defines those response mission areas to identify the capabilities necessary to save lives, protect property, meet basic human needs, stabilize the incident, and restore basic services and community functionality. There are 15 core capabilities in the response mission areas of the NRF, some of them are: planning, public information and warning, critical transportation, environmental response/health and safety, and logistics and supply chain management.

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."[85]

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."[86]

Take Appropriate Actions Prior to Requesting a Presidential Declaration

As a prerequisite to disaster assistance under the Stafford Act, the governor must take appropriate 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 has occurred.

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.

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 (HSA) assist the governor with counterterrorism efforts, including intelligence gatherring, so 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. A comprehensive communications 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 most important role of the governor is to set realistic expectations among disaster survivors and to provide comfort through both words and actions. 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 toward 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.

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 65). 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 emphasizing 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.

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;

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 has been collected. To achieve these ends the governor should operationalize a core response team to manage information flow coming into the office for critical decision-making as well as the dissemination of information to the public.

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 visually 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 (HSA) 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 important, 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 HSA 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.

- 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 other 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. A 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 (e.g., Twitter), social networking (e.g, Facebook), and high-volume text messaging enable instantaneous communication with large audiences. In the aftermath of Hurricane Maria in Puerto Rico, survivors used social media apps like Twitter, Facebook, Zello, and WhatsApp to gather information about recovery efforts, connect with loved ones, and communicate with authorities.

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.

SONY
3 KCRA HD
NOTICIAS 19
FOX40 NEWS

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.

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 $128,900 or more—payment is made on the basis of actual costs after the project is completed, though interim payments can be made. When 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.

Eligible Work Criteria

In order for reimbursement, eligible work must be required as a result of the declared incident, be located in the designated area, be the legal responsibility of the applicant, and conducted at a reasonable cost.

Eligible work is classified into the following categories:

1. *Emergency Work:*
   - Category A: Debris removal
   - Category B: Emergency Protective Measures

2. *Permanent Work:*
   - Category C: Roads and Bridges
   - Category D: Water Control Facilities
   - Category E: Public Buildings and Contents
   - Category F: Public Utilities
   - Category G: Parks, Recreational, and other facilities

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

Crisis Counseling Assistance and Training provides services to people affected by presidentially declared disasters or emergencies. Two separate parts of the Crisis Counseling Program 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, diagnostics, and counseling 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.

The Individuals and Households Program (IHP) Housing Assistance Provision

FEMA determines the appropriate types of housing assistance for which an individual or household may be eligible based on disaster-caused loss, access to life-sustaining services, cost-effectiveness, and other factors. Individuals and households may receive more than one type of housing assistance, including a combination of financial assistance and direct services for disaster damage to a disaster survivor's primary residence.

FEMA provides funds paid directly to eligible individuals and households and may include the following types of assistance:

1) Temporary housing for rent;
2) A government-provided housing unit when rental properties are not available;
3) Funds to help homeowners repair damage to their primary residence that is not covered by insurance;
4) Funding for homeowners to replace their home destroyed in the disaster when not covered by insurance; and
5) Permanent housing construction.

Direct assistance or money for permanent housing construction is provided only in insular areas or remote locations specified by FEMA, where no other type of housing assistance is possible.

To provide direct temporary housing assistance, FEMA offers the Multi-Family Lease and Repair Program (MLRP). This program allows FEMA to enter in lease agreements with owners of multi-family rental properties and make repairs to create temporary housing availability. In addition to grant assistance, the Disaster Relief Fund is used to reimburse federal agencies through mission assignments for relief and recovery work requested by FEMA.

IHP Other Needs Assistance Provision

Individuals and households may receive financial assistance for other disaster-caused expenses and serious needs. Eligibility for some types of Other Needs Assistance are dependent on eligibility with the U.S. Small Business Administration's (SBA) disaster loan program. The SBA provides low interest, long-term loans to help individuals and households with personal property, transportation, moving, and storage expenses incurred due to a declared disaster.

IHP is not intended to replace private recovery efforts but rather to complement those efforts when needed. FEMA's assistance is limited and is not intended to return a home to its pre-disaster condition. If a homeowner wishes to return their home to its pre-disaster condition, they may apply for a home disaster loan with the SBA.

Disaster survivors may need to provide documentation to help FEMA evaluate their eligibility, such as documents pertaining to proof of occupancy, ownership, income loss, and/or information concerning an applicant's housing situation prior to the disaster. Financial assistance is limited to an annually adjusted amount based on the Department of Labor Consumer Price Index.

Applicants whose homes are located in a special flood hazard area and who receive assistance for home repair, replacement, permanent housing construction, and/or personal property as a result of a flood-caused disaster must obtain and maintain flood insurance as a condition of accepting disaster assistance. Assistance is limited to 18 months following the disaster declaration and may be extended, if needed.

Some of the assistance that is offered includes the following programs:

FEMA IHP Other Needs Assistance is divided into two categories that are either dependent or non-dependent on the individual's or household's ability to qualify for an SBA disaster loan.

SBA Dependent Types of Other Needs Assistance includes only individuals or households who do not qualify for a loan from the SBA may be eligible for the following types of assistance:

- **Personal Property Assistance** is used to repair or replace essential household items including, but not limited to, furnishings and appliances, accessibility items defined within the Americans with Disabilities Act, and specialized tools and protective clothing required by an employer.

- **Transportation Assistance** includes repairs or a replacement of a vehicle damaged by a disaster and other transportation-related costs.

- **Moving and Storage Assistance** is used to relocate and store personal property from the damaged primary residence to prevent further disaster damage, such as ongoing repairs, and returning the property to the primary residence.

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.

Non-SBA Dependent Types of Other Needs Assistance may be awarded regardless of the individual's or household's SBA disaster loan status and may include:

- **Funeral Assistance** is available to individuals and households who have incurred or will incur eligible funeral expenses that are directly or indirectly related to the disaster.
- **Medical and Dental Assistance** is available to assist with medical or dental expenses caused by a disaster, which may include injury, illness, loss of prescribed medication and equipment, or insurance co-payments.
- **Child Care Assistance** is a one-time payment, covering up to eight cumulative weeks of childcare expenses, for a household's increased financial burden

to care for children ages 13 and under; and/or children ages 14 to 18 with a disability as defined by federal law.

- **Miscellaneous or Other Items Assistance** is a category used to reimburse for eligible items purchased or rented after a disaster incident for an individual or household's recovery, such as gaining access to the property or assisting with cleaning efforts. Eligible items are identified by the state, territorial, or tribal government and may include items such as a chainsaw, air purifier, or dehumidifier.

Housing & Urban Development (HUD)

HUD's mission is to increase homeownership, support community development, and increase access to affordable housing free from discrimination. As the federal experts on providing permanent housing assistance for low-income families, HUD is uniquely positioned to assist the housing needs of those affected by a disaster.

HUD's National Housing Locator (NHL) is a website that can assist individuals and families in finding rental housing in a presidentially declared or local disaster. It allows HUD and its business partners, in particular other federal agencies, to deliver housing assistance by rapidly locating rental housing and available government-owned, foreclosed homes for sale during an emergency. Through lenders approved by HUD's Federal Housing Administration (FHA), the department offers insured mortgages for disaster victims to rebuild substantially damaged or destroyed homes or to rehabilitate less damaged homes.

HUD also addresses community recovery needs through its management of the Community Development Block Grant (CDBG) program. The CDBG program focuses on a wide range of community and economic development and housing needs nationwide, representing about 1,200 cities and urban counties, and states, and is a funding vehicle for the rebuilding of communities devastated in disasters.

Following a disaster, HUD plays a key role in long-term community recovery under the National Response Framework. Long-Term Community Recovery, ESF #14, provides a mechanism for coordinating federal support to state, tribal, regional, and local governments, nongovernmental organizations, and the private sector to enable community recovery from the long-term consequences of extraordinary disasters. As one of four primary agencies for this Emergency Support Function, HUD provides building technical assistance for housing, community redevelopment and economic recovery, public services, infrastructure, mortgage financing, and public housing repair and reconstruction.

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 U.S. Small Business Administration (SBA) offers affordable financial help to businesses and private non-profit organizations in declared disaster areas. Help is available in the form of low-interest, long-term loans for losses not fully covered by insurance or other means.

SBA's disaster loans are the main federal assistance offered for the repair and rebuilding of non-farm, private sector disaster losses. This is the only SBA direct loan program and it is not limited to small businesses.

Businesses of all sizes as well as private non-profit organizations may borrow up to $2 million to repair or replace:

- Damaged or destroyed real estate;
- Machinery and equipment; and
- Inventory and other business assets

In some cases, SBA may be able to refinance all or part of a prior mortgage or lien. They may also be able to increase the loan up to 20 percent of the confirmed physical losses.

Applicants can use the increase to make improvements that reduce the risk of damage by future disasters. Examples of improvements include retaining walls, seawalls, sump pumps, safe rooms, and storm shelters.

The SBA offers Economic Injury Disaster Loans (EIDL) up to $2 million to help meet working capital needs caused by the disaster. Any of the following may qualify for EIDL:

- Small businesses
- Small agricultural cooperatives
- Small businesses engaged in aquaculture
- Most private non-profit organizations of all sizes

EIDL help is available regardless of whether the business had any physical property damage.

The statutory limit for business loans is $2 million. This applies to the combination of all funding paid to a business and its affiliates for each disaster.

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.

Emergency Conservation Program (ECP) provides funding to rehabilitate farmland damaged by wind erosion, floods, hurricanes or other natural disasters, and for carrying out emergency water conservation measures during periods of severe drought.

Emergency Forest Restoration Program (EFRP) provides payments to eligible owners of rural nonindustrial private forestland to carry out emergency measures to restore forest health on land damaged by natural disaster events, such as floods, or hurricanes.

Emergency Assistance for Livestock, Honeybees and Farm-Raised Fish Program (ELAP) provides payments to eligible producers of livestock, honeybees and farm-raised fish to help compensate for losses due to disease (including cattle tick fever), adverse weather or other conditions, such as blizzards and wildfires.

Emergency Loan Program (EM) provides loans to help producers recover from production and physical losses due to drought, flooding, other natural disasters or quarantine.

Livestock Indemnity Program (LIP) provides benefits to livestock owners and some contract growers for livestock deaths in excess of normal mortality that are the direct result of an eligible adverse weather event. In addition, LIP covers attacks by animals reintroduced into the wild by the federal government or protected by federal law.
Noninsured Crop Disaster Assistance Program (NAP) provides financial assistance for non-insurable crop losses due to drought, flood, hurricane, or other natural disasters.

Tree Assistance Program (TAP) provides financial assistance to qualifying orchardists and nursery tree growers to replant or, where applicable, rehabilitate eligible trees, bushes, and vines lost by natural disasters. A qualifying mortality loss in excess of 15 percent (in excess of normal mortality) must be sustained to trigger assistance.

Dairy Indemnity Payment Program (DIPP) provides compensation to dairy producers when a public regulatory agency directs them to remove their raw milk from the commercial market because pesticides, nuclear radiation or fallout, or toxic substances and chemical residues other than pesticides have contaminated it.

CHAPTER 15.

Long-Term Recovery Strategies

Key Concepts

- Governors play a key role in strengthening and rebuilding disaster- or emergency-affected communities by providing leadership, resources, and a plan for the long term in coordination with other stakeholders.
- Preparing for long-term recovery should begin well before a disaster strikes and include a pre-disaster recovery plan that can guide the response.
- The governor's office can establish recovery organizations in partnership with the state emergency management office to help 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 federal and state resources at the beginning of the recovery phase will greatly improve recovery outcomes and resilience to future incidents.

Governors can take proactive steps to ensure successful 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.

Pre-Disaster Recovery Planning

In many cases, affected states and communities do not have a robust long-term recovery plan in place and are forced to create ad hoc organizations and efforts to coordinate across agencies and manage the influx of resources from federal partners.

Pre-disaster recovery planning should follow a process that engages members of the whole community, develops the recovery capabilities of the state government and its partners (NGOs, private groups, and others) and combines these efforts to develop an organizational framework for a comprehensive recovery effort. This pre-disaster recovery planning process enhances resilience by clarifying roles and responsibilities, improving communication channels, and building robust community partnerships to spearhead recovery efforts.

An effective pre-disaster recovery plan highlights the goals for each party involved, the state's priorities and policies, and the roles and responsibilities of different stakeholders in the recovery process. Having these items in a pre-disaster recovery plan is essential because it enables external actors, like the federal government and NGOs assisting in the recovery process, to seamlessly integrate themselves into the ongoing recovery effort and understand the state's priorities. For a more comprehensive guide on the key tenets of a pre-disaster recovery plan, an in-depth discussion of its establishment, and necessary implementation procedures, please refer to the 2016 "Pre-Disaster Recovery Planning Guide for State Governments" published by FEMA.

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.

Businesses will assess damages, and may decide to rebuild or close indefinitely. At this point, the long-term recovery plan begins.[87]

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 those who may be homeless because of 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 citizens.

Currently, no enabling legislation exists to provide federal grants to states for long-term recovery efforts.[88] 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).[89] NDRF serves as a companion guide to the National Response Framework and provides federal guidance for long-term disaster recovery.

Coordinate State Support to Assist Local Recovery Efforts

Just as disaster preparation and response are primarily local functions, so is long-term recovery. Such efforts involve 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, and a broad range of state government agencies besides the state administrative agency may be involved in assisting local communities with recovery, including:[90]

- 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. For example, **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 Hurricane Harvey in 2017, the state of **Texas** was left with major devistation to the Costal Bend, central, and southeastern Texas. The damage caused by Harvey was so great that Governor Abbott requested between 150 billion and 180 billion dollars in aid from the federal government (the damage caused by hurricanes Katrina and Sandy were 120 billion and 50 billion, respectively). Further, he launched the Commission to Rebuild Texas to help guide the state's long-term recovery efforts. The commission focused on the following items:

- Marshalling state agency resources in order to coordinate the statewide effort to rebuild public infrastructure including roads, bridges, schools, government buildings, and others.

- Assisting local governmental entities and nonprofits with rebuilding needs and navigating the availability of state and federal resources.
- Establishing a "one-stop" support center for local officials who are seeking information and support for rebuilding public infrastructure.
- Issuing public updates on response efforts.

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.[91] Following the passage of the Post-Katrina Emergency Management Reform Act, FEMA established Recovery Support Functions (RSFs). The RSFs make up the coordinating framework for essential functional areas of assistance in the National Disaster Recovery Framework (NDRF). They work to support local governments by engaging in troubleshooting to improve access to resources and by encouraging coordination between federal and state actors, NGOs, and other vested parties in a recovery. The following groups and their associated federal departments are current RSFs as of June 2018:

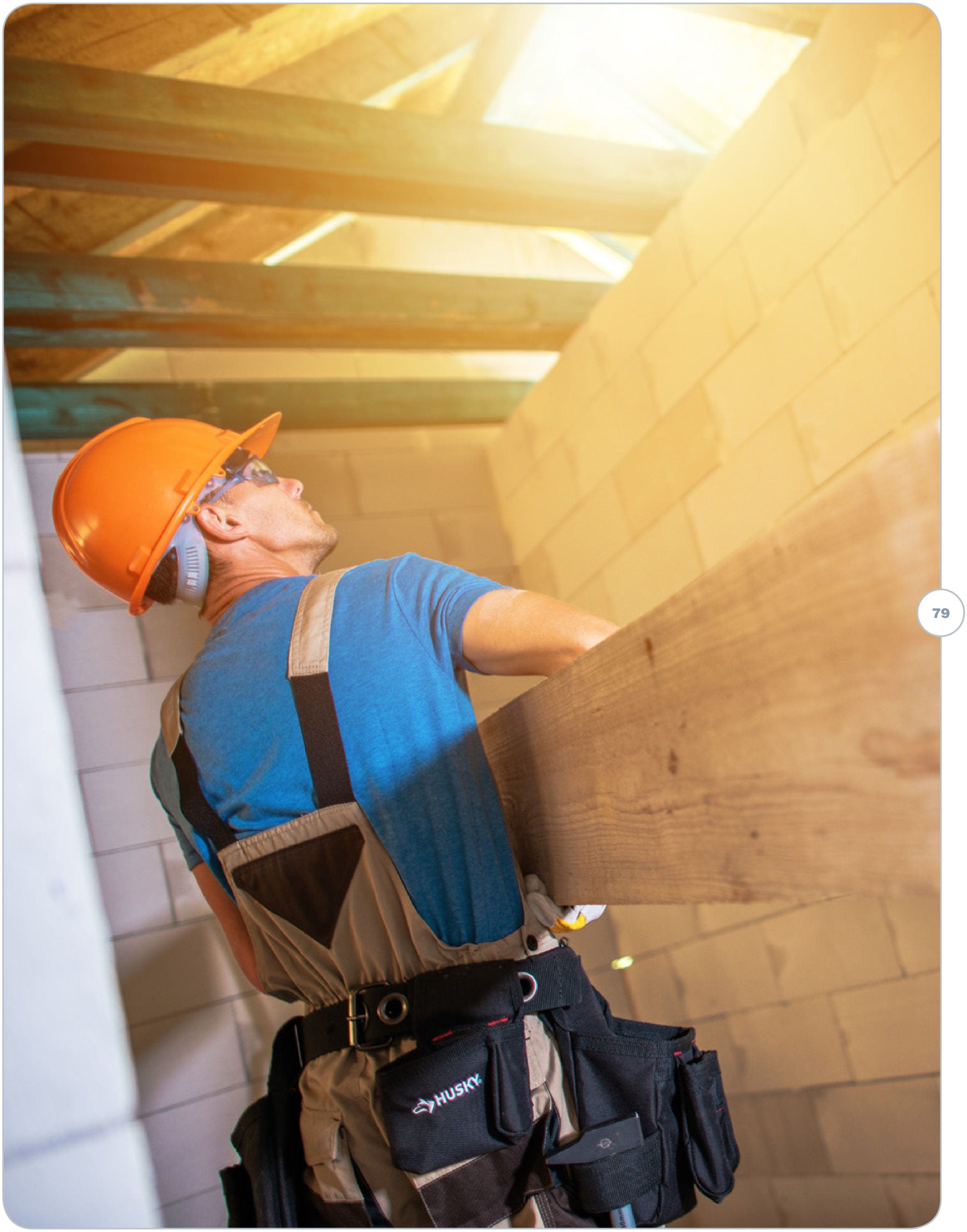
- Economic Recovery Support Function, U.S. Department of Commerce
- Health and Social Services Recovery Support Function, U.S. Department of Health and Human Services
- Housing Recovery Support Function, U.S. Department of Housing and Urban Development
- Infrastructure Systems Recovery Support Function, U.S. Army Corp of Engineers
- Natural and Cultural Resources Recovery Support Function, U.S. Department of Interior
- Community Planning and Capacity Building (CPCB), Federal Emergency Management Administration[92]

To activate a federal RSF 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 an RSF 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.[93]

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.[94]

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. However, empowering communities early on, 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 toward recovery. Indeed, discussions about long-term recovery will lead to planning for future events, bringing full circle the emergency management rubric—prepare, prevent, respond, and recover.



HUSKY

End Notes

1. Louisiana Governor's Office of Homeland Security & Emergency Preparedness website: http://gohsep.la.gov/ABOUT/OVERVIEW (accessed April 2, 2018).
2. Indiana Department of Homeland Security Mission website: https://www.in.gov/dhs/2358.htm (accessed April 2, 2018).
3. State of Minnesota, Division of Homeland Security & emergency Management, All Hazard Mitigation Plan March 14, 2014, page 14
4. West Virginia Division of Homeland Security and Emergency Management website: https://dhsem.wv.gov/about/Pages/default.aspx
5. DHS, "National Homeland Security Strategy" page 3. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurit y_2007.pdf (accessed August, 2018)
6. U.S. Department of Homeland Security; National Strategy for Homeland Security, 2007. Page 1. See http://www.dhs.gov/xlibrary/ assets/nat_strat_homelandsecurit y_2007.pdf (accessed August, 2018)
7. U.S. Department of Defense, DoD 101: "An Introductory 72 overview of the Department of Defense," http://www.defense.gov/ pubs/dod101/dod101.html (accessed August , 2010).
8. US Department of Homeland Security, National response Framework, Glossary, (https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf , accessed August, 2018).
9. Cyber Storm: Securing Cyber Space, https://www.dhs.gov/cyber-storm, 2018 (Date Accessed September 2018)
10. US Department of Homeland Security, "National response Framework," (June 2016), page 19. https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/ National_Response_Framework3rd.pdf (accessed September , 2018).
11. Federal Emergency Management Agency (FEMA), "National Incident Management System," December 2008, https://www.fema. gov/media-library/assets/documents/130743. (August 2018)
12. U.S. Department of Homeland Security; National Strategy for Homeland Security, 2007. Page 1. See http://www.dhs.gov/xlibrary/ assets/nat_strat_homelandsecurit y_2007.pdf (accessed September, 2018)
13. Federal Emergency Management Agency (FEMA), "Fiscal Year 2018 Port Security Grant Program Frequently Asked Questions," May 2018 (Accessed September 2018)
14. Federal Emergency Management Agency (FEMA), "Fiscal Year 2018 Nonprofit Security Grant Program Frequently Asked Questions," May 2018 (Accessed September 2018)
15. Department of Justice Programs, "Edward Byrne Memorial Justice Assistance Grant (JAG) Program," https://www.bja.gov/jag/. (September 2018)
16. Center for Disease Control and Prevention (CDC), "Public Health Emergency (PHEP) Cooperative Agreement," https://www.cdc.gov/phpr/readiness/phep.htm (September 2018)
17. U.S. Department of Health and Human Services, "ASPR Funding and Grant Opportunities," June 2018. https://www.phe.gov/Preparedness/planning/hpp/Pages/funding.aspx (Accessed September 2018)
18. National Emergency Management Association. "Homeland Security Grant Return on Investment", August 2018 (Accessed September 2018)
19. California emergency Management Agency, "Golden Guardian exercise Program,", August 2013 http://www.caloes.ca.gov/ CaliforniaSpecializedTrainingInstituteSite/Documents/GG13%20Exercise%20Series%20Executive%20Brief.pdf (Accessed September 2018).
20. California Governor's Office of Emergency Services, "State Level Exercises", http://www.caloes.ca.gov/for-schools-educators/training/ csti-exercises/state-level-exercise (2013) (accessed September 2018)
21. Office of Alabama Emergency Management Agency, "Alabama Mutual Aid Teams to Participate in Full Scale Exercise," Press Release, May 2009
22. Ibid.
23. Federal Emergency Management Agency (FEMA), National Exercise Program, https://www.fema.gov/national-exercise-program. 2018 (Date Accessed September 2018)
24. The Next Plague is Coming. Is America Ready?, The Atlantic, https://www.theatlantic.com/magazine/archive/2018/07/when-the-next-plague-hits/561734/, (Date accessed: August 2018)
25. Multistate Outbreak of E.coli O157:H7, "Infections Linked to Romaine Lettuce," https://www.cdc.gov/ecoli/2018/o157h7-04-18/ index.html. June 2018 (Date accessed: August 2018)
26. Telephone Interview with Robert Mauskopf, Virginia Department of Health, and Rue White, Virginia Department of Human Resources. July 28th, 2008
27. Arkansas Department of Information, "Arkansas Wireless Information Network," https://www.dis.arkansas.gov/about-dis (accessed September 2018).
28. Council to Improve Foodborne Outbreak Response (CIFOR), Center for Disease Control, https://www.cdc.gov/ncezid/dfwed/food-safety-office/cifor.html, (Date accessed: August 2018)
29. Strengthening US Public Health Preparedness and Response Operations, Health Security, https://www.ncbi.nlm.nih.gov/pmc/ articles/PMC5314964/, (Date Accessed: August 2018)
30. "Major Partners Involved in CDC's Response to the 2014-2016 Ebola Epidemic," Center for Disease Control and Prevention, https:// www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/partners.html, (date accessed: August 2018)
31. "In Ebola response, Big Pharama and public sector strive to make up for lost time," PRI, https://www.pri.org/stories/2015-01-29/ebola-response-big-pharma-and-public-sector-strive-make-lost-time, (Date Accessed: August 2018)
32. Oregon Department of Consumer and Business Services, "Your disaster preparedness checklist: Protect your personal finances," http://dfr.oregon.gov/gethelp/ins-help/home/Documents/5331-checklist.pdf (accessed April 10, 2018).
33. North Carolina Department of Public Safety, "Plan and Prepare," https://readync.org/EN/Plan.html (accessed April 10, 2018).
34. State of Oklahoma, Oklahoma Department of Emergency Management" "McReady Program" https://www.ok.gov/mcready/About_the_McReady_Program/index.html. September 2018
35. Virginia Department of Taxation, "May Sales Tax Holiday: Hurricane and emergency Preparedness equipment," http:// www.tax.virginia.gov/site.cfm?alias=HurricanePrepared nessequipmentHoliday (accessed September 2018).
36. 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 2018).

37. Paul Wormeli and Andrea Walter, “Disaster Preparedness & recovery: The evolution of the National Information Exchange Model,” Emergency Management Magazine, August 2009.
38. “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 2018).
39. US. Department of Homeland Security, Homeland Security Information Network (HSIN) 2017 Annual Report. https://www.dhs.gov/hsin-2017-annual-report. (Accessed September 2018)
40. Law Enforcement Enterprise Portal (LEEP), Federal Bureau of Investigations (FBI) https://www. fbi.gov/services/cjis/leep (Accessed September 2018)
41. Welcome to NJ ROIC, New Jersey Office of Emergency Management, https://www.state.nj.us/njoem/media/pdf/102308_oembulletin.pdf, (Accessed September 2018)
42. Ibid
43. 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
44. John Moteff, Critical Infrastructure: The National Asset Database, (Washington, DC Congressional research Service, 2007, page 1.
45. 2014 New York Laws Executive Article 26, JUSTIA US Law, https://law.justia.com/codes/new-york/2014/exc/article-26/716/ (Accessed September 2018)
46. Iowa Legislature, Senate File 2235, Office of the Governor, https:// www.legis.iowa.gov/legislation/BillBook?ga=87&ba=SF%202235, (Accessed September 2018)
47. State of New Jersey, “Administrative Order No. 2005-05” (2005) www.njwec.org/PDF/TCPA%20Ao% 20Final%20Signed.pdf
48. Regional Partnership Pacific Northwest Economic Region, https:// www.fema.gov/media-library-data/1470072945787-e15e127644b8e 2b418d5c000f5be4856/pnwer_partnership-1.pdf , (Accessed September 2018)
49. The Infrastructure Security Partnership, “About Us” http://www. tisp.org/index.cfm?pid=10213 (September 2018).
50. Presidential Policy Directive-Critical Infrastructure Security and Resilience, PPD-21, The Obama White House, (2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Accessed September 2018)
51. The Homeland Security Act of 2002. Public Law 107–296, (2002).
52. State of Oregon. “Constitution of Oregon - 2009 edition,” (2009): Section 9, http://www.leg.state.or.us/orcons/ orcons.html (September 3, 2010).
53. State of Alabama. “Constitution of the State of Alabama,” (1901): Section 131, http://alisondb.legislature.state.al.us/acas/ACASLogin.asp (September 3, 2010).
54. Maintenance and Operation of Equipment, 10 USC § 374, Office of the Law Revision Counsel, U.S. House of Representatives.
55. Prohibited transactions involving nuclear materials, 18 USC § 831, Office of the Law Revision Counsel, U.S. House of Representatives.
56. Emergency situations involving chemical or biological weapons of mass destruction, 10 USC § 382, Office of the Law Revision Counsel, U.S. House of Representatives.
57. 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.
58. Powers, authorities, and duties of United States Secret Service, 18 USC § 3056, Office of the Law Revision Counsel, U.S. House of Representatives.
59. Congressional, Cabinet, and Supreme Court assassination, kidnapping, and assault, 18 USC § 351, Office of the Law Revision Counsel, U.S. House of Representatives.
60. Federal aid for state governments, 10 U.S.C. §§ 331-335, 73 Office of the Law Revision Counsel, U.S. House of Representatives.
61. John Warner National Defense Authorization Act for Fiscal Year 2007, 109th Cong., 2d sess., 2006, http://www.rules.house.gov/109_2nd/text/hr5122cr/1092nd5 122cr_1.pdf (Accessed September 3, 2010).
62. 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 2018).
63. DHS, “National Homeland Security Strategy” page 3. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurit y_2007.pdf (Accessed September 2018)
64. U.S. Department of Homeland Security; National Strategy for Homeland Security, 2007. Page 1. See http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurit y_2007.pdf (accessed September 2018).
65. Idaho Bureau of Homeland Security, “About Us,” http://www.bhs.idaho.gov/pages/AboutUs.aspx (Accessed September 2018).
66. Washington Military Department, “About Us,” https://www.mil.wa.gov/about-us (Accessed October 2018).
67. Homeland Security Presidential Directive-5, https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf (Accessed October 2018)
68. Federal Emergency Management Agency, “ICS Organization,” https://emilms.fema.gov/IS200b/ICS0102280text.htm (Accessed October 2018).
69. Federal Emergency Management Agency, “National Disaster Recovery Framework,” https://www.fema.gov/media-librarydata/1466014998123-4bec8550930f774269e0c5968b120ba2/National_Disaster_Recovery_Framework2nd.pdf (Accessed September 2018).
70. National Emergency Management Association, Emergency Management Assistance Compact, “Model Mutual Aid Legislation” http://www.emacweb.org/?150 (Accessed August 2018).
71. National Emergency Management Association, “Article v- Licenses and Permits,” Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (Accessed September 2018).
72. National Emergency Management Association, “Article IX-Reimbursement,” Emergency Management Assistance Compact, http://www.emacweb.org/?1838
73. National Emergency Management Association, “Article VI-Liability,” Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (Accessed September, 2018).
74. National Emergency Management Association, “Article VIII-Compensation,” Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (Accessed September, 2018).
75. National Emergency Management Association, “Article I-Purpose and Authorities,” Emergency Management Assistance Compact, http://www.emacweb.org/?1838 (accessed September 2018).
76. Federal Emergency Management Agency, “Emergency Management Assistance Compact: Overview for National Response Framework,” https://www.fema.gov/media-library-data/20130726-1914-25045-8516/final_national_response_framework_20130501.pdf (Accessed August, 2018).
77. Pacific Coast Collaborative, Regional Best Practices: http://www.pacificcoastcollaborative.org/priorities/emergency/Pages/emergency.aspx (Accessed September 2010)
78. Mid America Alliance, Mission Statement: http://www.unmc.edu/apps/midamerica/index.cfm?L1_ID=1 &CoNreF=1 (Accessed September 2010).

79. State of Maine, Maine Emergency Management Agency, https://www.maine.gov/mema/ (Accessed September, 2018).
80. Northern New England Metropolitan Medical Response System, http://www.nnemmrs.org/ (Accessed September, 2018).
81. Definitions derived from the U.S. Department of Homeland Security. "National Emergency Communications Plan." 2015. https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf
82. SIECs and SIGBs are interchangeable terms. U.S. Department of Homeland Security. "National Emergency Communications Plan." 2015. https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf
83. U.S. Department of Homeland Security. "National Emergency Communications Plan." 2015.https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf
84. Ibid.
85. Federal Emergency Management Agency, "Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288) as amended," https://www.fema.gov/robert-t-stafford-disasterrelief-and-emergency-assistance-act-public-law-93-288-amended (Accessed September 2018).
86. Ibid.
87. Federal Emergency Management Agency, "Long Term Community Recovery Planning Process: A Self-Help Guide," 2005, https://www.fema.gov/media-library-data/20130726-1538-20490-8825/selfhelp.pdf (Accessed September 2018).
88. 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).
89. Ibid.
90. Ibid.
91. U.S. Department of Homeland Security, "The Department's Five Responsibilities," https://www.dhs.gov/blog/2009/06/08/departments-five-responsibilities (Accessed October 2018).
92. Ibid.
93. Ibid.
94. U.S. Department of Homeland Security, "The Road to Recovery: The Federal Family's Coordinated Efforts to Support Survivors in the Aftermath of Hurricane Harvey (2017) https://www.fema.gov/news-release/2017/09/02/road-recovery-federal-familys-coordinated-efforts-support-survivors (accessed September 2018).

NGA CENTER DIVISIONS

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

- **Economic Opportunity** 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, research synthesis, policy analysis, technical assistance and resources to governors and their staff on education topics spanning early childhood through college and career. At the center of the division's work are three principles: equity, alignment, and data-driven. The division focuses its work on five key initiatives: whole child; personalized education; human capital; standards, assessments, and accountability; and governance and finance. Each initiative includes a range of focus areas that align with the needs of governors and their education policy advisors.

- **Environment, Energy & Transportation** focuses on a range of energy, environment, and infrastructure issues including: developing a modren, efficient, reliable and resilient electricity grid, exploring state transportation solutions involving new technologies such as autonomous vehicles, drones, ride-hailing and electrification; managing the use of water resources including addressing the water-energy nexus; exploring innovative financing mechanizms for energy and infrastructure and exploring smarter states solutions including connected technologies and communications networks.

- **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.

NATIONAL GOVERNORS ASSOCIATION

National Governors Association
444 N. Capitol Street NW, Suite 267
Washington, DC 20001
202-624-5300 | www.nga.org