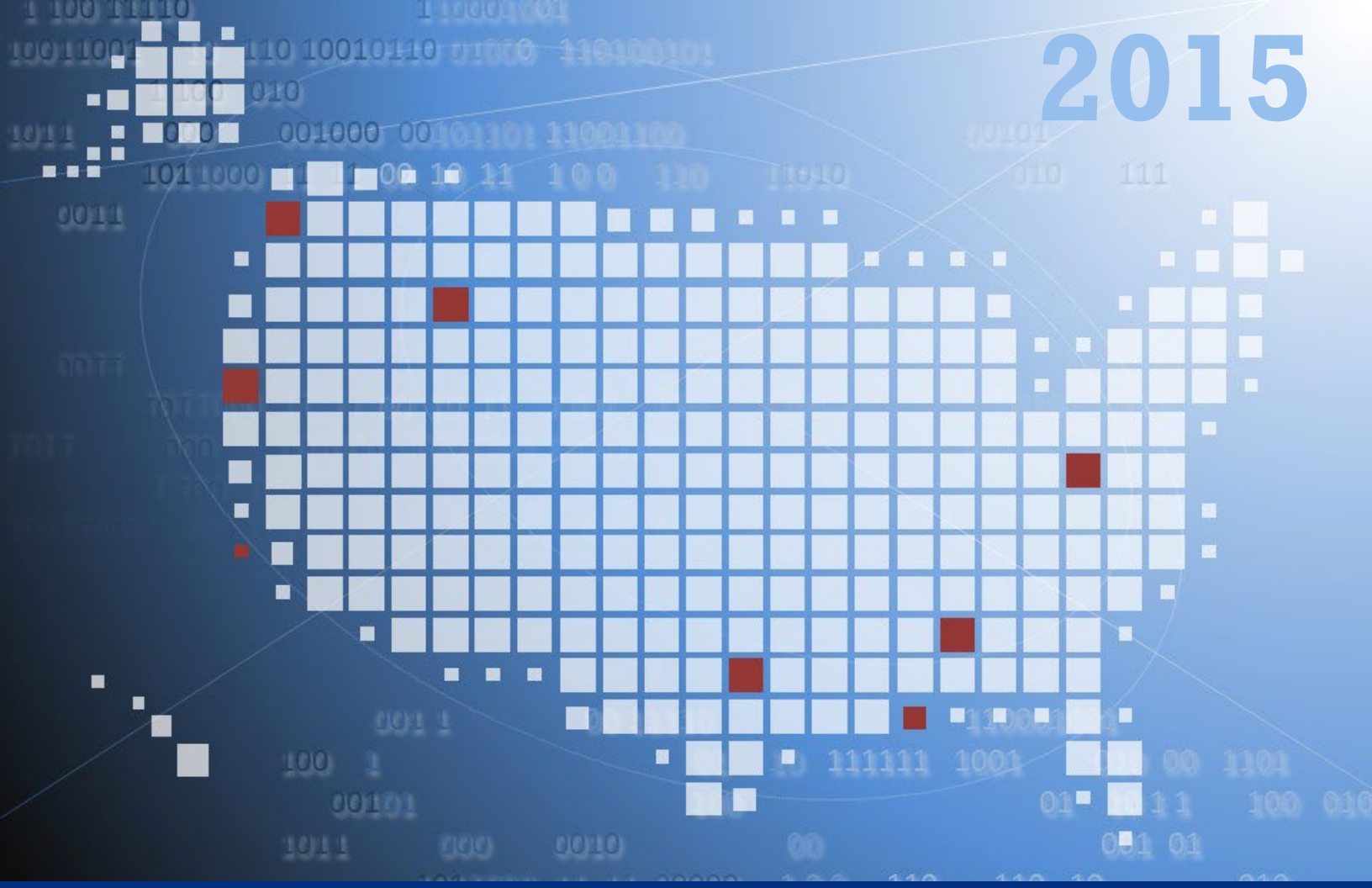


National Preparedness Report

March 30, 2015

Homeland Security

2015 *National Preparedness Report*

EXECUTIVE SUMMARY

This report marks the fourth *National Preparedness Report*. Required annually by *Presidential Policy Directive 8: National Preparedness*, the *National Preparedness Report* summarizes progress in building, sustaining, and delivering the 31 core capabilities described in the *National Preparedness Goal* (the Goal). Each year, the report presents an opportunity to assess gains that whole community partners—including all levels of government, private and nonprofit sectors, faith-based organizations, communities, and individuals—have made in preparedness, and to identify where challenges remain. The 2015 *National Preparedness Report* focuses primarily on preparedness activities undertaken or reported during 2014.

The intent of the *National Preparedness Report* is to provide the Nation with practical insights on preparedness that can inform decisions about program priorities, resource allocations, and community actions. The 2015 *National Preparedness Report* places particular emphasis on highlighting preparedness progress in implementing the National Planning Frameworks (the Frameworks) across the Prevention, Protection, Mitigation, Response, and Recovery mission areas. The Frameworks describe how the whole community works together to achieve the goal of a secure and resilient Nation.

The 2015 *National Preparedness Report* identifies six key findings that outline overarching national trends, as well as additional findings for each of the five preparedness mission areas included in the Goal.

Topic	Overarching Finding
Additional Capabilities to Sustain	Environmental Response/Health and Safety, Intelligence and Information Sharing, and Operational Coordination are additional core capabilities to sustain, which are capabilities in which the Nation has developed acceptable levels of performance for critical tasks, but which face potential performance declines if not maintained and updated to address new challenges.
National Areas for Improvement	Cybersecurity, Housing, Infrastructure Systems, and Long-term Vulnerability Reduction remain national areas for improvement, and Economic Recovery re-emerged as an area for improvement from the 2012 and 2013 *National Preparedness Reports*. Access Control and Identity Verification is a newly identified national area for improvement.
Response Coordination Challenges for Events that Do Not Receive *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act) Declarations	Recent events, including the epidemic of Ebola virus disease, have highlighted challenges with coordinating the response to and recovery from complex incidents that do not receive Stafford Act declarations.
Incorporating Emergency Preparedness into Technology Platforms	Businesses and public-private partnerships are increasingly incorporating emergency preparedness into technology platforms, such as Internet and social media tools and services.
Challenges Assessing the Status of Corrective Actions	While Federal departments and agencies individually assess progress for corrective actions identified during national-level exercises and real-world incidents, challenges remain to comprehensively assess corrective actions with broad implications across the Federal Government.
Self-assessment Results from States and Territories	Perspectives from states and territories on their current levels of preparedness were similar to previous years. All 10 core capabilities with the highest self-assessment results in 2012 and 2013 remained in the top-10 for 2014; Cybersecurity continues to be the lowest-rated core capability in state and territory self-assessments.

Table of Contents

Introduction

The *National Preparedness Report* summarizes progress in building, sustaining, and delivering the core capabilities outlined in the 2011 *National Preparedness Goal* (the Goal). Fulfilling an annual reporting requirement established by *Presidential Policy Directive 8: National Preparedness*, the 2015 *National Preparedness Report* focuses on progress achieved or reported in 2014. The report presents a national perspective, highlighting the contributions to preparedness made by the whole community—namely, Federal, state, local, tribal, and territorial governments, the private and nonprofit sectors, faith-based organizations, communities, and individuals.

Methodology

The Federal Emergency Management Agency (FEMA) coordinates the development of the *National Preparedness Report* with whole community partners. The approach for this year's report included the following activities:

- Researching open-source materials for information on notable progress and challenges related to the 31 core capabilities identified in the Goal;
- Soliciting Federal departments and agencies through a data call to identify their latest accomplishments toward national preparedness;
- Engaging Federal departments and agencies and senior interagency coordination groups to shape and enhance the report's content and validate key findings;
- Analyzing Threat and Hazard Identification and Risk Assessment and State Preparedness Report submissions from states and territories;
- Applying criteria—including assessments, exercises, funding, and long-term trends influencing preparedness—to identify national areas for improvement and capabilities to sustain among the 31 core capabilities; and
- Collaborating with stakeholders to review, comment on, and refine the report.

State Preparedness Report

The 2015 *National Preparedness Report* includes results from an integrated self-assessment process that states, territories, urban areas, and tribes completed in 2014. Through this process, states, territories, urban areas, and tribes conducted Threat and Hazard Identification and Risk Assessments to better understand risks and estimate capability requirements. States and territories then assessed their ability to meet those capability requirements through the State Preparedness Report. These self-assessment results reflect extensive whole community involvement across all 56 states and territories. State and territory homeland security and emergency management personnel led multi-disciplinary, statewide efforts that engaged representatives from law enforcement; fire service agencies; public health and medical systems, including emergency medical services, hospitals, and healthcare organizations; and nongovernmental organizations.

The 2015 *National Preparedness Report* reflects inputs from more than 143 stakeholders (including 14 non-Federal organizations) and more than 450 data sources.

Sources

FEMA compiled the *National Preparedness Report* using a combination of Federal and state input, qualitative and quantitative open-source research, and contributions from the whole community.

By the Numbers

97	129	450+	56
Federal Data Call Submissions	Federal Offices Engaged	Data Sources Referenced	State Preparedness Report Submissions

Additional Whole Community Engagement Included:

- American Red Cross
- Heritage Preservation
- National Academy of Sciences
- National Voluntary Organizations Active in Disasters
- Robert Wood Johnson Foundation
- Other private-sector partners

Report Organization

The 2015 *National Preparedness Report* begins with a Year in Review section that highlights examples of events from 2014 that tested the Nation's preparedness. Next, an Overarching Findings section highlights six key findings focused on national-level trends.

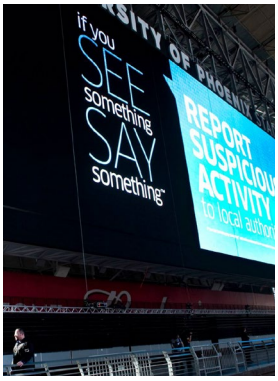
This year, the *National Preparedness Report* emphasizes progress in implementing the National Planning Frameworks (the Frameworks), which describe how the whole community works together to achieve the Goal. Specifically, the Frameworks outline critical tasks for the five preparedness mission areas and their associated core capabilities. Page 3 lists the core capabilities aligned to each mission area. Unlike previous years, the three core capabilities common to all five mission areas—Planning, Operational Coordination, and Public Information and Warning—are not discussed separately in the report but, instead, are integrated within each mission area.

While previous *National Preparedness Reports* have organized key findings by core capability, the 2015 *National Preparedness Report* uses the critical tasks identified in the Frameworks to develop key findings for each of the five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery. This approach provides greater flexibility to address crosscutting issues and progress arising within and across the mission areas. In total, the 2015 report identifies 43 key findings across the five mission areas. As relevant, the key findings include maps, charts, and case studies to enhance insights on preparedness progress and challenges. Additionally, call-out boxes titled "Mission Area Connections" under each mission area illustrate how activities occurring in one mission area link to other mission areas.

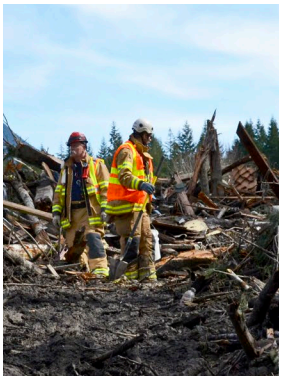
Each mission area section of the report begins with a brief overview describing Framework critical tasks and core capabilities in the context of real-world events, as well as state perspectives on preparedness. In addition, the overviews highlight examples of measurable achievements in current programs and initiatives, resilience innovations, and best practices from the whole community.

Mission Areas and Core Capabilities

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public Information and Warning				
Operational Coordination				
Intelligence and Information Sharing		Community Resilience	Infrastructure Systems	
Interdiction and Disruption		Long-term Vulnerability Reduction	Critical Transportation	Economic Recovery
Screening, Search, and Detection		Risk and Disaster Resilience Assessment	Environmental Response/Health and Safety	Health and Social Services
Forensics and Attribution	Access Control and Identity Verification	Threats and Hazard Identification	Fatality Management Services	Housing
	Cybersecurity		Mass Care Services	Natural and Cultural Resources
	Physical Protective Measures		Mass Search and Rescue Operations	
	Risk Management for Protection Programs and Activities		On-scene Security and Protection	
	Supply Chain Integrity and Security		Operational Communications	
			Public and Private Services and Resources	
			Public Health and Medical Services	
			Situational Assessment	








2014 Year in Review

In 2014, there were 45 major disaster declarations, 17 fewer than in 2013. However, as the examples below demonstrate, the Nation faces a range of threats and hazards each year that confirm the need to continuously enhance preparedness and promote security and resilience across the whole community.

January 9–20 A chemical spill into the Elk River in Charleston, West Virginia, resulted in a "do not use" order for residents of nine counties, affecting 300,000 people. For some residents, the order remained in place for more than a week. At the request of West Virginia officials, FEMA delivered more than 3 million liters of water to the region. In addition, a Laboratory Response Network laboratory tested 581 drinking water samples and provided Public Health Emergency Preparedness-funded epidemiology support from the U.S. Department of Health and Human Services' (HHS's) Centers for Disease Control and Prevention (CDC).

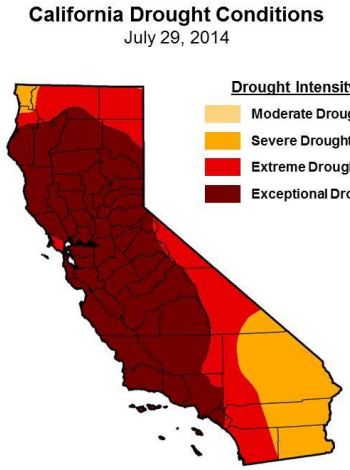


Figure 1. During the week of July 29, 2014, 100 percent of California experienced "Severe" to "Exceptional" drought conditions.

January–September With California under dry conditions since 2012, and 2014 projected as the driest year on record, the Governor of California declared a state of emergency and directed state officials to prepare for drought conditions. In July, the U.S. Drought Monitor reported that approximately 58 percent of the state was experiencing an "Exceptional Drought," the most severe drought level (see Figure 1). To increase California's resilience to water shortages, the Governor signed legislation in September strengthening local management and monitoring of key groundwater basins to ensure a sustainable water supply.

January 28–29, February 11–13 A winter storm struck northern and central Georgia from January 28–29, trapping motorists on highways and stranding approximately 2,000 students in their schools or on buses overnight in the Atlanta metropolitan area. A second, more powerful winter storm brought heavy snow and a record level of ice to northern and central Georgia February 11–13, causing over 700,000 customers to lose power and resulting in an emergency declaration (February 11) and a major disaster declaration (March 6) from the President.

February 22, April 30 Growth in U.S. oil production is increasing use of rail and barge shipments to transport crude oil to refineries. On February 22, more than 31,000 gallons of crude oil coming from the Bakken region of North Dakota spilled into the Mississippi River when a tank barge carrying the oil collided with a tugboat 154 miles north of the river's mouth, closing the waterway for several days. This and other recent accidents—including one on April 30 in Lynchburg, Virginia, that released crude oil into the James River—have highlighted potential environmental and public safety risks.

March 22 Heavy rain throughout February and March contributed to a mudslide that killed 43 people in Snohomish County, Washington. The mudslide covered a 360-yard section of highway with up to 20 feet of mud and debris and destroyed several homes. Searchers screened approximately 200,000 cubic yards of material, recovering the last victim in July. FEMA provided more than $16 million in disaster assistance, and the U.S. Small Business Administration (SBA) and U.S. Department of Agriculture (USDA) made additional Federal financial assistance available.

March 25—Present The 2014 Ebola virus disease epidemic is the largest in history, affecting multiple countries in West Africa. On March 25, CDC provided an initial announcement about an outbreak of Ebola virus disease in the West African country of Guinea. In September, a man traveling from Liberia to Texas became the first domestic laboratory-confirmed case of Ebola virus disease in the United States. CDC and U.S. Customs and Border Protection (CBP) enhanced screening procedures for travelers entering the United States from Guinea, Sierra Leone, and Liberia. Additional details on U.S. efforts with the Ebola virus disease are located on pages 29 and 54.

April 2 An active shooter at Fort Hood in Killeen, Texas, killed three people and wounded 16 others before killing himself. Eight minutes passed between the first 9-1-1 calls and confirmation that the shooter was neutralized. By April 4, 10 of the 16 wounded returned to duty. Over 150 law enforcement officials representing Federal, state, and local agencies participated in a Joint Task Force led by U.S. Army Criminal Investigation Command to investigate the incident. This incident was one of at least 13 active shooter events in 2014.

April 7 A cybersecurity industry report identified a vulnerability in OpenSSL (known as "Heartbleed") that could be exploited to expose sensitive data. In response, the U.S. Department of Homeland Security's (DHS's) U.S. Computer Emergency Readiness Team issued an alert to the public to share actionable information and ways to mitigate Heartbleed's effects. Moreover, DHS's Industrial Control System-Cyber Emergency Response Team contacted vendors and owners to determine potential vulnerabilities to essential computer systems.

April 27—May 6 Severe weather and tornados struck the central and southern United States, resulting in 34 fatalities. Between April 29 and May 6, the President issued major disaster declarations for Alabama, Arkansas, Florida, and Mississippi. In addition to FEMA disaster assistance, the Internal Revenue Service designated survivors in disaster-affected counties as potentially eligible for tax relief based on the President's disaster declaration and FEMA damage assessments. Moreover, the National Mobile Disaster Hospital deployed to Louisville, Mississippi, to temporarily replace a hospital that was heavily damaged by a tornado.

May 13–22 A series of wildfires in San Diego County, California, burned more than 26,000 acres and damaged or destroyed 119 buildings. Due to agreements put in place by the California Department of Forestry and Fire Prevention, 30 U.S. Navy and Marine Corps helicopters deployed to help combat fires across the county. These wildfires provided an opportunity for the San Diego County Operational Area Emergency Operations Center to test infrastructure improvements made after the 2003 and 2007 wildfires, including implementation of WebEOC®, an online incident management system.

June 2–October In response to a significant increase in the number of unaccompanied children crossing the U.S.-Mexico border, the President directed the establishment of an interagency Unified Coordination Group, consisting of representatives from FEMA, CBP, U.S. Immigration and Customs Enforcement, HHS's Assistant Secretary for Preparedness and Response (ASPR), HHS's Administration for Children and Families (ACF), U.S. Department of Defense (DoD), and other supporting agencies. The rise in apprehensions and processing of unaccompanied children in the Rio Grande Valley region presented unique challenges for DHS and HHS. In fiscal year 2014, CBP referred more than 57,000 children to the care and custody of the Office of Refugee Resettlement within ACF.

July 29 A rupture in a Los Angeles, California, water main resulted in over 20 million gallons of fresh water flooding sections of the University of California, Los Angeles campus. The failure of the water main—portions of which were installed in 1921—highlights the consequences of aging infrastructure systems.

August 24 Napa and Solano Counties in California experienced a 6.0-magnitude earthquake—the strongest Bay Area earthquake on record in 25 years. Test users of the U.S. Geological Survey (USGS) earthquake early warning system, ShakeAlert, in Berkeley, California, received alerts five seconds before shaking arrived from the earthquake. On September 11, the President issued a major disaster declaration for Napa and Solano Counties. FEMA has provided nearly $9 million in disaster assistance, and SBA has provided more than $10 million in low-interest Federal disaster loans to help residents and business owners recover.

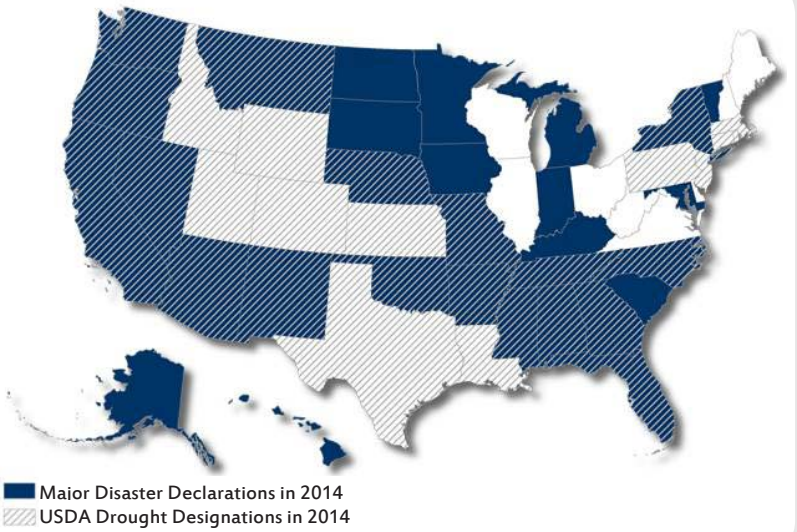
August–December The United States experienced a nationwide outbreak of enterovirus D68 (EV-D68), which results in severe respiratory illness. From mid-August to January 15, 2015, CDC and state public health laboratories had confirmed a total of 1,153 people in 49 states and the District of Columbia with respiratory issues caused by EV-D68. Laboratories also found EV-D68 in samples from 14 patients who died. The HHS National Syndromic Surveillance Program provided support in monitoring and responding to this outbreak.

November 24–December Sony Pictures Entertainment was the victim of a cyber attack that destroyed systems, stole large quantities of personal data and proprietary information, and disrupted business operations. Based on evidence gathered and intelligence sources, the Federal Bureau of Investigation (FBI) concluded that the government of North Korea sponsored the attack. In response to this cyber vandalism, the U.S. Department of the Treasury instituted new economic sanctions against three North Korean entities and 10 individuals. The scale and objectives of this attack demonstrate the challenges that cyber threats pose to social, economic, and national security.

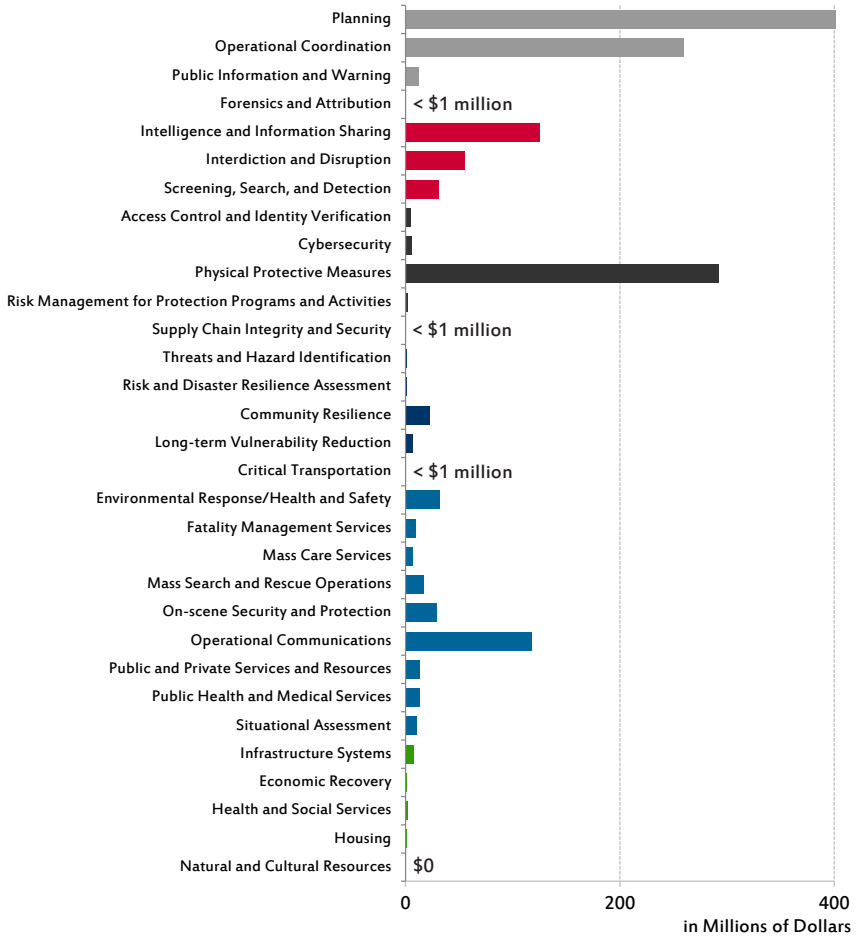
Supporting State, Local, Tribal, and Territorial Governments

In 2014, Federal agencies assisted in 45 major disaster declarations across 32 states and territories.

In fiscal year 2014, FEMA training programs achieved more than 2.1 million course completions across all 31 core capabilities.



Distribution of FEMA Preparedness (Non-Disaster) Grants
Fiscal Year 2013



In fiscal year 2014, FEMA and HHS provided more than $1.5 billion and $900 million, respectively, in preparedness grants.

Appendix A: Grant Case Studies provides additional examples of how FEMA preparedness grants have supported capability development at state and local levels.

Multi-year Progress Highlights

This report marks the fourth *National Preparedness Report*. Table 1 lists examples of key preparedness improvements taking place in the five mission areas over the past four years.

Preparedness Improvements 2011 to 2014	Prevention	Protection	Mitigation	Response	Recovery
Developing the **National Planning Frameworks, Federal Interagency Operational Plans**, and associated guidance to unify whole community preparedness planning	✓	✓	✓	✓	✓
Increasing the portion of the U.S. population covered by the **Integrated Public Alert and Warning System**, an integrated set of capabilities that enable authorities to alert and warn their communities	✓	✓	✓	✓	✓
Incorporating **social media and other technological innovations** to increase public awareness and communication	✓	✓	✓	✓	✓
Achieving full operational status for the **Next Generation Identification program**, which expands the use and accuracy of biometrics	✓				
Increasing the number of **fusion centers that meet designated standards** for gathering/receiving, analyzing, and sharing threat-related information across all levels of government, as determined through an annual assessment process	✓				
Expanding **training and support to enhance capabilities for chemical, biological, radiological, nuclear, and explosive threats**, and establishing the DoD CBRN [Chemical, Biological, Radiological, Nuclear] Response Enterprise, which provides personnel capable of supporting and conducting operations in chemical, biological, radiological, and nuclear environments	✓			✓	
Securing **vulnerable nuclear and radiological materials** around the world	✓				
Improving **abilities to detect and address infectious disease and chemical, biological, nuclear, and radiological threats**, and ensuring availability of medical countermeasures		✓		✓	
Increasing the whole community's **awareness of cybersecurity risks** and the availability of **cybersecurity training** opportunities and resources		✓			
Increasing the number of **critical infrastructure assessments by Federal programs**, which have aided critical infrastructure owners and operators in identifying and closing security gaps		✓			
Expanding efforts to plan for and adapt to hazards posed by **climate change**			✓		✓
Strengthening **links between Mitigation and Recovery** mission areas by tying resilient building practices to funding for post-disaster recovery			✓		✓
Applying the ***National Disaster Recovery Framework*** in real-world incidents, including the 2012–2013 drought and Hurricane Sandy					✓
Improving management and coordination of Federal assistance to support recovery, including innovative mechanisms such as the **National Drought Resilience Partnership and the Sandy Program Management Office**					✓

Table 1. Over the past four years, preparedness progress has occurred in all mission areas.

Overarching Findings

Environmental Response/Health and Safety, Intelligence and Information Sharing, and Operational Coordination are additional capabilities to sustain.

"Capabilities to sustain" are core capabilities in which the Nation has developed acceptable levels of performance for critical tasks, but which face potential performance declines if not maintained and updated to address new challenges. The 2015 *National Preparedness Report* identified three additional core capabilities—Environmental Response/Health and Safety, Intelligence and Information Sharing, and Operational Coordination—as capabilities to sustain.

Selection criteria for identifying capabilities to sustain included preparedness assessments; future trends and drivers influencing preparedness; and other preparedness indicators, such as exercise results and grant funding. No core capabilities in the Mitigation or Recovery mission areas have emerged as capabilities to sustain. All capabilities to sustain identified in the current and previous *National Preparedness Reports* are common core capabilities or fall under the Prevention, Protection, and Response mission areas.

Core Capabilities to Sustain

National Preparedness Reports **have identified eight core capabilities to sustain:**

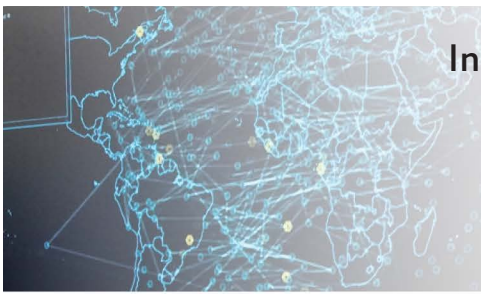
- **Environmental Response/Health and Safety**
- **Intelligence and Information Sharing**
- **Interdiction and Disruption**
- **On-scene Security and Protection**
- **Operational Communications**
- **Operational Coordination**
- **Public and Private Services and Resources**
- **Public Health and Medical Services**

Core capabilities to sustain have yet to emerge from the Mitigation or Recovery mission areas.

Additional Core Capabilities to Sustain

Environmental Response/Health and Safety

A diverse set of Federal, state, and local assets exists to address both routine and large-scale hazardous material and chemical, biological, radiological, nuclear, and explosive incidents. For example, Environmental Protection Agency (EPA) and U.S. Coast Guard (USCG) personnel respond to thousands of hazardous materials spills annually.



Intelligence and Information Sharing

States and territories rated Intelligence and Information Sharing among the top-10 core capabilities in their 2014 State Preparedness Report submissions. Progress in developing fusion center capabilities and an emphasis on addressing Intelligence and Information Sharing in exercises have helped support increases in state and territory self-assessment ratings over the past three years.

Operational Coordination

As highlighted in the 2012 *National Preparedness Report*, the National Incident Management System has become the nationwide standard for incident management. For the second consecutive year, states and territories assessed Operational Coordination as the highest-rated core capability.

A broad range of factors presents challenges to capabilities identified in 2014 and 2015 as capabilities to sustain. For example, decreasing state and local budgets have forced jurisdictions to prioritize preparedness efforts and rethink approaches to achieving preparedness results. Other factors, such as violent extremism and climate change impacts, may also place new or increased demands on capabilities. In other cases, results from exercises and state and territorial assessments have identified challenges in executing and sustaining core capabilities.

Cybersecurity, Housing, Infrastructure Systems, and Long-term Vulnerability Reduction remained national areas for improvement, and Economic Recovery re-emerged as an area for improvement from 2012 and 2013. Access Control and Identity Verification is a newly identified national area for improvement.

Each year, the *National Preparedness Report* identifies core capabilities as national areas for improvement based on consistent criteria, such as national findings on preparedness, indicators of exercise frequency and performance, funding support, State Preparedness Report results, and long-term trends influencing preparedness. The 2015 *National Preparedness Report* identified Cybersecurity, Housing, Infrastructure Systems, Long-term Vulnerability Reduction, Economic Recovery, and Access Control and Identity Verification as areas for improvement. Several of these core capabilities have experienced persistent challenges over time. Cybersecurity, Housing, and Infrastructure Systems have been areas for improvement for four consecutive years, and structural barriers hinder their successful execution. For the third time in four years, Economic Recovery also re-emerged as an area for improvement.

Areas for Improvement

Cybersecurity

The number of reported cyber incidents in the United States each year is increasing, and the Nation faces persistent challenges with a widespread, growing, and ever-changing threat of cyber attacks and an insufficient number of cybersecurity professionals. State and territorial perspectives from the 2014 State Preparedness Report reflect these challenges. Self-assessed ratings of Cybersecurity proficiency decreased overall, despite nearly 90 percent of states and territories identifying Cybersecurity as a high priority.

Housing

Coordination structures continue to mature as Federal agencies formalize operational guidance on how to implement the Housing capability under the *National Disaster Recovery Framework*. However, Housing lacks sufficiently trained Federal personnel to assist in large-scale incidents. In addition, states and territories have insufficient training options that address housing processes and programs. Additional challenges continue to impede progress, including: coordination of transitions in authority from response to long-term recovery; funding variability caused by supplemental disaster appropriations; timing of available housing options; and limited state resources to execute disaster-housing operations.

Infrastructure Systems

The Nation continues to apply lessons learned from Hurricane Sandy to improve coordination of large-scale infrastructure investments following a natural disaster. However, cost is a consideration in investment decisions, and limited public resources exist to bolster infrastructure systems. In many cases, the cost of improvements may be prohibitively expensive without broad stakeholder investment.

Long-term Vulnerability Reduction

The Nation is already experiencing the effects of climate change, such as rising sea levels, drought, and severe weather. The President's *Climate Action Plan* has prompted activities to improve resilience, including efforts to update and implement climate adaptation plans and encourage green infrastructure. However, many efforts are in early stages of maturity. Twenty percent of states and territories identified Long-term Vulnerability Reduction as most in danger of future decline, second only to Cybersecurity among all core capabilities.

Economic Recovery

States and territories reported the second-lowest self-assessment ratings for Economic Recovery in 2014 State Preparedness Report submissions. When compared to results from the 2013 State Preparedness Report, Economic Recovery experienced a four-percent decline in ratings at the top-two rating categories, the third-largest decrease among all 31 core capabilities. The National Level Exercise in 2014 revealed training and experience deficiencies among Federal staff needed to support Recovery Support Functions.

Access Control and Identity Verification

In 2014, new metrics revealed a slower rate of progress in adopting personal identity verification cards across Federal agencies. Self-assessments by states and territories also placed Access Control and Identity Verification in the bottom quarter of all capabilities, with approximately two-thirds of states and territories continuing to face challenges, both in controlling cyber access to systems and in controlling physical access to facilities.

Recent events, including the epidemic of Ebola virus disease, have highlighted challenges with coordinating the response to and recovery from complex incidents that do not receive *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act) declarations.

The National Planning Frameworks describe scalable, flexible, and adaptable coordinating structures that are essential for the whole community to work effectively together in delivering the core capabilities. In responding to and recovering from incidents, however, the whole community historically has perceived these national-level coordination structures—such as the Emergency Support Functions identified in the *National Response*

Framework—as only available during Stafford Act declarations. Despite being "always on," challenges remain in the process for their use in non-Stafford Act events. The Recovery Support Functions face the same challenge under the *National Disaster Recovery Framework*.

In recent years, several events that have not resulted in a Stafford Act declaration have required extensive Federal interagency coordination in support of state and local response efforts. These complex events have taken place over extended periods of time and often across large geographic areas, with uncertainty surrounding the role of existing coordination structures and authorities for multi-agency activity for non-Stafford Act events. Examples include:

- **2014 Epidemic of Ebola Virus Disease**: CDC made an initial announcement about the West Africa epidemic of Ebola virus disease in March 2014, and the first diagnosed case on U.S. soil occurred in September. The ongoing response to the epidemic has involved numerous Federal agencies, as well as states, private-sector companies, and other nations, with efforts occurring domestically and overseas.
- **2014 Increase in Arrivals of Unaccompanied Children**: The number of unaccompanied children crossing the U.S.-Mexico border increased in 2014. What began as a border security issue for CBP grew to an unprecedented humanitarian issue, as more than 57,000 children (over 30,000 more than the previous year) arrived in need of food, water, shelter, and social and medical services. While an issue in 2014, large annual increases in the number of unaccompanied children occurred the previous two years, as well.
- **2012 and 2013 National Drought**: This historic drought developed over many months, beginning in 2010 and covering 65 percent of the continental United States at its peak in 2012. The drought was the first disaster to use the *National Disaster Recovery Framework* without a Stafford Act declaration.
- **2010 Deepwater Horizon Oil Spill**: The response to the *Deepwater Horizon* oil spill fell under USCG's existing authorities. However, the scope and scale of the response to this oil spill—the largest in U.S. history—raised a number of issues, including monitoring immediate and long-term behavioral and public health, testing seafood, and addressing social and economic effects.

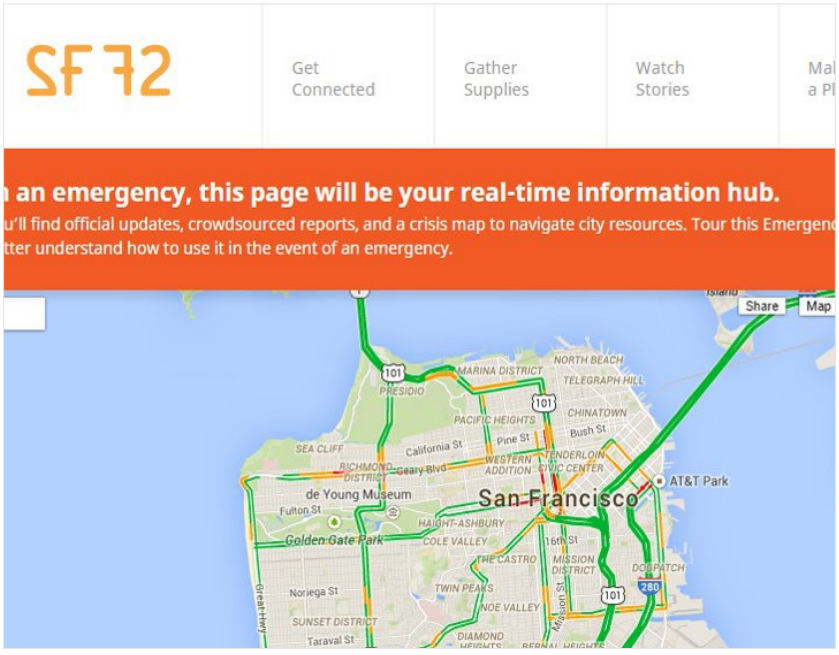
In 2014, the epidemic of Ebola virus disease and the increase in arrivals of unaccompanied children underscored the continuing need to improve understanding about how to rapidly identify when multi-agency collaboration across multiple levels of government is necessary and how to coordinate effectively. Although neither event received a Stafford Act declaration, both events resulted in a complex response taking place over several months. Moreover, unlike responses to Stafford Act events, in which FEMA manages multi-agency coordination, responses to these two events originated under the existing authorities of specific agencies. In both cases, the President acted to facilitate multi-agency coordination, establishing an Ebola Response Coordinator for the epidemic of Ebola virus disease and directing the DHS Secretary to establish a Unified Coordination Group for the increase in arrivals of unaccompanied children. These two events highlight the challenges of placing agencies unaccustomed to coordinating multiple agencies unexpectedly into that role, without previously exercising their responsibilities and capabilities. Moreover, these challenges are exacerbated as events increase in size, scope, and complexity. Greater clarity would enhance interagency decisions regarding when and how to use national-level coordination structures for non-Stafford Act events, as well as the role of existing authorities for non-Stafford Act events to support the use of these structures.

Businesses and public-private partnerships are increasingly incorporating emergency preparedness into technology platforms, such as Internet and social media tools and services.

Major incidents have demonstrated how technology can empower survivors, first responders, and government officials with critical information and resources. For example, during the 2014 Atlanta winter storm, an Atlanta resident created a Facebook page, SnowedOutAtlanta, that enabled volunteers to find and offer assistance to stranded motorists and individuals needing food, shelter, or transportation. Within one day, the page had more than 50,000 members.

In July 2014, the White House hosted "Innovation for Disaster Response and Recovery Demo Day"—as part of a broader White House Innovation for Disaster Response and Recovery Initiative launched in 2013—to identify challenges in disaster preparedness and disaster response and recovery efforts, as well as to showcase innovative technological solutions from businesses, nonprofit organizations, government agencies, and other groups. Several demonstrations highlighted the potential for businesses to use their existing tools to support emergency preparedness, including new avenues to obtain services in disaster-affected areas, provide preparedness and public warning information, and collect and analyze information from the public. Examples include the following:

- Airbnb, an online service for users to list and book accommodations, can activate a no-cost version of its service during disasters that allows nearby hosts to offer shelter to displaced individuals. In 2014, Airbnb partnered with San Francisco, California, and Portland, Oregon, to enhance this disaster service by pre-identifying hosts who have committed to housing displaced individuals and increasing their preparedness through training and educational materials.
- The City72 toolkit builds on the SF72 web-based platform created by the San Francisco Department of Emergency Management to connect community members and promote resilience. The SF72 platform takes advantage of everyday digital and neighborhood networks to promote preparedness, and the new toolkit allows other communities to develop similar websites, and provides information on how to create localized content and promote their site.



- Facebook's "Safety Check," released in 2014, builds on Facebook's social media platform and allows users in disaster-affected areas to notify friends and family that they are safe, as well as check on others.
- A partnership between Dataminr and Twitter allows Dataminr software to analyze social media posts (i.e., "tweets") to identify potential threats to public safety and disseminate real-time, map-based alerts. In 2014, Dataminr confirmed a gas explosion in New York City in less than four minutes and supported the City of Boston during the 2014 marathon by monitoring for potential threats.

Each of these tools and services reflects the benefits of applying private-sector technological expertise to emergency preparedness challenges, and several have fostered cooperation between and among public and private entities. In December 2014, the Federal Government launched the disasters.data.gov website, which provides a portal to access tools and innovations, as well as disaster-relevant datasets, to empower the whole community and increase preparedness.

While Federal departments and agencies individually assess progress for corrective actions identified during national-level exercises and real-world incidents, challenges remain to comprehensively assess corrective actions with broad implications across the Federal Government.

Exercises and real-world incidents teach lessons and provide best practices that can help improve preparedness for future events. Federal agencies use after-action reports and performance assessments to identify corrective actions that will help resolve gaps or shortcomings experienced during exercises and disasters.

Large-scale exercises and incidents have revealed high-priority issues that span multiple Federal agencies and require extended resources and time commitments to address. For example, the 2014 National Level Exercise identified challenges with communications and information flow among participating agencies, hindering development of a shared common operating picture.

In 2014, the U.S. Government Accountability Office (GAO) found that while Federal agencies individually monitor their corrective actions from national-level exercises, the Federal Government lacks mechanisms for comprehensively assessing the status of and outcomes from these actions. Federal agencies maintain multiple systems and processes to track corrective actions progress, with limited interoperability between systems. The lack of a timely, comprehensive mechanism for assessing implementation of corrective actions across the Federal Government makes it difficult to address persistent, complex preparedness challenges.

For exercises, FEMA's National Exercise Program serves as the principal mechanism for examining national preparedness and measuring readiness across the entire homeland security enterprise by coordinating, designing, and delivering a progressive cycle of exercises. FEMA requests regular status updates from Federal departments and agencies on the status of corrective actions from all national-level exercises. Currently, no Federal department or agency has the authority to require other agencies to implement corrective actions resulting from lessons learned during exercises or real-world incidents.

Sandy Program Management Office

The most systematic tracking of recommended actions from a real-world incident emerged from the *Hurricane Sandy Rebuilding Strategy*. A Program Management Office monitored implementation progress for 69 policy recommendations across 13 Federal agencies. The office also facilitated five quarterly meetings with senior Federal leaders to ensure continued Federal agency commitment to implementing the recommendations. In November 2014, the Program Management Office's responsibility for tracking and reporting progress on outstanding Hurricane Sandy funding and policy recommendations transferred to FEMA's Office of Federal Disaster Coordination from the U.S. Department of Housing and Urban Development (HUD).

Perspectives from states and territories on their current levels of preparedness were similar to previous years. All 10 core capabilities with the highest self-assessment results in 2012 and 2013 remained in the top-10 for 2014; Cybersecurity continues to be the lowest-rated core capability in state and territory self-assessments.

Through State Preparedness Report submissions, states and territories provide core capability self-assessments based on the unique preparedness targets they establish in their Threat and Hazard Identification and Risk Assessments. Figure 2

shows results of State Preparedness Report submissions from 2014, which used a 5-point scale (with 5 as the highest rating) to assess each capability in terms of planning, organization, equipment, training, and exercises. While rankings shifted slightly, the top-10 core capabilities remained unchanged from 2012 and 2013. Nine of these top-10 capabilities are common capabilities or from the Response mission area. Operational Coordination again received the highest self-assessment ratings, with 65 percent of responses falling into the top-two rating categories (i.e., a 4 or 5). Cybersecurity was the lowest-rated among all core capabilities for a fourth consecutive year.

The self-assessment ratings also continue to reflect state and territory priorities. In addition to rating themselves on a 5-point scale, states and territories assign each capability a high, medium, or low level of priority. Among the 10 core capabilities most frequently identified as high priority, eight were among the capabilities with the ten-highest self-assessment ratings. The two exceptions were Cybersecurity and Infrastructure Systems, which remain among the bottom half of core capabilities, despite more than three-quarters of states and territories identifying them as high priority.

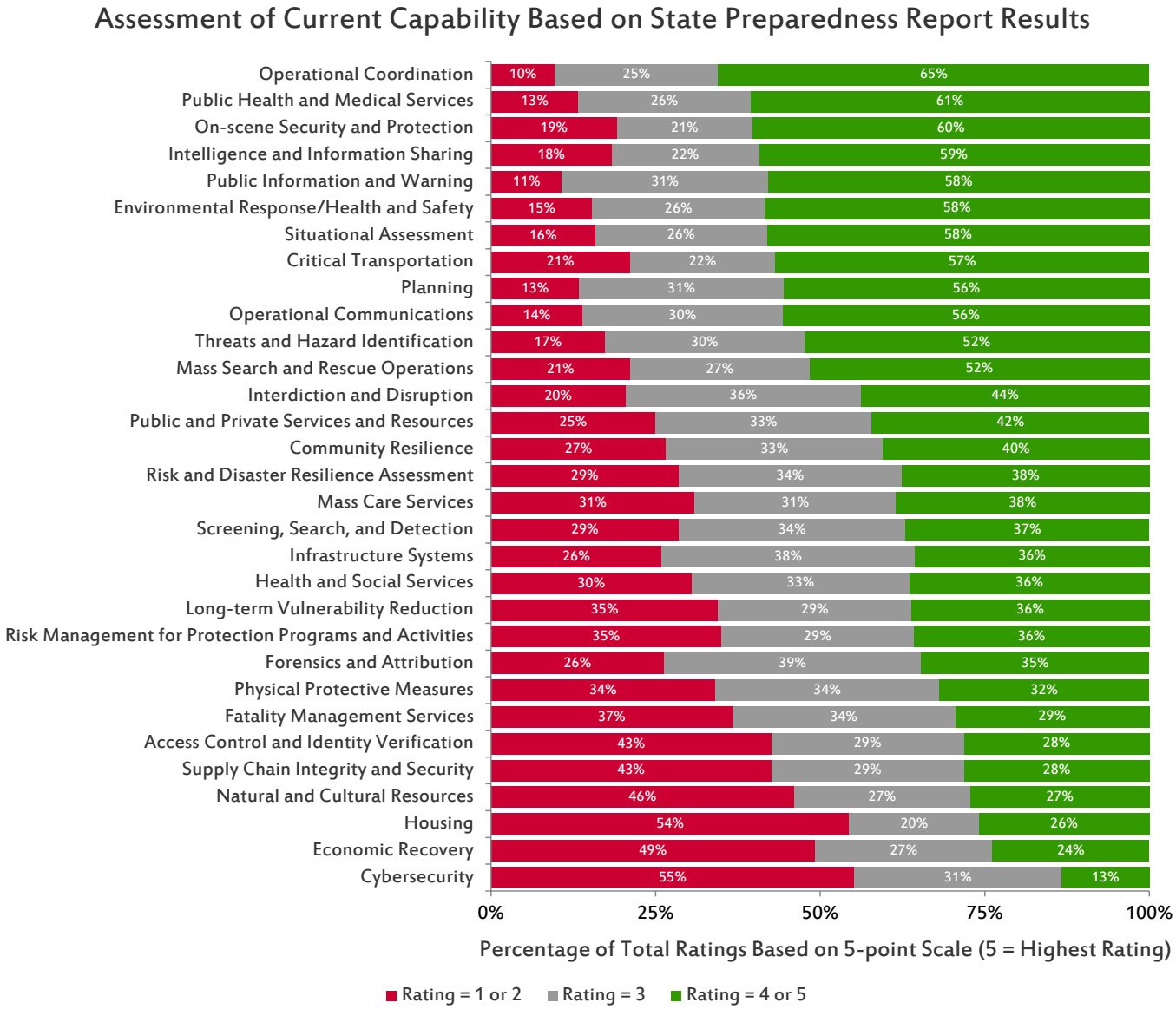


Figure 2. Results from 2014 State Preparedness Report submissions were similar to the previous year, with Operational Coordination and Cybersecurity once again receiving the highest and lowest self-assessment ratings, respectively, from 56 states and territories. *[Note: Due to rounding, some percentages may total slightly more or slightly less than 100 percent.]*

The 2014 State Preparedness Report revealed mixed progress in core capability ratings relative to the 2013 State Preparedness Report. Gains occurred in 17 out of the 31 core capabilities, with the largest gains in Threats and Hazard Identification and in Public and Private Services and Resources. In contrast, Physical Protective Measures and Forensics and Attribution reflected the largest decreases. Nine out of the 10 highest-rated capabilities in 2013 experienced positive gains. For capability gaps, states and territories shared their views on expected responsibilities for addressing those gaps in the long term (see Figure 3). Similar to 2013, states and territories believe that the Federal Government should play a larger long-term role in filling gaps for capabilities such as Fatality Management Services and Housing.

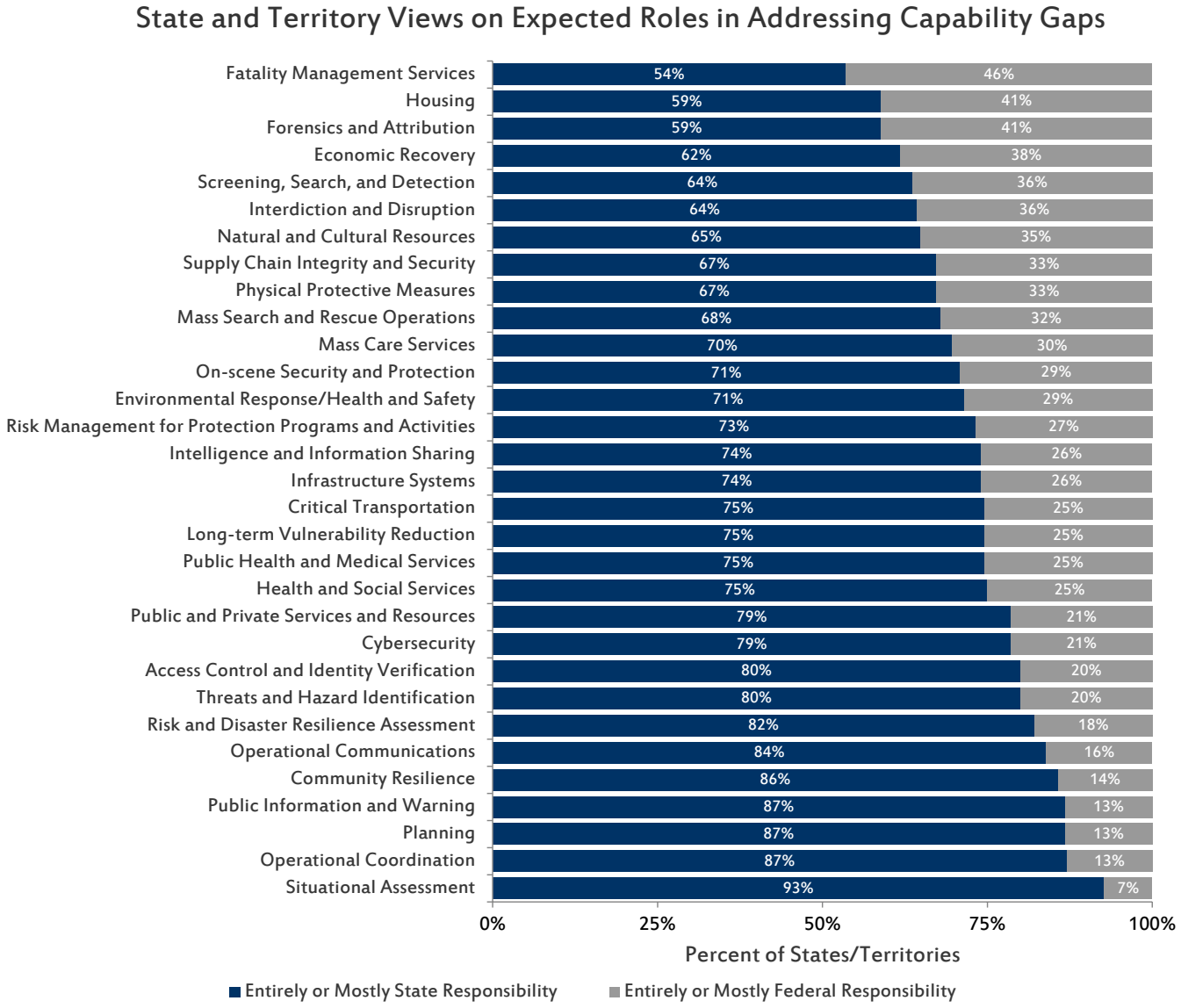
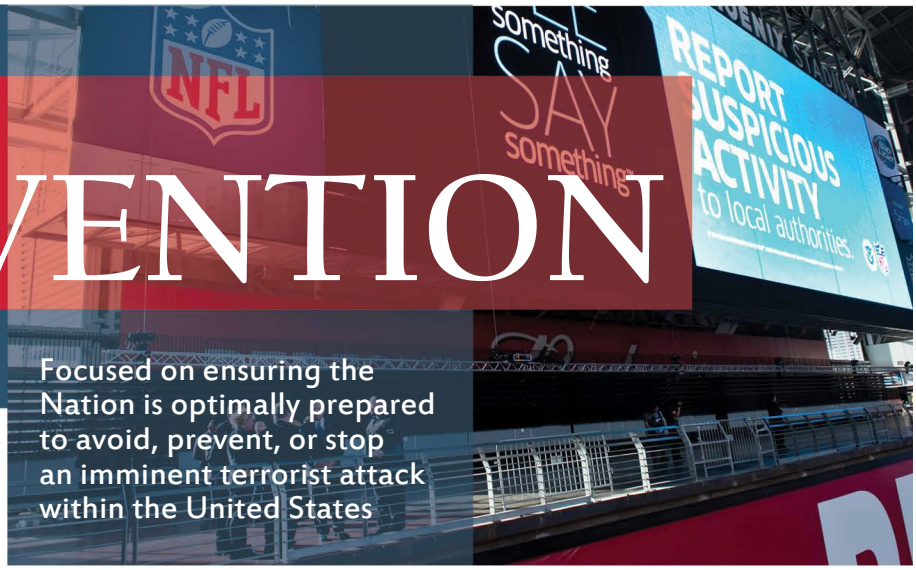


Figure 3. For each of the 31 core capabilities, a majority of states and territories believe that responsibility for addressing most, if not all, of the remaining gaps lies with the state or territory.

In their 2014 State Preparedness Report submissions, states and territories also reflected on progress during the past year and future concerns. More than one-third identified Planning (43 percent) and Operational Coordination (34 percent) as among the three core capabilities that made the most progress in the past year. Looking ahead, states and territories most frequently identified Cybersecurity as the capability in greatest danger of future decline. At 38 percent, Cybersecurity received nearly twice as many selections as the next most frequently selected capabilities, Long-term Vulnerability Reduction and Infrastructure Systems (both at 20 percent).

Mission Area Overview

Prevention



Focused on ensuring the Nation is optimally prepared to avoid, prevent, or stop an imminent terrorist attack within the United States

Highlights

- New policies increase accountability for intelligence collection and information-sharing activities across the Federal Government. (p. 20)
- State, local, tribal, and territorial governments are using Federal training and assistance programs to enhance their chemical, biological, radiological, nuclear, and explosive prevention capabilities. (p. 22)
- The law enforcement community faces new considerations in using financial tracking to detect criminal and terrorist networks, due to the increasing popularity of virtual currencies. (p. 23)

Frameworks in Action

The *National Prevention Framework* (the Prevention Framework) describes the capabilities and associated whole community roles, responsibilities, and coordination structures designed to prevent a threatened or actual act of terrorism against the United States. The Prevention Framework expands on the seven Prevention core capabilities in the Goal and identifies 53 critical tasks necessary for the successful execution of these capabilities. Moreover, three overarching principles guide these core capabilities and critical tasks: (1) engaged partnerships; (2) scalability, flexibility, and adaptability; and (3) readiness to act.

The Prevention Framework emphasizes that individuals and communities possess a strong understanding of the threats they face, and that they help prevent incidents by **sharing information with law enforcement**. To that end, the whole community is taking steps to advance partnerships among government agencies, the private sector, and the public. In 2014, for example, faith-based communities and individuals worked with law enforcement officials to report potential violent extremist activity, contributing to police **interdicting at least seven Americans before they traveled abroad to join the fighting in Syria, possibly with terrorist organizations**. Additionally, the public continued contributing information through the Nationwide Suspicious Activity Reporting Initiative and the "If You See Something, Say Something" campaign. The National Network of Fusion Centers receives these tips and shares them with the FBI. The fusion centers also vet, assess, and analyze the tips to identify and extract valuable intelligence information to further terrorism or other law enforcement investigations. In 2014, the fusion centers enhanced their accuracy in **analyzing intelligence to refine investigative leads**—238 out of the 4,326

Core Capabilities in the Prevention Mission Area

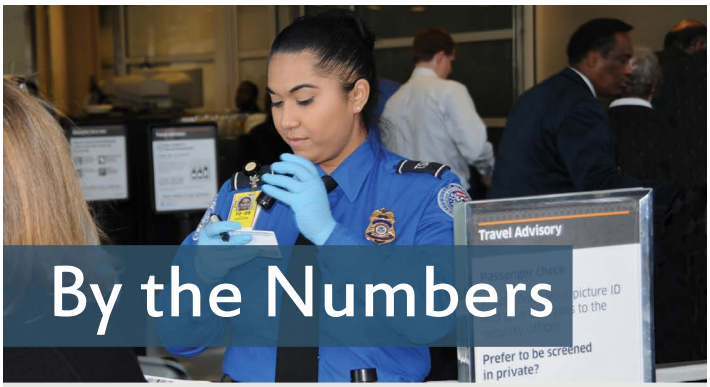
- Forensics and Attribution
- Intelligence and Information Sharing
- Interdiction and Disruption
- Operational Coordination
- Planning
- Public Information and Warning
- Screening, Search, and Detection

reports (5.5 percent) submitted to FBI aided an investigation or helped identify, locate, or interdict individuals on the Terrorist Screening Center watch list, up from 3.3 percent in 2013.

The Federal Government continued to **engage with the public and private sectors** using scalable and flexible technology platforms. For example, FBI's InfraGard platform—a public-private partnership established to prevent attacks on critical infrastructure—continues to grow, with over 80 chapters nationwide that include more than 350 of the Nation's Fortune 500 companies. As of December 2014, InfraGard includes 34,403 active members. Another platform, DHS's Homeland Security Information Network, disseminated over 950 situational awareness and current situation reports to 13,500 critical infrastructure partners during a 10-month span in 2014. Additionally, the Federal Government developed new products to support the private sector. For example, the Transportation Security Administration's (TSA's) SMARToolbox provides the transportation industry with a self-assessment tool to analyze security measures already in place, and a corresponding database of measures that can be taken to improve security.

Private-sector organizations also continued sharing surveillance video camera feeds with local police in 2014, enhancing law enforcement's ability **to locate and identify people associated with imminent terrorist threats**. In 2014, at least 22 cities began voluntary programs to share private video feeds with local police to enhance situational awareness and assist with identifying terrorist suspects.

In 2014, the whole community also initiated new efforts to balance privacy with the sharing of security-related information. In September, several technology companies introduced privacy software that precludes any entity except the user from accessing data stored on mobile devices. These software updates allow users to protect their information if their device is lost or stolen, but the software also limits law enforcement's ability to **conduct digital forensic analysis on the devices**, even after obtaining a warrant. In reaction, FBI has called for a national conversation on the benefits and risks of these software updates.

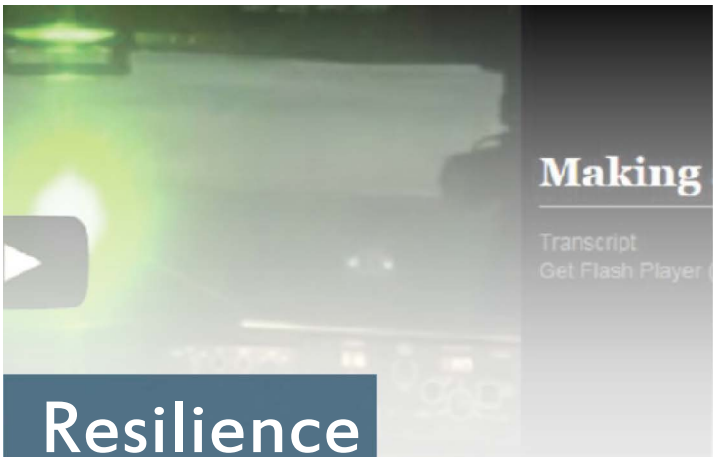


By the Numbers

3.48 petabytes of data
The U.S. Secret Service completed digital forensics examinations on 5,482 devices in fiscal year 2014, inspecting 3.48 petabytes of data, up from 1.25 petabytes in fiscal year 2013.

653 million airline passengers
In 2014, TSA screened over 653 million airline passengers, intercepting 2,212 firearms, as well as bomb-making supplies and hundreds of other weapons.

65 evaluations
In fiscal year 2014, the Domestic Nuclear Detection Office (DNDO) completed 65 comprehensive evaluations and demonstrations of new and improved technologies to prevent nuclear terrorism.



Resilience Innovations

- The Financial Services Information Sharing and Analysis Center and the Depository Trust & Clearing Corporation worked together to develop the first industry-driven platform to share cyber threat intelligence, released December 2014.
- DoD and the Federal Aviation Administration (FAA) released a video, and FBI initiated a pilot program in 12 field offices to raise awareness of the danger of aiming laser pointers at aircraft. Since the February launch, metropolitan areas in the pilot program reported a 19-percent decrease in the number of such incidents.

Whole Community Accomplishments

Ohio Ohio Homeland Security released the "Safer Ohio" phone application to engage the public in anti-terrorism and public safety efforts. The application's "See Something, Send Something" feature allows users to report suspicious activities to Ohio Homeland Security analysts.

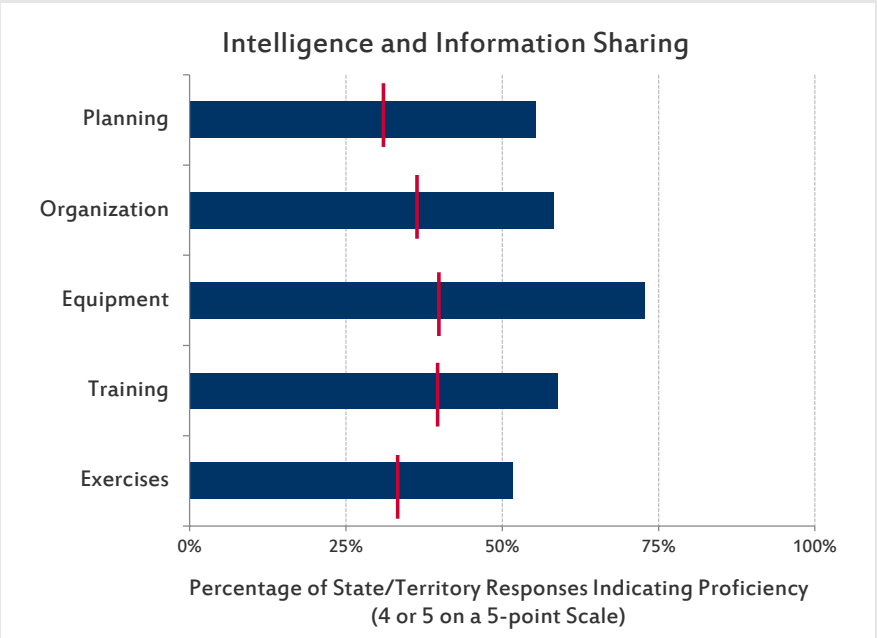
Muslim Public Affairs Council In March 2014, the Muslim Public Affairs Council launched their community-based Safe Spaces Initiative, a nationwide effort to identify individuals who may be susceptible to committing violent acts and positively intervene in their development. The initiative uses a three-tiered approach—prevention, intervention, and ejection—to help youth workers and community leaders offer a healthy outlet and prevent violence at the community level.

University of California, San Francisco, and Pacific Northwest National Laboratory
A group of researchers from the University of California, San Francisco, and the Pacific Northwest National Laboratory developed a new platform that can simultaneously detect 10 biothreat toxins, the largest number to be simultaneously detected to date, in a variety of environmental and clinical samples. In the event of a bioterrorist attack, this platform can decrease the time required to determine which agent was released, helping individuals to take the necessary measures to prevent people from becoming exposed and to deliver appropriate medical treatment.

State Perspectives on Preparedness

2014 State Preparedness Report Results

- Intelligence and Information Sharing was the highest self-assessed core capability in the Prevention mission area, with 59 percent of responses falling into the top-two rating categories (i.e., a 4 or 5).
- Compared to other Prevention mission area core capabilities, Intelligence and Information Sharing had superior ratings for planning, organization, equipment, training, and exercises.
- Intelligence and Information Sharing was the only Prevention capability ranked in the top-10 of all 31 core capabilities.



Notes: Vertical red lines (|) indicate the average rating for all other Prevention core capabilities in each respective category. The chart and statements do not include contributions from the three common core capabilities—Planning, Operational Coordination, and Public Information and Warning.

Prevention Mission Area

Key Findings

The Federal Government continued efforts to integrate the Nation's capabilities to address imminent weapons of mass destruction threats.

In May 2013, the President delivered remarks to the National Defense University in which he laid out his priorities and approach to counterterrorism. In response, FBI, in conjunction with the National Security Council, led an initiative involving 16 agencies and 50 components to map out the Nation's reaction to imminent weapons of mass destruction threats across Prevention, Protection, Mitigation, and Response mission areas. The mapping effort connected strategic- and tactical-level actions to resolve imminent threats, save lives, and protect critical infrastructure. More broadly, it highlighted the need for strong coordination to address interdependencies among all levels of government and across mission areas, leading to the creation of two interagency operational teams in fiscal year 2014—the Weapons of Mass Destruction Strategic Group and its Crisis Consequence Management Unit. The Weapons of Mass Destruction Strategic Group brings together interagency subject-matter experts and FBI leadership to produce classified and unclassified threat information products tailored to the needs of state, local, tribal, and territorial law enforcement. The FEMA-led Crisis Consequence Management Unit organizes real-time terrorist threat information from the protection, mitigation, and response communities. These efforts also align with a recommendation from a 2014 Inspector General's report on the Boston Marathon bombings that FBI share threat information with state and local partners more proactively and uniformly.

The Federal Government has developed policies to increase accountability for intelligence collection and information-sharing activities.

The Federal Government took several steps in 2014 to strengthen its oversight of intelligence activities, affecting the mechanisms for sharing classified and unclassified information. In late 2013, the Federal Government partnered with an independent group of subject-matter experts to review existing signals intelligence programs, which gather information by intercepting electronic signals from communications systems, weapons systems, or radar. Using the review group's recommendations, the President announced a series of reforms to increase transparency of intelligence collection and information sharing in January 2014. These reforms included creating a Civil Liberties and Privacy Office within the National Security Agency and initiating a White House review of privacy and big data. The big data report, released in May 2014, recommended expanding privacy protections and promoting privacy-enhancing technologies.

In January 2014, the White House also issued *Presidential Policy Directive 28: Signals Intelligence Activities*, which represents the first-ever unclassified, public document to outline the Federal Government's standards for collecting signals intelligence. The Directive limits government collection of bulk signals intelligence, outlines principles for safeguarding personal information, and requires relevant departments and agencies to annually review intelligence requirements and advise on the necessity of maintaining classified intelligence programs.

Fusion centers strengthened their processes for categorizing data and sharing intelligence in accordance with standards and through common systems.

State and major urban area fusion centers serve as focal points for the gathering and receipt, analysis, and sharing of threat-related information across all levels of government. In 2014, the National Network of Fusion Centers made progress in several key areas:

- **Standardized analytic processes:** The number of fusion centers that tagged their analytic products according to established topics of interest (i.e., Homeland Security Standing Information Needs) increased from 19 percent in 2013 to 69 percent in 2014. Tagging products provides a basis for tracking the number of products and the extent to which they meet customer needs. Tagged documents also facilitate searches for information between Federal, state, and local partners and the Intelligence Community. Additionally, the percentage of fusion centers that did not tag any documents decreased from 41 percent in 2013 to 4 percent in 2014.
- **Requests for information:** Fusion centers responded to over 4,300 requests (65 percent) for information from the FBI Terrorist Screening Center, up slightly from 64 percent in 2013. Fusion centers varied in the timeliness of their responses, ranging from two hours to more than a day.
- **Information-sharing portals:** DHS's Homeland Security Information Network Intelligence Community of Interest is the most commonly used sensitive-but-unclassified system for information sharing and analytic collaboration among fusion centers and Federal partners. Forty-four percent of fusion centers used the Homeland Security Information Network Intelligence Community of Interest as their primary system for sharing information among fusion centers and Federal partners. Moreover, 82 percent of fusion centers posted all distributable products to that portal, up from 46 percent in 2013; of the remainder, 10 fusion centers posted products on their own Community of Interest rather than to the portal, and five reported a need for additional training on using the portal.

Despite progress, the National Network of Fusion Centers is still striving to meet goals for tagging 100 percent of analytical products to Homeland Security Standing Information Needs, responding to 100 percent of FBI Terrorist Screening Center information requests, and posting 100 percent of distributable analytic products to relevant information-sharing portals. Key fusion center customers—including state police, state investigative agencies, homeland security advisors, state emergency management directors, major city police chiefs, county sheriffs, and FBI field offices—reported a decrease of 5.6 percent in the relevancy of fusion center products and an increase of 15.1 percent in their timeliness to support mission needs.

Federal training and assistance programs are helping state, local, tribal, and territorial governments to enhance their chemical, biological, radiological, nuclear, and explosive prevention capabilities.

DNDO's Securing the Cities initiative continued establishing local capabilities to detect and report dangerous radiological and nuclear materials within high-risk metropolitan areas. In September 2014, DNDO expanded the program to its third urban area, the National Capital Region. The first Securing the Cities urban area, New York City, demonstrated a regional ability to detect and interdict radiological and nuclear threats. As a result, the program's focus at this location shifted to sustaining capabilities in 2014. DNDO has provided more than 5,800 pieces of detection equipment, trained nearly 11,000 personnel, and conducted more than 100 drills in the New Jersey-New York-Pennsylvania tri-state area. As of December 2014, the Securing the Cities program had covered 23 million people. When fully implemented, it will include 10 high-risk areas, covering nearly 100 million people and 42 percent of the Nation's critical infrastructure.

In fiscal year 2014, through Securing the Cities and other programs, the Federal Government continued training state, local, tribal, and territorial partners in chemical, biological, radiological, nuclear, and explosive materials detection and planning:

- FBI's Hazardous Devices School, the Nation's authority for accrediting bomb squads, updated the *National Guidelines for Bomb Technicians* in March 2014 and trained approximately 1,500 state, local, tribal, and territorial partners.
- FBI field offices offered 40 National Improvised Explosives Familiarization workshops to provide field demonstrations of bomb and chemical threats, training 314 bomb technicians and 1,029 law enforcement personnel and first responders.
- FBI's Counter-Improvised Explosives Device Section of the Critical Incident Response Group—a cadre of specialists who provide expertise in crisis negotiations, hostage rescue, hazardous device mitigation, and tactical operations—provided approximately 400 training opportunities for state and local bomb squads to enhance detection and investigation capabilities for attacks ranging from improvised explosives to weapons of mass destruction.
- The DHS Office of Bombing Prevention held 13 planning workshops on improvised explosive security, training 626 people to identify and close planning gaps related to explosives.
- DNDO and the DHS Office of Bombing Prevention trained more than 9,925 public- and private-sector partners through more than 240 courses to prevent chemical, biological, radiological, nuclear, and explosive incidents.
- The Center for Domestic Preparedness—DHS's only federally chartered weapons of mass destruction training center—trained more than 52,000 state, local, tribal, and territorial first responders in 2014.

Additionally, the Federal Government supported state and local governments to prevent chemical, biological, radiological, nuclear, and explosive threats at special events. DNDO maintains mobile deployable units to provide training and enhanced radiological and nuclear detection capability at large events, such as the Super Bowl or the President's State of the Union Address. In fiscal year 2014, these units deployed to 70 events, up from 54 in fiscal year 2013, providing 20 to 40 personnel with detection equipment at each event. The DHS Office of Infrastructure Protection assisted in planning,

exercises, conducting security assessments, and developing geospatial situational awareness products for 17 events. The USCG provided bridge and ferry security for the 2014 New York City marathon. In 2014, National Guard Joint Forces Headquarters–State organizations deployed Weapons of Mass Destruction-Civil Support Teams to nearly 2,400 missions (including stand-by mission support).

The increasing popularity of virtual currencies means that Federal agencies face new considerations in executing their law enforcement and national security responsibilities.

The Federal Government investigates the financing of terrorism to help identify, arrest, and prosecute terrorists and their supporters. The U.S. Department of Justice (DOJ) investigates and prosecutes cases of terrorism financing, which occurs through charitable organizations, corporations, criminal activity, and other means. Virtual currencies—digital representations of value that can be traded and exchanged for goods and services—present new challenges to law enforcement and counterterrorism officials because they are more difficult to track. As of March 2014, GAO estimated that Bitcoin, the most popular virtual currency in circulation, was worth a total of over $5.6 billion. While virtual currencies can provide lower transaction costs and facilitate global commerce, law enforcement agencies have indicated that virtual currencies also present new opportunities for terrorists to conceal their actions when purchasing weapons, selling illegal drugs, or laundering funds.

Criminals are already using virtual currencies to conceal their illegal activities. When law enforcement disrupted two of the world's largest online black markets, Silk Road and Silk Road 2, they seized over $150 million worth of virtual currencies that had been used to exchange drugs, weapons, and services. Additionally, U.S. Secret Service cyber investigations led to the 2014 arrest and dismantling of Liberty Reserve, a centralized digital currency service with over 5 million users that laundered and distributed an estimated $6 billion in proceeds from criminal activity. Law enforcement officials have also arrested individuals using virtual currencies to plot attacks, including a San Francisco, California, man arrested for buying bomb-making materials from an online black market.

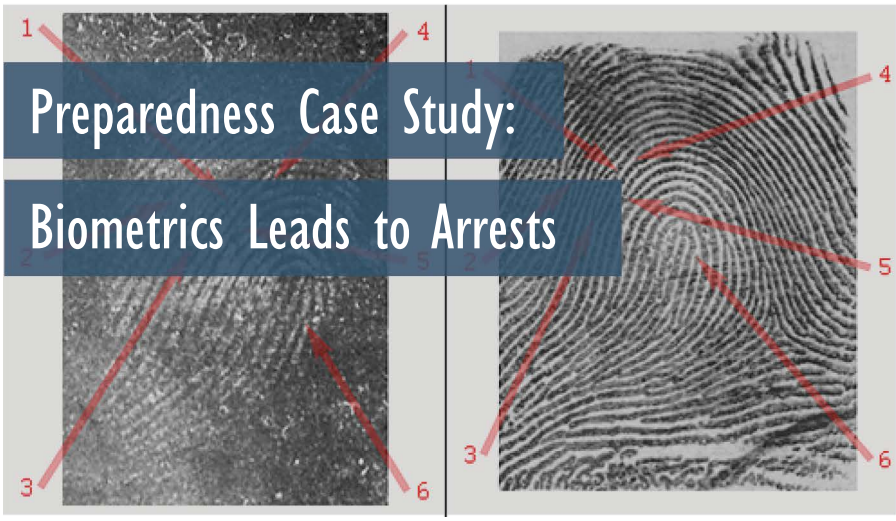
The U.S. Department of the Treasury is leading efforts in the Financial Action Task Force—the international body that sets standards for anti–money laundering and combating the financing of terrorism—to develop risk-based standards for virtual currencies.

In November 2014, FBI—in partnership with the U.S. Attorney's Office for the Southern District of New York, Europol's European Cybercrime Centre, and Eurojust—launched an operation to shut down over 400 Tor network addresses. Tor is a free anonymizing software that allows an estimated one million daily users to hide their identities online, sometimes obscuring illicit activity. The operation targeted Tor dark market websites selling illegal goods, such as drugs, firearms, stolen credit card information, fake passports, counterfeit currency, and computer-hacking services and tools, often in exchange for virtual currency. In addition to shutting down Tor websites, FBI and partners arrested 17 individuals and seized over $1.2 million worth of currencies and goods.

The Next Generation Identification program became fully operational nationwide in 2014, contributing to greater use and accuracy of biometrics across the Federal Government.

Law enforcement officers use biometric data—such as fingerprints, facial recognition, and iris scans—to identify and interdict malicious actors. To aid in such efforts, FBI initiated the Next Generation Identification biometric program in 2010, which replaced and expanded upon the capabilities of FBI's longstanding system. In September 2014, FBI announced that the new program was fully operational and available nationwide, including two new components called Rap Back and the Interstate Photo System. The Rap Back system notifies agencies that conduct background checks of subsequent criminal activity by individuals who undergo those checks; as of February 10, 2015, four states and several Federal agencies had been working toward participation in Rap Back. Using facial recognition software, the Interstate Photo System will aid investigations by allowing law enforcement officers to query more than 21 million images of criminals.

Meanwhile, other Federal biometric systems and previously established components of the Next Generation Identification program are improving. Fingerprint matches using the Next Generation Identification system are over 99-percent accurate, and hits on latent prints, which require powders or chemicals to visualize, were 81-percent accurate—up from 27-percent accuracy using the old fingerprint-identification system. Additionally, the average search time for queries from U.S. ports of entry to the biometric watch list maintained by the Office of Biometric Identity Management improved from 6.9 seconds in fiscal year 2013 to 6.5 seconds in fiscal year 2014. During fiscal year 2014, CBP had 264,580 hits in its biometric database, which the agency referred for additional screening at air, land, and sea ports of entry. Of those referrals, 4,045 cases had a traveler exclusion code in the system, such as an indicator that the traveler was being processed for expedited removal.



Police officers around the Nation are using biometric tools to assist law enforcement activities. In August 2014, FBI recognized a Massachusetts police officer for solving a 27-year-old murder case using biometric technology to examine fingerprints left at the scene. Similarly, FBI's Albuquerque Division used the Next Generation Identification facial recognition software to locate and arrest a fugitive who had been on the run for 14 years.

Nationwide demand for unmanned aircraft systems continues to rise, and state governments are passing regulations to limit law enforcement use of these systems.

Unmanned aircraft systems technology continues to improve rapidly, and can perform a variety of tasks with greater flexibility and at a lower cost than comparable manned aircraft. In the public sector, unmanned aircraft systems can help law enforcement agencies gather information during high-risk situations, such as hostage situations; investigate hazardous materials incidents (including incidents potentially involving explosive devices); or quickly document crime scenes. As of December 31, 2014, the FAA had issued 603 certificates of waiver or authorization for public-sector use of unmanned aircraft systems, up from 545 as of December 2013. Federal, state, and local law enforcement agencies received 292 of those certificates.

However, these systems present privacy concerns when outfitted with cameras or other monitoring devices. In February 2015, the White House issued a Presidential Memorandum on "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," which establishes principles that govern the Federal Government's use of unmanned aircraft systems and promotes responsible use of this technology in private and commercial sectors. In addition, 14 states have passed or enacted legislation requiring public-sector agencies to obtain a warrant to use unmanned aircraft systems to conduct surveillance for use in an investigation or trial. Two states have passed legislation that bans the use of the systems. As illustrated in Figure 4, in 2013, only seven states had passed legislation limiting public-sector use of unmanned aircraft systems, and one state had passed legislation banning it.

State Regulation for Law Enforcement Use of Unmanned Aircraft Systems

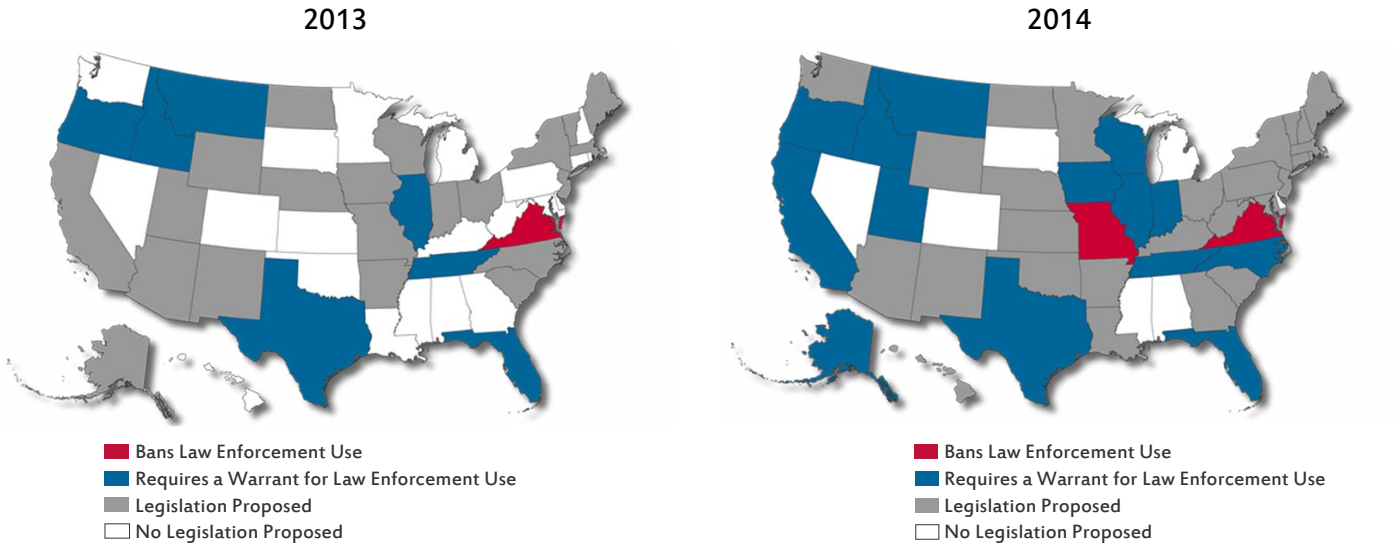


Figure 4. Several states passed or proposed regulation for unmanned aircraft systems in 2014.

Unmanned Aircraft Systems

Prevention	▪ Gather information during a terrorist standoff or hostage situation.
Protection	▪ Conduct surveillance for hazardous weather or border crossings. ▪ Inspect infrastructure, from oil rigs to dams and bridges, to ensure safety. ▪ Document crime scenes and fatal traffic accidents.
Response	▪ Use thermal scanners to detect hot spots in a wildfire to avoid firefighter injury. ▪ Reduce the need for first responders to enter dangerous environments to conduct search and rescue. ▪ Enable responders to more rapidly search large areas for missing persons.
Recovery	▪ Assist in conducting post-disaster damage assessments.

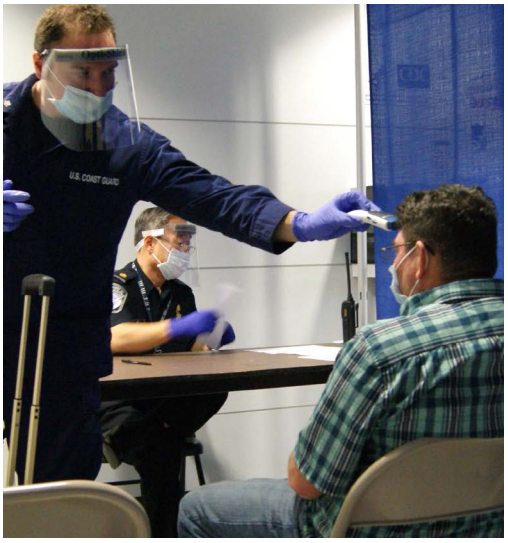
Mission Area Overview

Protection

Focused on actions to safeguard the Nation's people, critical assets, and networks against acts of terrorism and manmade or natural disasters in a manner that allows American interests, aspirations, and way of life to thrive

Highlights

- The West Africa epidemic of Ebola virus disease prompted enhanced health screening measures at airports and highlighted varying approaches to quarantine policies at state and local levels. (p. 29, 30)
- DoD and HHS are consolidating biosurveillance systems to streamline reporting procedures and increase efficiency. (p. 31)
- The Nation has intensified programs to combat violent extremism in response to threats within the United States and from Americans trained abroad. (p. 34)



Frameworks in Action

The *National Protection Framework* (the Protection Framework) provides guidance to the whole community by describing the 11 core capabilities necessary to protect the Nation against acts of terrorism, natural disasters, and other threats or hazards. The Protection Framework identifies 66 critical tasks for implementing Protection activities under three overarching principles: (1) a risk-informed culture; (2) resilience and scalability; and (3) shared responsibility.

Recent attacks highlight the importance of a **risk-informed culture** in protecting the Nation's energy infrastructure. In June 2014, an improvised explosive device ruptured a fuel tank at a power station in Nogales, Arizona. This followed a 2013 incident in which armed assailants opened fire on a substation's cooling systems in San Jose, California, knocking out power to 17 transformers. The Congressional Research Service reports that a coordinated attack on multiple high-voltage transformers could leave large regions without power for days or weeks.

In response to these incidents, the Federal Energy Regulatory Commission ordered the North American Reliability Corporation to develop new reliability standards that require grid owners to **conduct risk assessments and implement security measures** to protect against attacks. FBI also partnered with the U.S. Department of Energy (DOE) to ensure the capacity to **interdict persons associated with a potential threat** at facilities that use radiological material. In fiscal year 2014, this partnership supported security enhancements at 96 facilities, 14 courses that trained 396 personnel, and 6 tabletop exercises.

The 2014 epidemic of Ebola virus disease in West Africa also highlighted the Nation's ability to develop scalable capabilities for screening and

Core Capabilities in the Protection Mission Area

- Access Control and Identity Verification
- Cybersecurity
- Intelligence and Information Sharing
- Interdiction and Disruption
- Operational Coordination
- Physical Protective Measures
- Planning
- Public Information and Warning
- Risk Management for Protection Programs and Activities
- Screening, Search, and Detection
- Supply Chain Integrity and Security

detection. Prior to the epidemic, the CDC laboratory in Atlanta, Georgia, and DoD's U.S. Army Medical Research Institute of Infectious Diseases were the only U.S. laboratories capable of testing human specimens for clinical diagnosis of Ebola virus disease. By August 2014, 13 laboratories in the Laboratory Response Network qualified to test individuals for Ebola virus disease. As of February 25, 2015, 55 laboratories in 43 states are approved to test for Ebola using a DoD test authorized for emergency use by HHS's U.S. Food and Drug Administration (FDA). This increase, in addition to technological improvements, **broadened the capacity to identify and interdict persons who may be infected with the Ebola virus disease**, and decreased the turnaround time for Ebola virus disease test results from 24 hours to between 4 and 6 hours. This improved the ability of public health authorities and hospitals to **monitor and analyze public health threats** posed by the epidemic of Ebola virus disease.

Several cyber incidents in 2014 also illustrate how the Protection mission area relies on **shared responsibility** to coordinate capabilities across the whole community. In April 2014, private-sector cybersecurity engineers discovered a vulnerability in commonly used encryption software that exposed up to two-thirds of all web servers to exploitation by cyber criminals. The vulnerability, known as Heartbleed, enabled hackers to intercept and decrypt private information transmitted online. Once notified, the Federal Government promptly **shared cyber threat information** with the public using alerts that included actionable measures for reducing the risk. Moreover, DHS's National Coordinating Center for Communications provided situational awareness to partners in the communications sector to inform their protective measures. The same team worked with partners to deny access to networks, applications, and systems that could be exploited. On February 13, 2015, the President signed an Executive Order that promotes information sharing about cyber threats within the private sector and between the private sector and the Federal Government. The Executive Order encourages the formation of hubs to share information, and calls for a common set of standards to facilitate information sharing between Federal agencies and these hubs and improve access to classified cybersecurity threat information.

Federal agencies and private-sector partners also provided updated cyber risk assessments to help stakeholders in healthcare, financial services, and retail sectors assess the likelihood of cyber attacks and identify industry-wide capability gaps. For several years, HHS has sponsored briefings on cyber threats with the healthcare and public health sectors to encourage security. Moreover, the FBI issued a Private Industry Notification to healthcare providers in April 2014 warning of their increased risk for cyber attacks. During summer 2014, however, a cyber attack on one of the Nation's largest hospital operators exposed patient identification data for more than 4.5 million individuals. DHS's U.S. Computer Emergency Readiness Team worked with FBI and HHS to **implement countermeasures, share information on the threat, and secure networks from additional breaches of personal information**. In October, FDA hosted a workshop on "Collaborative Approaches to Medical Device and Healthcare Cybersecurity" to address the challenges of cybersecurity in the healthcare and public health sector.

By the Numbers

34 dam inspections and risk assessments — The U.S. Bureau of Reclamation conducted 34 dam inspections and risk assessments in fiscal year 2014 to determine potential means of failure and resulting consequences.

43 Maritime Security Plans — USCG updated and tested all 43 Maritime Security Plans in 2014. These plans help ports, vessels, and facilities coordinate information sharing and preparedness for transportation security incidents.

116 cyber exercises — In fiscal year 2014, the National Cyber Exercise and Planning Program conducted 116 cyber exercises that focused on building cybersecurity capabilities across the whole community.

Resilience Innovations

- USCG developed a Cyber Quick Response card, which provides guidance for quickly managing Federal agency coordination during a cyber attack.
- DHS developed the Cybersecurity Evaluation Tool to assist organizations in protecting key national cyber assets through a systematic and repeatable self-assessment.
- CDC introduced Red Sky, a web-based dashboard that provides CDC programs with a platform to inform leadership of emerging public health emergencies and uses a tiered system to show the severity of an event.

Whole Community Accomplishments

Hewlett Foundation The Hewlett Foundation launched the Cyber Initiative in April 2014, which pledged $20 million over the next five years to develop a network of experts who will identify Internet security best practices, help individuals and institutions comprehensively analyze cybersecurity problems and solutions, and fill critical research gaps.

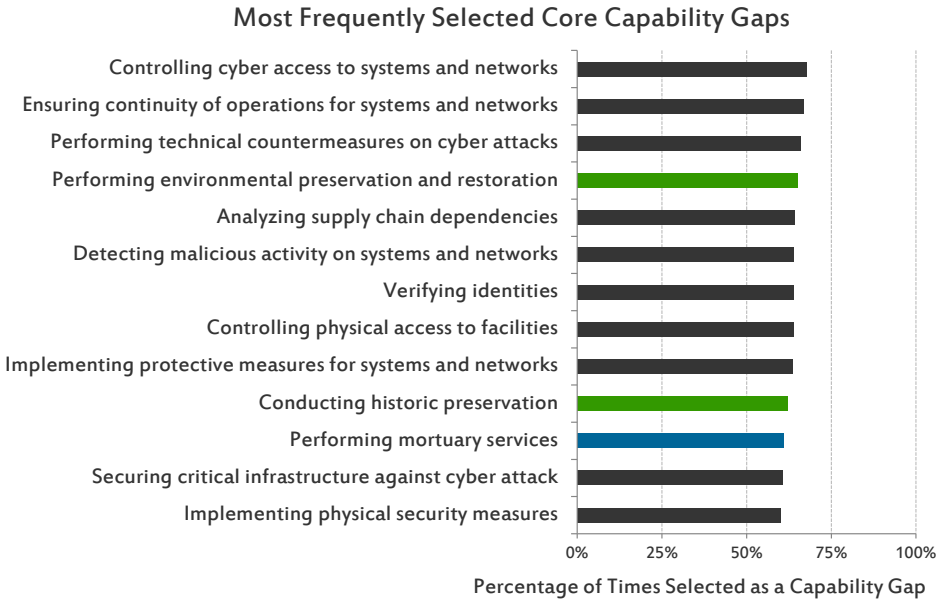
University of California, Berkeley In December 2014, the University of California, Berkeley—in partnership with prevention and environmental nongovernmental organizations—held a series of events to commemorate the 30th anniversary of the Union Carbide gas disaster in India and draw attention to chemical disaster risk in the United States. Events included educational presentations at local university medical centers and high schools, film screenings, community art exhibitions, staged performance art, and panel discussions.

University of Maryland In May 2014, researchers at the University of Maryland's Supply Chain Management Center created an online portal called CyberChain, which allows organizations to assess their cyber and supply chain risks, track developing threats, map their information technology supply chains, and anonymously measure themselves against industry peers and the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework and supply chain guidelines. Companies from aerospace manufacturing, telecommunication, real estate, medical, and professional services industries have used the portal to assess their resiliency and determine supply chain vulnerabilities.

State Perspectives on Preparedness

2014 State Preparedness Report Results

- Of over 200 specific core capability gaps listed in the State Preparedness Report survey tool, 13 gaps were selected in 60 percent or more of the responses. Capabilities in the Protection mission area accounted for 10 of these.
- Cybersecurity accounted for 6 of the 13 most frequently selected gaps, including the top-three selected gaps. Physical Protective Measures, Access Control and Identity Verification, and Supply Chain Integrity and Security accounted for four additional gaps.



Notes: The chart and statements do not include contributions from the three common core capabilities—Planning, Operational Coordination, and Public Information and Warning. The bar chart colors designate the mission areas to which gaps correspond (see page 3). The number of standardized gaps varied by core capability from 3 to 13.

Protection Mission Area

Key Findings

Based on previous interagency planning efforts, CBP and CDC adopted enhanced health screening measures for travelers who have been in countries experiencing widespread transmission of Ebola virus disease.

On October 11, 2014, CBP and CDC enhanced screening procedures at the five U.S. airports that received 94 percent of all inbound passengers from Guinea, Sierra Leone, and Liberia. On October 21, the DHS Secretary announced that all passengers arriving in the United States from those three countries were required to fly into those five airports. When health officials identified cases of Ebola virus disease in Mali, CBP and CDC implemented enhanced screening in mid-November for travelers arriving from that country, as well. CDC removed Mali from the list of nations subject to enhanced screening for Ebola virus disease in January 2015, after 42 days had passed (i.e., two incubation cycles for the Ebola virus disease) since the last patient with Ebola virus disease in Mali came into contact with a person not wearing personal protective equipment.

CBP's Office of Information Technology automated the CDC Health Questionnaire form, allowing CBP officers to complete and submit screening forms to CDC in real time via a computer or mobile device; as of December 31, CBP had screened 6,846 total passengers arriving from affected countries. CBP referred 430 (6 percent) of those travelers to CDC public health officers for additional evaluation; of those, 13 received further evaluation at medical facilities. Evaluations revealed that none had Ebola virus disease.

These domestic screening efforts complement the exit health screening processes that were put into place for travelers leaving Guinea, Sierra Leone, and Liberia. CDC provided technical assistance for these exit-screening programs, which were initiated in early August 2014 and expanded to Mali in late November. CDC has been training screeners and general airport staff in the affected countries to perform the screening procedures. This screening requires airport personnel or other relevant authorities in these four countries to administer questionnaires, visually assess travelers for symptoms, and take travelers' temperatures before permitting them to board a plane. Of the approximately 118,500 people who underwent exit screening as of December 31, 2014, 120 did not receive permission to board. The combination of domestic and foreign screening efforts enhances opportunities for early detection and containment of individuals with Ebola virus disease potentially entering the United States.

Preparedness Case Study:

Supply Chains for Personal Protective Equipment

In October 2014, CDC issued revised guidance for use of personal protective equipment when caring for patients with Ebola virus disease. The guidance created a surge in demand by U.S. hospitals for personal protective equipment and led to delays in filling some equipment orders. In response, manufacturers have increased production of personal protective equipment, and distributors are identifying ways to provide the requested quantities and meet the delivery timelines. HHS has been working with manufacturers to better understand the demand for and availability of products, as well as the actions taken to address any shortages in additional orders. CDC provided additional guidance that links the amount of personal protective equipment a hospital needs to its degree of potential involvement in identifying, isolating, evaluating, and treating patients with Ebola virus disease. Through these efforts, manufacturers expect to return to typical order-fulfillment times for many of their personal protective equipment product-lines by April 2015.

The epidemic of Ebola virus disease highlighted varying approaches to quarantine at state and local levels.

Differing quarantine policies for Ebola virus disease demonstrate the difficult balance between supporting medical workers who fight the disease on the front lines in Africa (as well as reducing unnecessary costs and restrictions) and minimizing risk to the public. Prior to the 2014 epidemic of Ebola virus disease, several state quarantine laws were between 35 and 100 years old, and they focused on a small number of specific diseases such as tuberculosis or typhoid fever. As of October 2014, eight states had specific statutes for quarantine and isolation of people suspected of having tuberculosis, but no state had statutes for any other specific diseases. At least eight state governors issued orders addressing quarantine protocols for Ebola virus disease in 2014.

In early August 2014, CDC released interim guidance for monitoring the movement of persons potentially exposed to Ebola virus disease. The CDC guidance uses a risk-based method to determine the level of quarantine or monitoring, based on an individual's exposure history and clinical state. For example, based on CDC guidance, an asymptomatic healthcare worker who had direct contact with an Ebola patient while wearing appropriate personal protective equipment should undergo direct active monitoring (i.e., a public health authority checks the individual for symptoms and fever each day through direct observation) and movement restrictions for 21 days after the last potential exposure.

At least 14 states decided to maintain or develop stricter policies than CDC's guidance (see Figure 5). These diverse approaches can create public confusion

about the necessary restrictions to protect the public and can lead to complications when a person with possible exposure to Ebola virus disease travels through different states. Two states with stricter policies—New York and New Jersey—ordered mandatory quarantine for all healthcare workers returning from affected regions of West Africa, requiring them to avoid interaction with others for 21 days. In contrast, Virginia's policy was more aligned with CDC guidance. The Commonwealth ordered active monitoring in-residence for asymptomatic healthcare workers, allowing them to interact with small groups of friends and family, but asking them to avoid large community gatherings. Between October and November 2014, 10 states were actively monitoring at least 854 people.

Another area of concern has been transporting a patient infected with Ebola virus disease from an assessment center to a U.S. treatment facility. Interstate transport of patients infected with Ebola virus disease is primarily handled by state and local public health authorities, with CDC providing support and guidance. Moreover, the U.S. Department of State helped coordinate international transport of U.S. citizens infected with Ebola virus disease in West Africa back to the United States.

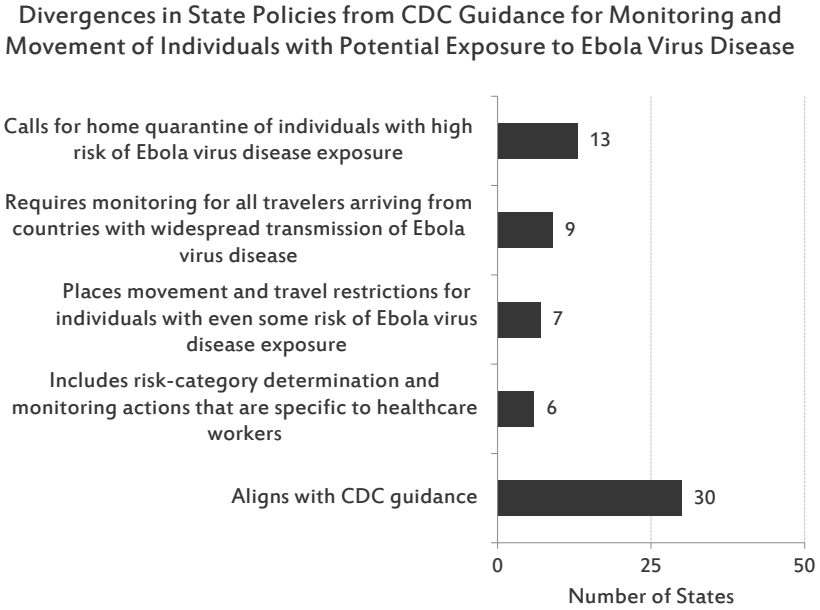


Figure 5. Several states have policies that diverge from CDC guidance for monitoring and movement of persons with potential exposure to Ebola virus disease.

HHS and DoD are consolidating biosurveillance networks and databases to streamline reporting procedures for state and local health systems, and to increase reporting efficiency.

As of early 2014, CDC operated, funded, or worked with more than 100 biosurveillance systems. Of those systems, nearly 65 monitor agents, conditions, or activities that could lead to a potential outbreak or other public health emergency. The large number of systems imposed duplicative requirements on state and local public health departments and complicated the process of reporting diseases and conditions to the proper surveillance systems. In 2014, 73 percent of states and territories reported one or more significant gaps in biosurveillance planning, organization, equipment, training, or exercises. CDC released the *Surveillance Strategy* in February 2014 to consolidate biosurveillance programs, eliminate redundancies, and reduce reporting burden.

The strategy highlights four initiatives that target existing biosurveillance activities—three of which include measurable performance targets to monitor progress. One of these initiatives calls for the acceleration of electronic laboratory reporting to public health agencies. This effort will improve surveillance of diseases and conditions by increasing the timeliness and accuracy of reporting to public health authorities. The performance target for this initiative is for 80 percent of laboratory reports to public health agencies to be received electronically by 2016. As of October 2014, 47 states electronically received lab reporting data, and 43 states electronically received syndromic surveillance data from hospitals and other clinical settings; this is up from 44 and 33 in 2012, respectively.

DoD uses 10 to 15 key biosurveillance systems and has been making efforts to combine these systems internally and with Federal partners. In May 2014, DoD moved forward on the development of the Global Biosurveillance Portal. The portal will provide unclassified global access to geo-located and time-stamped biosurveillance data to support environmental, health, force health protection, and medical planning. Additionally, DoD is working with HHS and DHS to ensure that they can

leverage DoD's new prototype Biosurveillance Ecosystem. This system provides automated surveillance on global data feeds for over 400 human infectious diseases and uses pilot-stage analytics and algorithms to provide early warning of disease patterns to inform decisions.

Preparedness Case Study:

International Health Regulations

The International Health Regulations (2005) is an international framework established to prevent, protect against, control, and respond to the international spread of disease, while avoiding unnecessary interference with international traffic and trade. As part of their International Health Regulations obligation, countries must notify the World Health Organization of all events that may constitute a potential public health emergency of international concern (according to criteria outlined in the regulations) and respond to public health risks that may spread internationally. In addition, the International Health Regulations contains requirements for sharing information during unexpected or unusual public health events. For example, the United States reported biosafety lapses in Federal laboratories in summer 2014. As a result, the White House urged Federal agencies working with infectious agents to take steps to enhance the safety and security of their research. This included an immediate review of more than 4,000 U.S. facilities—examining inventory and documentation for more than 40 million samples—to identify select biological agents and toxins; and ensure their proper registration, safe stewardship, and secure storage or disposal.

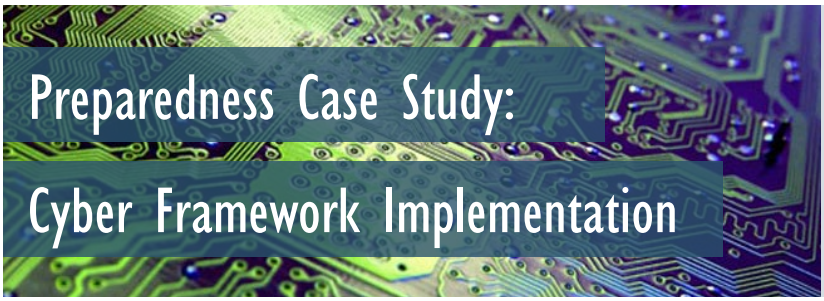
The 2014 *Framework for Improving Critical Infrastructure Cybersecurity* is guiding government and industry development of cybersecurity initiatives.

In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* to help organizations across the public and private sectors better manage cybersecurity risks. The framework provides a flexible set of cybersecurity standards and best practices, which allows stakeholders to adapt and adopt pieces of the framework as they see fit. NIST solicited feedback on the framework through targeted outreach, and stakeholders suggested that NIST publish "real-world" applications, lessons learned, and case studies to highlight examples of how organizations of varying sizes, types, and cybersecurity capabilities can use the framework to improve their security. Stakeholders also recommended sharing more extensive mappings of existing standards and guidelines to the framework. NIST will continue to explore options for hosting publicly available framework reference materials and will continue to hold workshops, webinars, and similar meetings on the framework to bring in additional stakeholders.

Some stakeholders also provided feedback regarding the lack of standardized measures available to assess implementation progress. The development and use of metrics is at the discretion of individual framework users, allowing them to tailor measures to the specific priorities of their organization. As the framework continues to mature, NIST will evaluate the approach to measuring its implementation and effectiveness.

To help facilitate use of the framework, DHS created the Critical Infrastructure Cyber Community (C^3) Voluntary Program to aid academia, businesses, and governments with implementation; and develop sector-specific guidance for

using the framework. In 2014, 420 stakeholders from across the Federal Government and the private sector participated in C^3 Voluntary Program regional meetings. Additionally, this program features more than 30 DHS programs and tools on its website, including an updated self-assessment tool called the Cyber Security Evaluation Tool, which assesses an organization's security practices for its information-technology network against recognized industry standards. C^3 stakeholders downloaded or received the tool 5,132 times in fiscal year 2014.



In October 2014, the Securities Industry and Financial Markets Association published *Principles for Effective Cybersecurity Regulatory Guidance*, which advises financial institutions on creating effective cybersecurity initiatives and encourages them to leverage NIST's framework on cybersecurity.

The Federal Government has expanded cybersecurity workforce hiring and training programs to state, local, tribal, and territorial partners in order to address widespread shortages of trained cybersecurity professionals.

Thousands of cybersecurity jobs across all levels of government and the private sector remain unfilled, despite years of effort to boost hiring of cybersecurity professionals. In a 2014 survey of 49 state Chief Information Security Officers, 59 percent indicated that hiring cybersecurity professionals was a top barrier to strengthening their state's cybersecurity. Additionally, despite 88 percent of states and territories listing the Cybersecurity core capability as a high priority in their 2014 State Preparedness Report responses, only 15 percent rated their Cybersecurity training capabilities as proficient (i.e., a 4 or 5 on a 5-point scale). To help address Cybersecurity needs, Federal departments and agencies expanded several ongoing training and hiring initiatives to state, local, tribal, and territorial partners in 2014 (see Table 2), which include scholarship programs, collaborative tools, and online-lab practice opportunities. In addition, states (e.g., Delaware), nonprofit organizations, and private-sector cybersecurity companies started their own cybersecurity hiring initiatives in 2014 to address workforce gaps.

Program	Description
Cyber Shield Alliance	An online platform with cyber training opportunities and cyber incident reporting to state and local law enforcement partners
Federal Cybersecurity Training Events	A platform for hosting interactive events that bring participants together to share cybersecurity best practices
Federal Virtual Training Environment	A library of more than 800 hours of cybersecurity classroom training and over 100 hands-on labs
National Computer Forensics Institute	A training campus operated by the U.S. Secret Service offering cybersecurity training courses to officials from over 700 state and local agencies, departments, and judicial offices from around the country (In fiscal year 2014, the Institute trained 1,533 students for a total of 84,800 hours, exceeding their fiscal year 2014 goals of 1,000 students and 45,000 hours)
National Initiative for Cybersecurity Careers and Studies	An online resource for cybersecurity career, education, and training information
Scholarship for Service	A program providing scholarships for students to obtain cybersecurity degrees in exchange for government service (As of December 2014, 54 academic institutions were participating)

Table 2. Federal cybersecurity hiring and training programs are available to state, local, tribal, and territorial governments as of 2014.

The Nation has intensified its efforts to combat violent extremism in response to threats within the United States and from Americans trained abroad.

Law enforcement officials are concerned that Americans and Europeans traveling to fight and train with violent extremists abroad may return and conduct terrorist attacks in the United States. Since 2001, law enforcement officers have accused at least nine Americans who fought for or received training from violent extremist organizations abroad of plotting terrorist attacks after their return to the United States. In addition, more than 100 Americans have joined over 1,000 Europeans in traveling or attempting to travel to Syria to fight in the country's civil conflict. In response, DHS has imposed enhanced screening measures on Europeans normally allowed to visit without visas, out of concern that Europeans who have fought in Syria may try to enter the United States. FBI has also created a hotline and requested the public's assistance in identifying individuals who have traveled (or plan to travel) overseas to engage in terrorist activities.

Violent extremism led to several incidents within the United States in 2014, including an attempted airport bombing and an attack on a Jewish Community Center. The Federal Government has recently expanded its efforts to address domestic violent extremism. In September 2014, DOJ initiated a pilot program in three regions that engages education administrators, mental health professionals, religious leaders, and other social service providers at the local level to identify individuals susceptible to radicalization and intervene to prevent acts of violence. Similarly, DHS and the National Counterterrorism Center held six exercises in 2014 to improve communication between Federal law enforcement and local communities on countering violent extremism. Afterward, exercise facilitators helped each community develop a community action plan that local governments can use to identify and respond to incidents of violent extremism. In 2014, DHS also supported the implementation of 15 roundtables on Building Communities of Trust. The roundtables provided a forum for community leaders and law enforcement officials to discuss how to keep communities safe from terrorism, crime, violence, and other locally based problems.

Recent incidents and analysis have led Federal departments and agencies to increase physical protections for high-risk facilities and radioactive materials.

After the DoD review of the September 2013 Washington Navy Yard shooting, the Secretary of Defense accelerated DoD's efforts to deploy the Identity Matching Engine for Security and Analysis, which enhances access control by checking the identification cards of individuals entering military installations against arrest and warrant records. Deployed to more than 100 military installations as of November 2014, the program identified over 170 individuals with outstanding arrest warrants attempting to enter DoD bases during a two-month period. DoD alerted law enforcement authorities to arrest these individuals, instead of allowing potentially dangerous persons to enter the military installations.

In the energy sector, DOE initiated and led a series of briefings in conjunction with DHS across 10 states to enhance physical security of electric substations in response to an April 2013 sabotage incident that damaged 17 transformers transmitting power to Silicon Valley. Additionally, FBI partnered with DOE to strengthen physical security at facilities that use radiological material. In fiscal year 2014, law enforcement and energy communities joined together to install security enhancements at 96 facilities, train 396 personnel, and conduct 6 tabletop exercises.

In May 2014, the North American Electric Reliability Corporation adopted a new reliability standard designed to enhance physical security measures for bulk-power system facilities to lessen their vulnerability to physical attacks. The Federal Energy Regulatory Commission approved the new standard in November 2014. The standard requires that owners and operators perform a risk assessment of their systems, analyze potential threats to those systems, and identify system vulnerabilities.

The Nuclear Regulatory Commission (NRC) also codified previously issued orders for physical protection of highly radioactive material in March 2014. Two months later, in partnership with the National Nuclear Security Administration and a nonprofit organization, NRC distributed a best practices guide to provide benchmarks and assistance for implementing the new requirements. The NRC is currently conducting inspections and taking enforcement actions to ensure compliance with the physical protection requirements of the 2014 regulation.

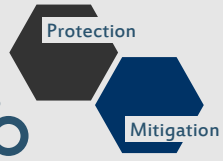
Critical infrastructure owners and operators are increasingly using Federal risk-analysis tools and implementing recommended security improvements, while Federal assessments are expanding focus to address new hazards.

Critical infrastructure owners and operators continue to use Federal tools and programs to help conduct risk assessments, leading to an increased number of implemented security measures in 2014. In fiscal year 2014, DHS completed 2,202 critical infrastructure surveys or facility visits to assess overall security and increase security awareness, up 13 percent from fiscal year 2013. Over the same period, DHS conducted an additional 246 site-assistance visits and 623 web-based assessments. Fiscal year 2014 follow-up visits confirmed that 76 percent of facilities had planned, started, or completed at least one security improvement since the DHS risk assessment. Of those that had completed improvements, 86 percent reported that the security enhancement was a direct result of the DHS assessment.

Through the Regional Resiliency Assessment Program, DHS also provided 10 regional vulnerability assessments in 2014 that focused on groups of critical infrastructure and key resources. These studies assess specific infrastructure sectors against a range of hazards, including the first-ever climate change and cyber-focused regional assessments in 2014. Of the regional assessments completed, 65 percent of primary stakeholders reported that they implemented, are in the process of implementing, or plan to implement at least one security enhancement.

Additionally, private-sector partners used sector-specific tools and programs to analyze risk and protect against hazards in 2014. The Dams Sector Analysis Tool—a web-based platform of analysis tools and data-collection mechanisms to protect the Nation's dams—helped stakeholders run more than 1,300 dam-break, flood-inundation simulations to test for screening, prioritization, characterization, and analysis of critical assets, and update plans and policies accordingly. The Bureau of Reclamation also helped improve dam preparedness by conducting 34 dam inspections and risk assessments in fiscal year 2014 to determine potential means of failure and resulting consequences. Moreover, DHS began a series of resilience webinars to address risks from cross-sector interdependencies for commercial stakeholders.

Mission Area Connections



Risk Analysis

Conducting risk analysis helps design successful strategies to minimize consequences on critical infrastructure for both the Protection and Mitigation mission areas. Protection uses risk analysis to enhance security, while Mitigation relies on risk analysis (using concepts of risk identification and vulnerability assessment) to strengthen resilience. Many of the same steps to conducting effective mitigation are equally applicable to protecting critical infrastructure (see page 38 for additional details).

Preparedness Case Study: IP Gateway

In September 2014, DHS released the IP Gateway—an online interface where state, tribal, and territorial partners can access a range of tools and information to conduct risk analysis using a standardized, streamlined assessment methodology. Within a month of its release, 35 states adopted the IP Gateway to support their critical infrastructure security and resilience efforts.

The Federal Government is working with chemical facility owners and operators to improve information-sharing platforms and to provide guidance on regulatory requirements for facility security.

A key element of *Executive Order 13650: Improving Chemical Facility Safety and Security* is strengthening the relationship between government and chemical facility owners and operators. EPA, the U.S. Department of Labor, and DHS developed several initiatives to improve information-sharing platforms in 2014. Specifically, they partnered to update online systems to help chemical facilities determine regulatory requirements and enabled the Federal Government to compare a facility's information across nearly 90 separate Federal and state systems. These comparisons help identify at-risk facilities by examining compliance history and chemical storage information.

DHS also worked with high-risk chemical facilities to implement security plans authorized under the Chemical Facility Anti-Terrorism Standards regulations. Chemical facility inspectors found that the highest-risk chemical facilities implemented 78 percent of required security measures in 2014, an increase from 46 percent in fiscal year 2013, but short of DHS's goal of 97 percent. In fiscal year 2014, FBI tested cross-jurisdictional response capabilities in six Livewire tabletop exercises, which addressed the acquisition and release of toxic industrial chemicals by terrorists. Additionally, in October 2014, EPA and the National Oceanic and Atmospheric Administration (NOAA) updated the Computer-Aided Management of Emergency Operations Suite, a system of software applications that the whole community can use to plan for and respond to chemical emergencies. In 2014, users downloaded the suite of programs over 80,000 times. Improving the Computer-Aided Management of Emergency Operations Suite was one of several actions that a working group established by Executive Order 13650 recommended in a May 2014 report to the President, entitled *Actions to Improve Chemical Facility Safety and Security – A Shared Commitment*, to further minimize chemical facility safety and security risks.

DHS also conducted over 250 compliance-assistance visits and 130 presentations to assist chemical facilities in meeting Federal security standards in fiscal year 2014. DHS's Infrastructure Security Compliance Division has found that as facilities move through the Chemical Facility Anti-terrorism Standards regulations, compliance assistance visits become less necessary. As a result, DHS saw a slight downward trend in the number of these visits in 2014 and an upward trend in the number of regulatory inspections. Chemical facilities also took initiative to improve security practices, completing 3,994 web-based Chemical Security Awareness Trainings in fiscal year 2014.

Implementation of personal identity verification cards for network access across the Federal Government was at 72 percent overall in 2014, but implementation gaps remain in several Federal agencies. Excluding DoD, implementation was at 41 percent.

The 2004 *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* requires all Federal agencies to issue and adopt smartcards to verify user identity for access to Federal facilities and information systems. These credentials allow access to Federal facilities and systems, using more than one means of authentication to create a high level of identity assurance. Fifty-four percent of Federal civilian cybersecurity incidents in fiscal year 2014 were related to or could have been prevented by these strong authentication measures, down from 66 percent of incidents in fiscal year 2013. Implementation of personal identity verification cards across the Federal Government to allow access to Federal information networks increased from 67 percent in fiscal year 2013 to 72 percent in fiscal year 2014. However, as of fiscal year 2014, 18 of the 24 agencies required to implement smartcard verification had not made a majority of privileged users on their networks log on using smartcard authentication, and three agencies had not implemented smartcard verification at all. DoD's inclusion resulted in a higher overall percentage of implementation because of its large number of network users and strong performance in authentication implementation.

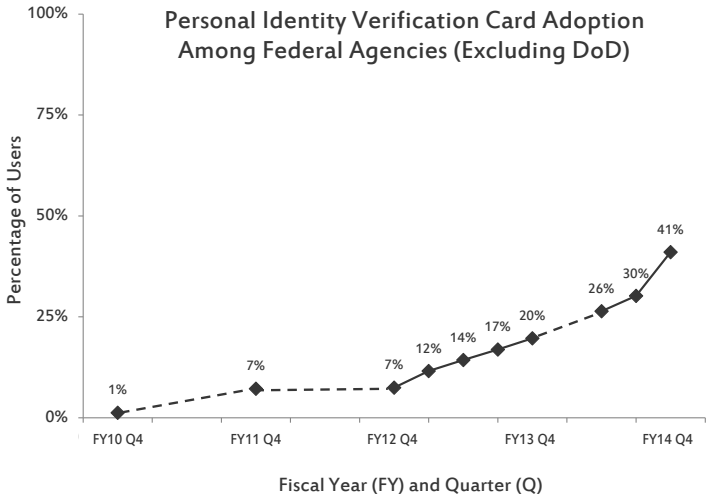


Figure 6. Despite progress in recent years, less than half of the Federal workforce (when excluding DoD) require personal identity verification cards for access to information systems. [*Note: Dashed lines indicate quarters in which data were unavailable.*]

To provide a more nuanced view of the Federal Government's overall progress, in March 2014, the White House began reporting implementation metrics for personal identity verification cards that do not include DoD contributions. As shown in Figure 6, 41 percent of non-DoD agency personnel had adopted cards by the fourth quarter of fiscal year 2014, an increase of more than 20 percentage points since the previous year. The new metrics reveal opportunities for improving implementation of personal identity verification cards across the Federal Government.

The Federal Government has initiated pilot programs in preparation of implementing the International Trade Data System.

The Federal Government requires businesses that engage in international trade to submit import/export data to help law enforcement interdict illicit goods before they enter the United States, while facilitating the flow of legitimate trade and travel. Since 2006, 48 agencies, led by CBP, have worked to build and implement the International Trade Data System, which establishes a single electronic platform for import/export data. By centralizing, automating, and integrating data-collection processes, the system allows for easier identification of items of concern, while reducing the reporting burden for industry. In 2014, the White House issued *Executive Order 13659: Streamlining the Export/Import Process for America's Businesses*, establishing a December 2016 deadline for completing the International Trade Data System. The Executive Order also charges the Border Interagency Executive Council—an interagency working group—to develop processes that enhance coordination for supply chain management and to establish common risk management principles and methods that inform CBP operations associated with cargo review and release.

The Federal Government continued implementing the International Trade Data System in 2014. CBP, the Food Safety Inspection Service, and EPA began testing the system through two programs in spring 2014. By the end of 2014, CBP automated 73 of the 189 forms that it intends to automate using the International Trade Data System.

Mission Area Overview

Mitigation

Focused on reducing loss of life and property by lessening the impact of disasters through increasing risk awareness and leveraging mitigation products, services, and assets across the whole community

Highlights

- Severe drought continues to affect much of the western United States, but new tools and guidance are available to assist states in improving their drought plans. (p. 41)
- The Nation faces growing risks associated with climate change, but Federal agencies and states are taking steps to adapt to those risks. (p. 43)
- The Federal Government is studying how green infrastructure projects that harness natural processes can reduce damage from natural disasters. (p. 44)
- The whole community is increasingly using resilience competitions to spur innovations that will strengthen disaster preparedness nationwide. (p. 46)
- The National Flood Insurance Program continues to face challenges to its long-term financial sustainability. (p. 49)

Frameworks in Action

The *National Mitigation Framework* (the Mitigation Framework) builds on the seven mitigation core capabilities identified in the Goal and describes 88 critical tasks to support their execution. The Mitigation Framework employs a risk-based approach to reduce loss of life and property and increase community resilience. By reducing risk, mitigation activities reduce the resources needed to respond to and recover from disasters.

As shown in Figure 7, effective mitigation begins with **risk identification**, in which a community identifies the threats and hazards it faces and the likelihood of their occurrence. The community then conducts a **vulnerability assessment** to understand the effects that these threats and hazards would have if they occurred. Based on this understanding of risk, a community can choose one or more **risk management strategies**, including:

- *Risk avoidance* – Preventing exposure to an event (e.g., using zoning laws and other standards to prevent the construction of homes in high-risk areas);
- *Risk reduction* – Minimizing vulnerabilities (e.g., retrofitting buildings to be more resistant to earthquakes);
- *Risk transfer* – Eliminating or limiting financial liability, without reducing vulnerability (e.g., purchasing insurance); and
- *Risk acceptance* – Tolerating any remaining risk and liability (e.g., agreeing to pay a deductible).

Efforts to improve resilience after Hurricane Sandy demonstrate how the Mitigation Framework guides the whole community in employing the Mitigation core capabilities. The President established the Hurricane Sandy

Core Capabilities in the Mitigation Mission Area

- Community Resilience
- Long-term Vulnerability Reduction
- Operational Coordination
- Planning
- Public Information and Warning
- Risk and Disaster Resilience Assessment
- Threats and Hazard Identification

Rebuilding Task Force (the Task Force) to improve rebuilding and develop a comprehensive set of recommendations that cover every component of effective mitigation.

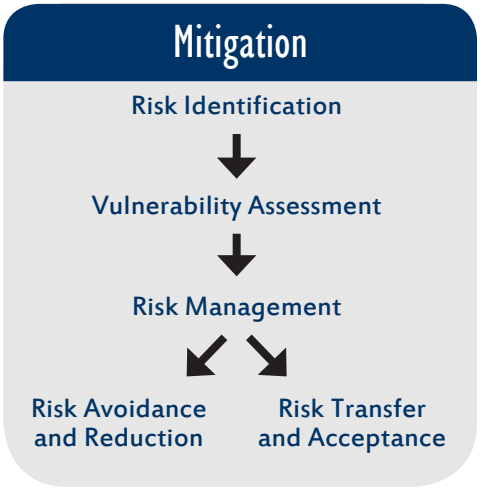
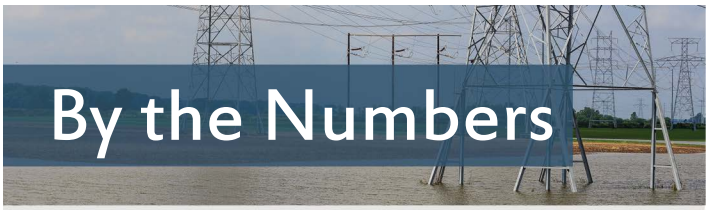


Figure 7. Multiple steps are necessary to conduct effective mitigation.

Risk Identification & Vulnerability Assessment: The Task Force recognized the need to identify risks associated with rising sea levels and incorporate them into future vulnerability assessments. Acting on the Task Force's recommendation, NOAA, FEMA, the U.S. Global Change Research Program, and the U.S. Army Corps of Engineers (USACE) coordinated to develop a sea level–rise calculator and an interactive web-based map to identify risks posed by sea level rise. The mapping tool combines the best available data from peer-reviewed, global sea level–rise scenarios with existing FEMA National Flood Insurance Program maps to estimate where the 100-year floodplain boundaries will be in the future. The interactive web-based map translates data into actionable information by allowing users to see how vulnerable their properties are to the risk of rising sea levels.

Risk Management: The majority of the Task Force's recommendations focus on improving risk management. The Task Force embraced both risk-avoidance and risk-reduction strategies in its green infrastructure recommendations. For example, the U.S. Department of the Interior's (DOI's) Coastal Resilience/Green Infrastructure projects restored 147 acres of floodplains, helping jurisdictions avoid future flood risk by removing existing structures from floodplains and preventing new structures from being built in those locations. Additionally, by freeing the floodplain land to absorb water, jurisdictions have likely reduced the risk of flooding in surrounding communities.

Effectively transferring risk is also critical, as adequate insurance provides policyholders with funds to rebuild quickly after an event. Acting on Task Force recommendations to promote insurance coverage, FEMA has begun clarifying its insurance requirement for obtaining Public Assistance under the Stafford Act and is seeking to incentivize increased levels of private insurance coverage. In addition, the National Academy of Sciences is examining how to make the National Flood Insurance Program more affordable.



By the Numbers

$1.4 billion — In October 2014, USDA announced the availability of $1.4 billion in loan guarantees to support projects that improve rural electrical infrastructure in 21 states.

1,000 organizations — NOAA has recognized nearly 1,000 organizations under its new Weather-Ready Nation Ambassador™ initiative to build community resilience in the face of increasing vulnerability to extreme weather and water events.

43 cents — For every dollar that FEMA spent on Public Assistance in New York for Hurricane Sandy recovery, 43 cents supported mitigation activities. The program's national average is six cents.

Resilience Innovations

- USGS's Coastal Change Hazards Portal is an interactive mapping product that shows shoreline change, extreme storms, and sea level rise. It supports planning and preparedness to enhance coastal resilience.
- A partnership of Federal agencies developed the U.S. Climate Resilience Toolkit, which provides scientific tools, information, and expertise to help people manage their climate-related risks.
- NOAA completed construction of the National Water Center, which will serve as a catalyst for Integrated Water Resources Science and Services, enabling NOAA to work with Federal partners to deliver state-of-the-art analyses and forecasts for floods and droughts.
- DOE published a study of four major metropolitan areas that offer a flexible and scalable approach to identify energy facilities potentially at risk for flooding from rising sea levels through the year 2100.

Whole Community Accomplishments

Los Angeles and Long Beach, California In 2014, the cities of Los Angeles and Long Beach, California, working with the State of California and DHS, invested nearly $6 million for 125 new seismic stations across the region, which advance the capacity to provide early earthquake warnings.

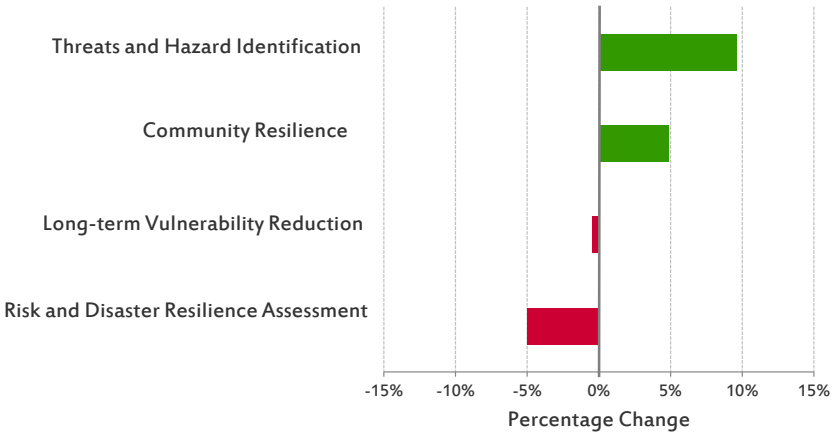
Washington State Washington State is partnering with the University of Washington, FEMA, NOAA, and USGS to build the first tsunami-resistant building in North America. Construction began in 2014.

Nevada Nevada Division of Forestry led an effort that resulted in all counties in Nevada developing plans to provide communities with a prioritized list of hazards and step-by-step recommendations to protect people, infrastructure, and resources from wildfires.

State Perspectives on Preparedness

2014 State Preparedness Report Results

- From 2012 to 2014, the percentage of proficient ratings for Threats and Hazard Identification increased by 9.6 percentage points, second only in progress to Operational Coordination. In contrast, Risk and Disaster Resilience Assessment experienced the third-worst decline in performance among all 31 core capabilities.
- On average, when comparing performance among planning, organization, equipment, training, and exercises, Mitigation core capabilities achieved the highest ratings for planning. Sixty-four percent of states and territories assessed themselves as proficient for planning under Threats and Hazard Identification—an increase of nearly 20 percentage points since 2012.



Note: The chart and statements do not include contributions from the three common core capabilities—Planning, Operational Coordination, and Public Information and Warning.

Mitigation Mission Area

Key Findings

Risk Identification and Vulnerability Assessment

Severe drought continues to affect much of the western United States. Most states do not have recently updated drought-specific plans, but new guidance and tools are available to help states identify their drought risks and improve their plans.

Much of the western United States continued to experience drought throughout 2014. For example, California experienced its third-driest water year in recorded history from October 2013 to September 2014. During the past three years, California's average precipitation reflected the second-driest conditions since recordkeeping began in 1895. Although severe rainstorms brought some drought relief in early December, National Aeronautics and Space Administration scientists have determined that California would still need 11 trillion gallons of water to recover from the three-year drought.

Across the United States, severe drought conditions have caused more than $57 billion in damages from 2009 to 2013 (see Table 3). An estimate in July projected that the 2014 drought in California alone would cost the state $2.2 billion in damages and 17,100 seasonal and part-time jobs.

Year	Region(s) Affected by Drought	Estimated Losses
2014	Western Drought	> $1 billion
2013	Western /Plains Drought	$10 billion
2012	Expansive/U.S. Drought	$30 billion
2011	South Plains/Southwest Drought	$12 billion
2009	Plains/Southwest Drought	$4 billion
	Total	**> $57 billion**

Table 3. Drought conditions have cost the United States billions of dollars in five of the last six years.

Although the Secretary of Agriculture issued drought disaster designations for counties in 31 states in 2014, only eight states have updated their drought plans since 2010 (see Figure 8). Furthermore, five states do not have a statewide drought-specific plan; three of these states are currently experiencing drought. Regularly updating drought plans allows jurisdictions to incorporate new technology, research, or laws.

New guidance is available to assist state and local jurisdictions with planning for drought and its related impacts. In January 2014, the National Integrated Drought Information System, the National Drought Mitigation Center, and the American Planning Association issued a new drought planning guidebook, which assists planners in preparing for risks associated with drought, including the need to plan for secondary hazards such as increased risk of flooding or wildfire. In 2014, CDC also assembled a set of drought-related information resources for individuals and communities, including guidance on how to prevent fire hazards resulting from drought. Additionally, the National Drought Resilience Partnership—a collaboration between seven Federal agencies established in 2013 as part of the President's *Climate Action Plan*—issued new guidance for Federal agencies to advance drought resilience in November 2014.

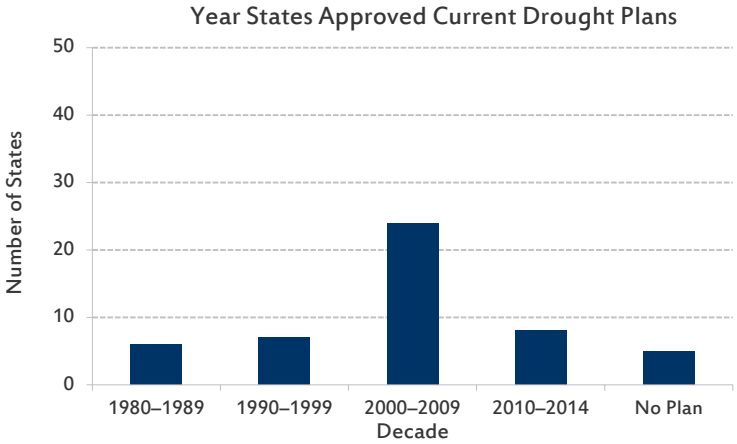


Figure 8. Most states have not updated their drought plans since 2010.

In addition, Federal agencies are working together to provide states with tools that help identify their drought risks. The U.S. Drought Portal is continuing to enhance its capabilities to predict the onset of drought. Currently, the U.S. Drought Outlook tool can predict drought conditions up to three months in advance. In 2014, NOAA awarded $6.6 million to support 15 new, multi-year projects that enable university partners and Federal researchers to improve understanding of drought and advance drought prediction and monitoring capabilities.

The Federal Government is improving the quality of the Nation's flood maps, particularly in coastal areas.

FEMA's Risk Mapping, Assessment, and Planning program (Risk MAP) provides the public and emergency managers with high-quality flood maps. In fiscal year 2014, Risk MAP updated maps for 56 coastal projects, bringing the total number of updated projects to 153. As of June 2014, updated Risk MAP products covered more than 53 percent of the U.S. population, exceeding the program's goal of 50 percent. FEMA is also using the expertise of the whole community to improve the quality of its maps. The 2014 *Homeowner Flood Insurance Affordability Act* requires FEMA to convene a Technical Mapping Advisory Council to provide expert guidance during the map-making process and certify that FEMA is using technically credible data and mapping approaches. The council—which includes representatives from six Federal agencies, as well as state and local experts—held its first public meeting in September.

Other Federal agencies also contribute to the national flood-mapping effort. In 2014, NOAA's National Geodetic Survey conducted two aerial surveys of coastal areas using a laser-based remote sensing technology known as LiDAR to improve the accuracy of data used for mapping floodplains, managing coastal zones, and reducing impacts from storms. USGS, in partnership with other Federal agencies, also launched a $13.1 million program to develop three-dimensional mapping data of the United States for flood risk management, water resource planning, and mitigation of coastal erosion. FEMA is using the data collected by NOAA and USGS to update coastal flood insurance studies, including storm surge and wave modeling.

Preparedness Case Study:

Mapping Non-accredited Levees

To improve flood map quality, FEMA launched 25 pilot programs across eight FEMA Regions to map the Nation's non-accredited levee systems. The new approach recognizes that these levee systems—which do not currently meet Federal regulations for levees—may still provide some level of protection, resulting in more accurate assessments of communities' flood risks. As of October 2014, 4 of the 25 projects had completed final analysis and mapping plans. Including the pilots, FEMA initiated 65 projects in fiscal year 2014 to analyze and map levees.

Risk Management: Risk Avoidance and Reduction

The third *National Climate Assessment* reported that the Nation faces growing risks associated with climate change. Federal agencies and states are responding by taking steps to adapt to these risks.

In January 2015, NOAA and the National Aeronautics and Space Administration issued separate assessments concluding that 2014 was the hottest year worldwide since 1880. Earlier in 2014, the U.S. Global Change Research Program published the third *National Climate Assessment*. Using the best available science, the report identifies current and possible future impacts of climate change on the United States, including an increased risk of sea level rise and severe storms. The President's *Climate Action Plan* is helping direct efforts to increase climate resilience. *Executive Order 13653: Preparing the United States for the Impacts of Climate Change* created a State, Local, and Tribal Leaders Task Force on Climate Preparedness and Readiness to advise the Federal Government on how to respond most effectively to community-level needs regarding climate change adaptation. This task force issued several recommendations, including: (1) improving the Nation's ability to address challenges that communities face to provide physical, programmatic, and effective communication accessibility inclusive of individuals with access and functional needs; (2) promoting and prioritizing the use of green infrastructure; and (3) examining how incentives can increase economic resilience. Federal agencies are actively reviewing and prioritizing actions they can take to respond to the task force's recommendations.

The Executive Order also required Federal agencies to update their climate adaptation plans. In 2014, 38 agencies publicly released updated plans outlining how they will reduce climate risk. Federal agency adaptation plans also support collaboration across regions and promote data sharing and tool development. For example, USDA launched Regional Climate Hubs in 2014 to provide technical support, assessments, and forecasts to regional and local stakeholders. FEMA's National Exercise Division also launched a Climate Change Preparedness and Resilience Exercise Series to advance dialogue on climate resilience among participants and identify collaborative and sustainable approaches to community-based adaptation. In 2014, FEMA held climate exercises in Anchorage, Alaska; Fort Collins, Colorado; Houston, Texas; and Hampton Roads, Virginia. Exercise participants included Federal, state, and local government representatives, as well as private-sector, nongovernmental, and academic partners.

Preparedness Case Study:

New Federal Flood Risk Management Standard

The President's *Climate Action Plan* directed Federal agencies to update their flood risk reduction standards to better account for future risks from climate change. In response, Federal agencies developed a new Federal Flood Risk Management Standard, established in Executive Order 13690, which seeks to support implementation of *Executive Order 11988: Floodplain Management* and to improve the Nation's resilience to current and future flood risk. When implemented, the new standard gives Federal agencies the flexibility to select one of three approaches for establishing the flood elevation and hazard area they use in siting, design, and construction. They can:

- Use data and methods informed by best-available, actionable climate science;
- Build two feet above the 100-year (one-percent annual chance) flood elevation for standard projects, and three feet above for critical buildings such as hospitals and evacuation centers; or
- Build to the 500-year (0.2-percent annual chance) flood elevation.

The standard allows exceptions for emergency actions, national security considerations, and other mission-critical needs. Federal agencies will reassess the standard annually to determine if updates are needed outside of a comprehensive update every five years.

In addition to Federal efforts, some states are responding to the risks of climate change by creating climate adaptation plans. As of 2014, 14 states had finalized state-led adaptation plans, and another nine states began planning efforts. The Georgetown Climate Center State Adaptation Progress Tracker monitors progress in implementing goals and milestones in state adaptation plans. On average, states have begun to address more than 50 percent of their identified goals, but have only completed 5.4 percent of those goals. California and New York have completed the most, having each finished 14 percent of their goals. Despite progress, 48 percent of states did not consider climate change in their Threat and Hazard Identification and Risk Assessments for 2014. Of those states, 60 percent are located in coastal areas.

Federal agencies are exploring the potential benefits of green infrastructure for disaster mitigation.

The President's State, Local, and Tribal Leaders Task Force on Climate Preparedness and Resilience recommended that agencies promote and prioritize green infrastructure due to its potential economic, environmental, and risk-reduction benefits. As a result, EPA and the White House Council on Environmental Quality launched a Green Infrastructure Collaborative in 2014 to coordinate green infrastructure initiatives and align public and private knowledge and resources to promote green infrastructure. As of October 2014, the partnership had consisted of 26 organizations and associations. Federal commitments to the collaborative that may provide risk-reduction benefits include:

- EPA providing assistance to 25 communities to create integrated stormwater management and hazard mitigation plans; and
- DOI committing $100 million for green infrastructure projects through the Hurricane Sandy Coastal Resilience Grant Program.

The extent of risk reduction provided by green infrastructure projects, however, is difficult to measure, which has limited private-sector adoption of green infrastructure as a tool for risk reduction. To address this knowledge gap, NOAA and USACE are assessing the effectiveness of green infrastructure to reduce risks as part of long-term research projects. In one of its multi-year projects for the Sandy-affected region, NOAA is assessing green infrastructure performance metrics and techniques that use plants, sand, and rocks to provide shoreline protection, as well as other nature-based protections and restoration options. For example, NOAA is funding a project to analyze suitable shoreline restoration approaches for damaged areas in Staten Island and Jamaica Bay, including developing decision support criteria and providing technical assistance to decision-makers. In addition, USACE's *North Atlantic Coast Comprehensive Study* provides a framework to help communities assess the value of natural and nature-based protections. This framework includes:

- Examples of construction costs associated with natural and nature-based features;
- A matrix showing how each type of green infrastructure feature contributes to environmental and mitigation benefits (e.g., biodiversity, reduction of storm surge, erosion protection); and
- Performance metrics for measuring the effectiveness of each type of green infrastructure feature in delivering associated benefits.

In accordance with recommendations from the Hurricane Sandy Rebuilding Task Force, a task force organized under the National Science and Technology Council, with guidance from the White House Office of Science Technology and Policy, is developing a Federal research agenda to address knowledge gaps related to the societal benefits—often referred to as "ecosystem services"—associated with green infrastructure, and how this infrastructure can be used to protect and enhance the resilience of our Nation's communities, particularly in coastal areas.

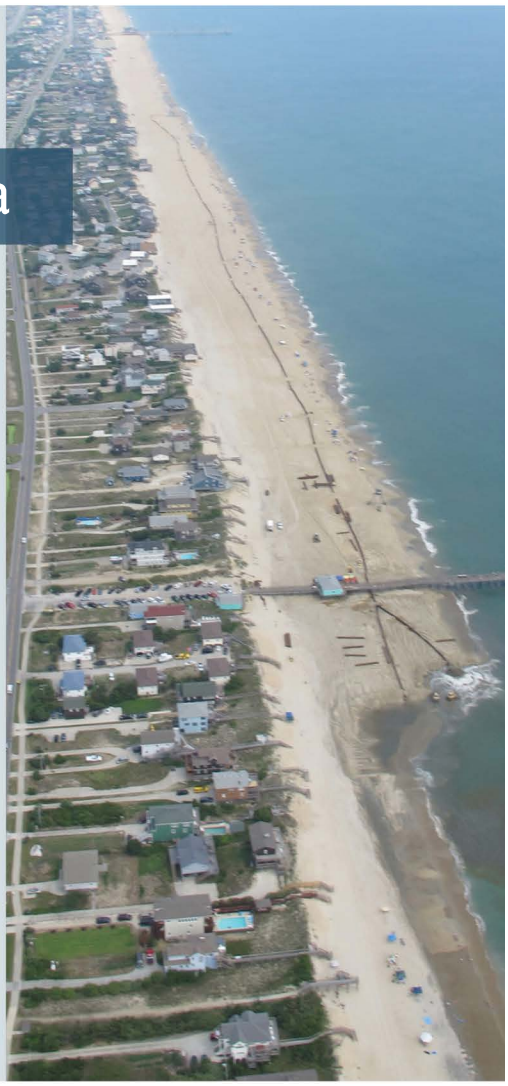
Preparedness Case Study:

Long-term Mitigation Efforts in North Carolina

On July 3, 2014, Hurricane Arthur made landfall on the coast of North Carolina. Although the Category-2 hurricane produced high winds and flooding, North Carolina experienced minimal damage. This was due in part to North Carolina's pursuit of a long-term mitigation strategy that had increased the resilience of local communities affected by earlier hurricanes and severe storms.

Since 2003, North Carolina has used the majority of its mitigation funding to buy out vulnerable properties and elevate structures. Moreover, North Carolina Emergency Management conducts vulnerability assessments to prioritize which structures to modify when funding becomes available. To date, North Carolina has acquired more than 5,000 homes located in vulnerable areas and elevated 800 flood-prone properties. In March 2014, North Carolina became one of only 11 states in the Nation with an Enhanced Hazard Mitigation Plan, indicating superior floodplain-management practices and qualifying the state for additional hazard mitigation grant funding following a disaster.

North Carolina has also invested in natural protections against storm surge. The town of Nags Head, on North Carolina's Outer Banks, placed 4.6 million cubic yards of sand from offshore areas and restored a 10-mile stretch of beach to protect structures from storm surge. The project succeeded in mitigating losses from Hurricane Irene in 2011, Hurricane Sandy in 2012, and Hurricane Arthur in 2014.



Mitigation grant funding is incentivizing state and local governments to engage in multi-hazard mitigation planning, but gaps remain.

FEMA requires states to have approved hazard mitigation plans to qualify for permanent repair and restoration of damaged public infrastructure, as well as for FEMA Hazard Mitigation Grants. Additionally, states can increase the amount of Hazard Mitigation Grants they receive by 33 percent if they maintain an "enhanced" hazard mitigation plan. This status indicates that the state has expended additional effort to reduce losses, protect its resources, and create safer communities. While all 50 states have approved hazard mitigation plans, as of September 2014, only 11 states achieved enhanced status.

Local jurisdictions must also maintain hazard mitigation plans to qualify for FEMA Hazard Mitigation Grants. Over the past five years, the percentage of the U.S. population living in jurisdictions with FEMA-approved local hazard mitigation plans has risen steadily from less than 70 percent to nearly 80 percent. However, 96 percent have lived in jurisdictions that initially had an approved hazard mitigation plan, indicating that some plans have expired. Despite progress, variations exist among regions in the development and maintenance of hazard mitigation plans. For example, hazard mitigation plans cover over 90 percent of populations in the Mid-Atlantic, Southeast, and Great Plains, whereas plans cover 61 percent of the population in the Northeast. Moreover, only 127 of the 566 federally recognized tribes maintain an approved or pending hazard mitigation plan; however, this is an increase from 88 tribes five years earlier.

The 2013 tornados near Oklahoma City, Oklahoma, highlighted the importance of maintaining local hazard mitigation plans. The original major disaster declaration included five counties, but, of the five, only one county had a FEMA-approved local hazard mitigation plan at the time of the disaster. Thus, FEMA could not provide mitigation funding to four of the five counties, despite authorizing more than $2.3 million in Hazard Mitigation Grant Program funding in Oklahoma within 30 days of the disaster declaration. The remaining counties had previously received FEMA Hazard Mitigation Grant funds to create or renew their plans. FEMA worked with these counties to expedite the renewal of their expired plans and eventually qualified them for funding, but most missed project application deadlines by not proactively submitting applications.

Mission Area Connections

Mitigation

Recovery

Hazard Mitigation Plan

Mitigation	Qualifies states for FEMA Hazard Mitigation Grant funding, with additional funding for states that maintain Enhanced Hazard Mitigation Plans.
Recovery	Allows communities to receive more Federal mitigation funding after a disaster, enabling them to complete more recovery projects to increase future resiliency.

The Federal Government and other organizations are increasingly using sponsored competitions to incentivize innovations that improve community resilience across the Nation.

In the aftermath of Hurricane Sandy, Federal and local governments sponsored design competitions to encourage resilient rebuilding projects in the affected area. For example, the HUD-sponsored "Rebuild by Design" competition sought to provide communities with new, more durable infrastructure designs. For this competition, HUD partnered with the

Rockefeller Foundation, academic institutions, and regional nonprofit organizations. In May 2014, HUD announced the availability of $930 million in Community Development Block Grant Disaster Recovery funds for projects in the Sandy-affected area that incorporate these winning designs. New York City's Urban Post-Disaster Housing Prototype Program is also testing an interim post-disaster housing unit based on the winning design entry in the city's "What If New York City…" innovation competition (see page 70 for more details).

In 2014, Federal agencies and the Rockefeller Foundation also sponsored competitions to address other resilience challenges facing the Nation:

- In June 2014, the President announced the National Disaster Resilience Competition, which awards nearly $1 billion to help disaster-affected communities build toward a more resilient future. Participants must identify unmet needs in a community, commit to actions that permanently strengthen resilience, and propose innovative approaches to deliver resilience to multiple sectors. The estimated date for the announcement of the competition winners is December 2015.
- The Rockefeller Foundation is sponsoring the 100 Resilient Cities competition, which helps cities around the world mitigate the risks of extreme weather. The Foundation has selected the first 67 cities, including 17 located in the United States. Winning applicants receive support for developing resilience plans and hiring a Chief Resilience Officer to guide the city's resilience efforts.
- In December 2014, the White House announced 16 communities from around the country as the first cohort of Climate Action Champions. Selected communities receive a broad range of Federal support, including facilitated peer-to-peer learning, technical assistance, exercise opportunities, and climate data and tools.

Mission Area Connections

Mitigation

Recovery

National Disaster Resilience Competition

The $1 billion competition is eligible within any state that received a major disaster declaration from 2011 to 2013 and encourages communities to consider not only how they can recover from past disasters, but also how to avoid future losses. The application process requires communities to demonstrate how they are approaching the recovery from the previous disaster as an opportunity to reduce future risks and advance broader development goals.

Preparedness Case Study:

Kentucky and Georgia Promote Emergency Response Drills for Schools through America's PrepareAthon!

In 2014, FEMA launched America's PrepareAthon!—a community-based campaign focused on encouraging emergency preparedness through planning, drills, discussions, and exercises. Over 26 million individuals registered to participate in the spring and fall campaigns. In FEMA Region IV, the Kentucky Center for School Safety collaborated with America's PrepareAthon! to promote earthquake and tornado readiness exercises in all Kentucky schools. Over 1.3 million students, teachers, and administrators completed drills in September 2014. Similarly, Ready Georgia—a statewide campaign supported by the Georgia Emergency Management Agency aimed at motivating Georgians to prepare for a disaster—initiated a school tornado drill to increase awareness of the severe autumn tornado season. Organizers synchronized the event with America's PrepareAthon! to generate community awareness and engagement in the drill. More than 1.1 million students from 1,400 Georgia schools completed a tornado drill in October 2014.

The Federal Government, states, and the private sector are working together to develop and test microgrids. States are applying funding for Hurricane Sandy recovery to further these and related efforts to improve the resilience of their electrical grids.

Federal research institutions, private companies, and state and local governments are partnering to develop microgrid projects that enhance the resilience of the electrical grid. Disasters of all sizes commonly result in power outages. The Council of Economic Advisers and DOE's Office of Electricity Delivery and Energy Reliability estimate that the susceptibility of the electrical grid to these outages costs the U.S. economy between $18 and $33 billion annually. Microgrid technology—which provides a self-sustained electrical supply that can operate independently from traditional large-scale distribution networks—can help mitigate these impacts.

DoD, DOE, and Sandia National Laboratories are completing a multi-year pilot project called the Smart Power Infrastructure Demonstration for Energy Reliability and Security to test new microgrid technology. The project installed microgrids at military bases in Hawaii and Colorado, allowing the bases to continue operating even when the external grid experiences power loss. While primarily focused on cybersecurity for military installations, the technology has broader disaster applications for the public and private sector to improve the resiliency of energy infrastructure. In April 2014, the U.S. Northern Command hosted an event for stakeholders interested in microgrid development to facilitate information sharing on how to apply the pilot technology to public utilities and the commercial sector.

States are also increasing the resilience of electrical grids and mass transit systems in Sandy-affected areas. DOE and Sandia National Laboratories are working with Hoboken, New Jersey, to improve the resilience of the city's electrical grid, including installing microgrids. DOE and Sandia are also partners in a New Jersey Transit project to build a resilient energy supply system for trains running between New York and New Jersey. The U.S. Department of Transportation (DOT) provided over $400 million in funding for this project, which will be the largest microgrid in the United States. FEMA and HUD are also providing $705 million in combined grant funding to repair and increase the resilience of the Long Island power grid by elevating damaged substations, strategically relocating power circuits to underground

positions, and implementing other related strategies. In addition, New York State announced the NY Prize, a $40 million competition to help build community-scale microgrids for areas with approximately 40,000 residents.

The City of Los Angeles, California, partnered with the USGS to develop *Resilience by Design*, a strategic plan to proactively address the city's earthquake vulnerabilities. The partnership studied vulnerabilities; convened stakeholders and experts from academia, industry, business, government, and local communities; and incorporated cutting-edge research and lessons learned from past earthquakes. The city recommended steps to fortify buildings, water systems, and telecommunications networks against seismic hazards.

Risk Management: Risk Transfer and Acceptance

The long-term financial viability of the National Flood Insurance Program remains at risk.

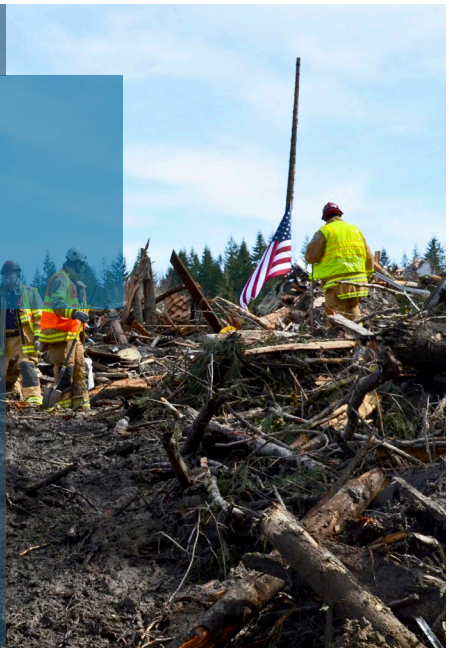
Through the National Flood Insurance Program, the Federal Government offers private and commercial flood insurance policies, providing property owners with protection that is usually unavailable or unaffordable in the private insurance market. FEMA currently owes the U.S. Department of the Treasury $23 billion, primarily to pay claims from Hurricane Katrina and Hurricane Sandy. FEMA made a $1 billion principal payment in December 2014, but estimates that it will not be able to repay this debt within the next 10 years.

Congress has taken steps to convert the program from being taxpayer-dependent to financially self-sufficient. For example, the 2012 *Biggert-Waters Flood Insurance Reform Act* (the Reform Act) required FEMA to eliminate the subsidy for certain grandfathered policies, with some policies increasing by thousands of dollars. The resulting affordability challenges led to the passage of the *Homeowner's Flood Insurance Affordability Act of 2014*. This law modified certain provisions of the Reform Act, including the reinstatement of subsidies that the Reform Act eliminated. New statutory limitations on premium increases also limit FEMA's ability to build sufficient reserves for future expenses or pay down the program's existing debt, making the National Flood Insurance Program's long-term financial stability an ongoing challenge.

Mission Area Overview

Response

Focused on ensuring that the Nation is able to respond effectively to all types of incidents, including those of catastrophic proportion that require marshaling the capabilities of the entire Nation



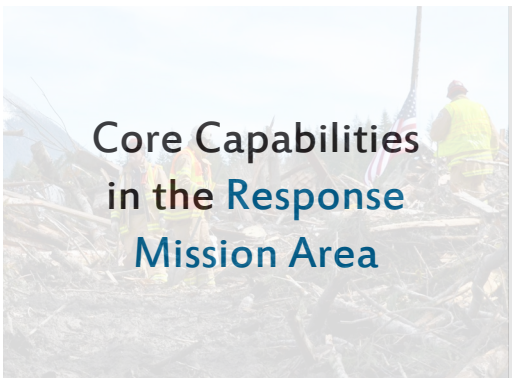
Highlights

- The Federal Government supported the response to the Ebola virus disease epidemic in West Africa and cases in the United States. (p. 54)
- The discovery of a major cyber vulnerability called Heartbleed prompted the Federal Government to establish new guidelines to delineate the roles and responsibilities of Federal cyber response assets. (p. 57)
- Increasingly violent and frequent mass shooting incidents prompted whole community partners to develop new response planning, training, and exercise initiatives for managing active shooter events. (p. 58)
- The large increase in unaccompanied children across the U.S.-Mexico border tested the ability of Federal agencies to expand and coordinate services in a non-Stafford Act event. (p. 60)

Frameworks in Action

The *National Response Framework* (the Response Framework) guides how the Nation responds to all types of incidents by describing the principles, roles and responsibilities, and coordinating structures for delivering the 14 core capabilities—and 29 associated critical tasks—necessary in incident response.

The whole community response to the March 2014 mudslide in Snohomish County, Washington, demonstrated the execution of several critical tasks. The American Red Cross provided 142 overnight stays in shelters for victims, highlighting the ability **to establish, staff, and equip emergency shelters**. Northwest Regional Aviation, an aircraft-sharing consortium created with support from the Seattle Urban Areas Security Initiative, **conducted** mass **search and rescue operations** and, in cooperation with the U.S. Navy, **rescued** 16 survivors. Additionally, the Governor activated more than 100 Air National Guardsman to assist in search and extraction operations. A collaborative effort among local, state, and Federal agencies **established operations** leading to the recovery of all 43 human remains. This collaboration also **established physical access** to the area through debris removal efforts, supported efforts to decontaminate responders and equipment exposed to spilled fuel and other hazardous liquids, and helped to dispose of animal remains. In addition, mental health professionals from various organizations (e.g., American Red Cross, Green Cross, Critical



Core Capabilities in the Response Mission Area

- Critical Transportation
- Environmental Response/Health and Safety
- Fatality Management Services
- Infrastructure Systems
- Mass Care Services
- Mass Search and Rescue Operations
- On-scene Security and Protection
- Operational Communications
- Operational Coordination
- Planning
- Public and Private Services and Resources
- Public Health and Medical Services
- Public Information and Warning
- Situational Assessment

Incident Stress Management response teams) provided counseling and support services to the families of victims.

The Response mission area also comprises several mature capabilities—including Mass Search and Rescue Operations, which focuses on **conducting search and rescue operations to locate persons in distress**. For the past seven years, USCG has consistently deployed assets to support search and rescue operations within two hours, meeting this target more than 95 percent of the time. The past year also saw emerging challenges for some mature capabilities. For example, the increasing frequency of wildfires and the length of the fire season stressed the highly capable wildfire response community in 2014. Nearly 3,000 more wildfires occurred in 2014 than 2013. Recognizing the need to **provide support to state and local wildfire operations**, the U.S. Forest Service continued to modernize its airtanker fleet in 2014, operating 18 next-generation and older airtankers and over 100 exclusive-use helicopters. An additional 100 helicopters and fixed-wing aircraft were on-call for the 2014 fire season.

USCG Expands Search and Rescue Capability to New Operating Environment

USCG continued to expand their operating environment, exercising new methods and technologies in the Arctic Circle. During Arctic Shield 2014, USCG focused on delivering search and rescue capabilities to Western Alaskan tribal regions and the Bering Strait, while testing new unmanned aerial systems, radars, and specialized ice-cutting tools.

By the Numbers

90 percent of Federal Departments and Agencies

Approximately 90 percent of Federal departments and agencies responding to a 2014 preparedness survey reported that they were developing operational plans supporting the Response Framework, and nearly 50 percent have developed an inventory of incident management assets conforming to nationally standardized definitions (i.e., resource typing).

127 Chemical Industry Outreach Workshops

FBI conducted 127 Chemical Industry Outreach Workshops to present information on preventing terrorists from acquiring bomb-making chemicals, and provide integrated response training among chemical industry personnel, academia, law enforcement, and first responder communities.

200 tribes

FEMA, with support from DOI's Bureau of Indian Affairs, engaged 200 tribes during 60 in-person meetings to inform new guidance for tribes seeking presidential disaster declarations.

Resilience Innovations

- DoD and partner organizations collaboratively developed the Geospatial capabilities for Security, Humanitarian Assistance, Partner Engagement (GeoSHAPE). This mapping technology supports disaster relief by giving users the ability to create and dynamically display the locations of disaster response resources and the extent of damage in near real time.
- The Guardian Indoor Gunshot Detection System adapts military technology that identifies gunshot locations for use in schools, public spaces, and airports. The system links to smartphones and provides real-time "shots fired" information on an interactive map, helping potential victims avoid encounters with shooters and directing law enforcement to the shooter's location.
- NOAA employed a novel aerial photographic technique to conduct post-storm surveys for Hurricane Arthur. By taking photographs at an angle, the technique captures more comprehensive ground images, allowing users to document storm damage and erosion, identify hazards and effects on navigation routes, and support damage assessments.
- The DHS Office of Health Affairs (OHA) publicly released two products that provide guidance and lessons learned to the whole community on how to respond to a large-scale chemical release: (1) an abridged after-action report from the Baltimore Demonstration Tabletop Exercise; and (2) *Patient Decontamination in a Mass Chemical Exposure Incident: National Planning Guidance for Communities*.

Whole Community Accomplishments

Honolulu, Hawaii Building on the previous year's success, the second annual "Ready 2 React Whole Community Emergency Preparedness Event" provided an opportunity for over 25 city, state, Federal, and nongovernmental agencies to engage with the public to discuss preparedness activities for emergencies or disasters that may affect the island.

Galveston Bay, Texas In March 2014, as part of the whole community's response to an oil spill in Galveston Bay, over 200 volunteers supported Federal, state, and local government agencies in surveying more than 100 miles of beachfront and identifying areas and wildlife in need of cleaning.

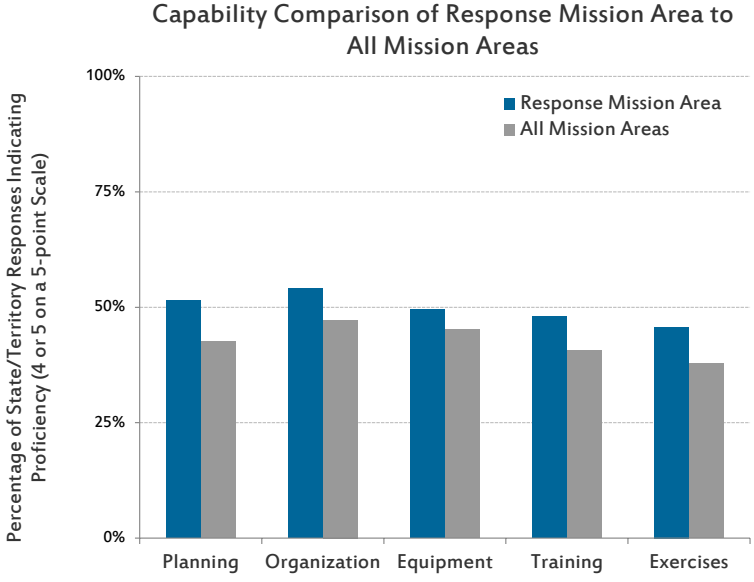
Raleigh, North Carolina The North Carolina Office of Emergency Medical Services deployed a mobile medical facility to Mississippi after Mississippi's governor requested assistance through the Emergency Management Assistance Compact.

San Francisco, California In October 2014, the City of San Francisco used Fleet Week to teach and improve whole community disaster preparedness and enhance coordination between first responders and the military for a large-scale disaster in the Bay Area. As a precursor to Fleet Week, more than 150 officials from Federal, state, and local government agencies and the military participated in a tabletop exercise focused on military support in response to a 7.8-magnitude earthquake on the San Andreas Fault.

State Perspectives on Preparedness

2014 State Preparedness Report Results

- Ratings for the Response mission area in planning, organization, training, and exercises were superior to those for all other mission areas. Equipment ratings for the Response mission area were slightly lower than for the Prevention mission area.
- Response core capabilities accounted for 6 of the 10 core capabilities with the highest self-assessment ratings.
- States and territories reported the lowest ratings for Fatality Management Services among all Response mission area core capabilities, with approximately 60 percent identifying gaps in mortuary services and body recovery.



Notes: The chart and statements do not include contributions from the three common core capabilities—Planning, Operational Coordination, and Public Information and Warning.

Response Mission Area

Key Findings

Since the release of the *National Health Security Strategy 2010–2014*, the Nation has leveraged whole community partners to make significant progress toward improving health security.

The *National Health Security Strategy 2010–2014* describes a unified national approach that facilitates collaboration among government agencies and private-sector, nonprofit, and community organizations, as well as academic and research partners, to improve the Nation's health security. In accordance with legislative requirements, ASPR reviewed and updated this strategy in 2014 with the involvement of other Federal departments and agencies and a broad array of other whole community partners. The second iteration, *National Health Security Strategy 2015–2018*, builds upon past progress, sustains the Nation's momentum, and sets the strategic direction for achieving the Nation's health security goal, which is to strengthen and sustain communities' abilities to manage incidents with negative health consequences.

The *National Health Security Strategy 2015–2018* includes a section that reflects on the Nation's progress in health security over the past five years, which centers on the following:

- **Community Resilience**: Stakeholders are increasingly incorporating initiatives to promote community health resilience (such as public outreach tools and partnerships with community organizations) into their planning and emergency response programs.
- **Public Health Emergency Medical Countermeasures Enterprise**: This interagency partnership continued to strengthen existing relationships and foster new ones across the Federal interagency and with industry partners to coordinate medical countermeasures against chemical, biological, radiological, and nuclear threats.
- **Health Situational Awareness**: Through extensive collaboration, health security stakeholders continued to develop a common understanding that informed decision-making requires situational awareness of both health- and non-health-related data.
- **Healthcare Coalitions**: There are nearly 24,000 members in Hospital Preparedness Program–supported coalitions, including 5,288 of the Nation's 6,340 hospitals. Hospitals can now communicate with other responders through interoperable communication systems; track bed and resource availability using electronic systems; protect healthcare workers with proper equipment; train healthcare workers on how to handle medical crises and surges; develop fatality management, hospital evacuation, and alternative care plans; and coordinate regional training exercises.
- **Global Health Security**: The Federal Government continued to foster new and stronger relationships with other countries to improve global health security, as part of the Nation's commitment and contribution to the Global Health Security Agenda.

In 2014, the evolving U.S. response to assist with the epidemic of Ebola virus disease in West Africa and to domestic cases demonstrated the Nation's progress in health security. The response also highlighted the need to expand such efforts, especially for managing a variety of unfamiliar, prolonged, and geographically dispersed incidents, such as emerging infectious disease threats. The *Infectious Disease Policy Report Series "Outbreak: Protecting Americans from Infectious Diseases 2014*," from Trust for America's Health, substantiates this need for protecting the health of Americans.

The Federal Government dedicated resources and personnel to support response efforts for the epidemic of Ebola virus disease in West Africa.

To help the World Health Organization and affected West African countries prevent a global epidemic of Ebola virus disease, the United States played a key role in a coordinated international public health and medical response in West Africa. The U.S. strategy has focused on containing the epidemic of Ebola virus disease in West Africa to minimize the spread of the virus. Specifically, as of December 2014, the United States deployed assets—including more than 285 personnel from CDC, over 10,000 diagnostic kits for Ebola virus disease and a field-deployable hospital from DoD, and 130,000 sets of personal protective equipment from the U.S. Agency for International Development (USAID)—to support public health and medical response operations and to provide humanitarian assistance. In addition, DoD deployed approximately 2,800 personnel to West Africa in support of USAID. The DoD missions focused on command and control, logistics, engineering, and training. DoD constructed 10 Ebola Treatment Units. At the height of the crisis, DoD provided and staffed six mobile testing laboratories in Liberia to support Liberia's national laboratory for Ebola testing. DoD also trained healthcare workers to care for patients with Ebola virus disease, and established a logistics system for countries to use. In addition, DoD is collaborating with the National Institute of Allergy and Infectious Diseases (within HHS's National Institutes of Health), the National Institutes of Health, the CDC, and the Liberian Institute for Biomedical Research to support long-term capacity development for laboratory diagnostic testing and broader biosurveillance capabilities.

Overall, U.S. response missions in West Africa include:

- Providing diagnostic testing, sample transport support, patient treatment, infection control, safe burial, traveler screening, and biosurveillance capabilities;
- Training local healthcare workers to support the response;
- Educating the local population on the facts and risks of Ebola virus disease;
- Establishing an incident management system to

Examples of the Federal Government's Response to Ebola Virus Disease in West Africa

- USAID deployed a 28-member Disaster Assistance Response Team to coordinate the U.S. response.
- USAID provided more than 16 tons of medical supplies and equipment.
- CDC assisted the government of Nigeria in coordinating the response to Ebola virus disease from the Nigeria Emergency Operations Center.
- CDC supported exit screenings at airports in West Africa.
- The U.S. Public Health Service Commissioned Corps staffed a 25-bed hospital constructed by DoD to treat healthcare workers diagnosed with Ebola virus disease.

coordinate the response to Ebola virus disease; and

- Building temporary medical care facilities to augment existing in-country medical care infrastructure.

The domestic response to Ebola virus disease identified needs to improve hospital preparedness and to continue research and development for public health and medical countermeasures.

The Ebola virus disease epidemic highlighted the need to improve hospital preparedness across the United States for contagious diseases, which can potentially result in large numbers of geographically dispersed cases. Although the Federal Government has provided technical expertise (e.g., through the CDC [Ebola virus disease] Team and the DoD Medical Support Team) and evolving guidance regarding hospital preparedness for Ebola virus disease, the capabilities of hospitals to respond to cases of Ebola virus disease and similar threats vary across the Nation.

To enhance U.S. healthcare system preparedness, HHS, in collaboration with state and local public health agencies, devised and built out a nationwide system of Ebola Treatment Centers—facilities designated by state health officials to treat a patient with Ebola virus disease safely and effectively. As of February 2015, 55 hospitals across 18 states and the District of Columbia were Ebola Treatment Centers (see Figure 9).

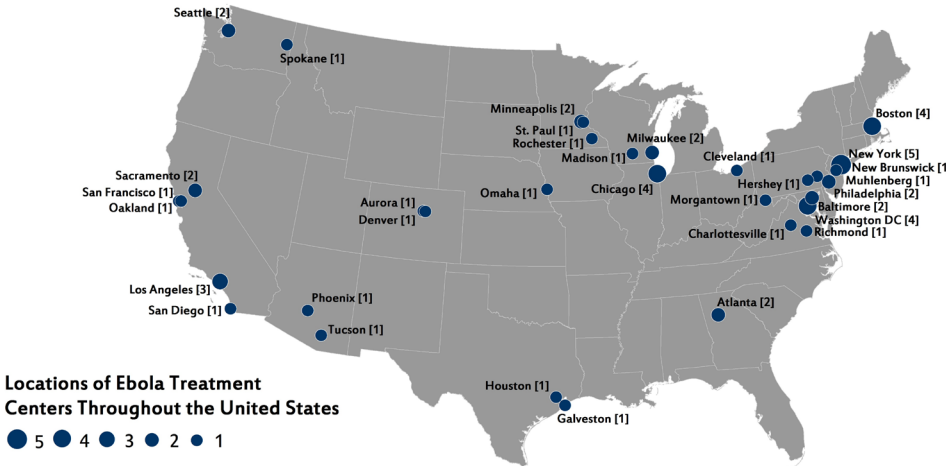


Figure 9. Fifty-five Ebola Treatment Centers exist nationwide to manage patients confirmed with Ebola virus disease.

In addition, HHS has worked with state and local public health officials to identify Ebola Assessment Hospitals; these facilities are equipped to evaluate and care for potential Ebola virus disease patients for up to 96 hours, to coordinate testing for case confirmation, and to transfer confirmed cases to a designated Ebola Treatment Center. Finally, HHS published interim guidance for all hospitals regarding possible or confirmed patients with Ebola virus disease. The guidance provides a framework for hospitals to rapidly identify patients with Ebola virus disease, immediately isolate them and inform appropriate agencies and hospital personnel, and determine needs.

Since the first domestic case of Ebola virus disease, Federal partners have also rapidly expanded Ebola-related training efforts. HHS has trained more than 675,000 healthcare workers through a combination of webinars and online training courses; these efforts also include regular calls with 10,000 nurses and 20,000 physicians and dentists, as well as outreach to emergency responders, laboratory workers, waste management workers, hospital executives, and other response personnel. Additionally, more than 8,000 responders attended live training events on infection control and personal protective

Medical Countermeasures Development

Through the Biomedical Advanced Research and Development Authority, ASPR and DoD's Medical Countermeasure Systems Joint Vaccine Acquisition Program are working to increase development of medical countermeasures using public-private partnerships. In the last two years, seven products supported by the Biomedical Advanced Research and Development Authority received FDA approval and three received Emergency Use Authorizations for prevention, treatment, or diagnosis of chemical, biological, radiological, and nuclear agents and pandemic influenza associated diseases.

equipment, with an additional 20,000 trained online. CDC has also continued to refine and disseminate guidance on adequate and effective use of personal protective equipment, including equipment from the Strategic National Stockpile. Moreover, FEMA's National Domestic Preparedness Consortium developed and conducted Ebola response training for 941 responders, with a specific focus on personal protective equipment and staffing of Ebola Treatment Units abroad. Finally, the Occupational Safety and Health Administration and CDC's National Institute for Occupational Safety and Health collaborated with Federal and state partners to develop guidance for improving Ebola preparedness for workers in various sectors (e.g., healthcare, airlines, sanitation, environmental services) who may be at risk of occupational exposure to Ebola virus disease.

The epidemic also highlighted the importance of effective medical countermeasures. The Public Health Emergency Medical Countermeasure Enterprise—an ASPR-led interagency collaborative established to combat chemical, biological, radiological, and nuclear agents through medical countermeasures—has supported extensive research and development of potential medical countermeasures for Ebola virus disease, including vaccine trials, the first of which began in September 2014 at the National Institutes of Health, and ongoing clinical trials in West Africa—conducted by the National Institutes of Health, CDC, and ASPR's Biomedical Advanced Research and Development Authority—to evaluate vaccine safety and efficacy. The National Institutes of Health, the Biomedical Advanced Research and Development Authority, and DoD's Defense Threat Reduction Agency funded research and development on vaccines and therapeutics for Ebola virus disease, including the treatment used for the first two infected healthcare workers in the United States. The Biomedical Advanced Research and Development Authority also has engaged with pharmaceutical manufacturers to expand the production of possible vaccine and therapeutic candidates to large, commercial scales. Additionally, because no approved therapies exist, FDA granted several Emergency Investigational New Drug Applications for experimental antiviral medications to treat patients with Ebola virus disease. FDA continues to work with product sponsors, manufacturers, and other interagency and international partners on clinical trial designs for both vaccines and antiviral therapies.

FDA also issued eight Emergency Use Authorizations (as of February 24, 2015) for diagnostic tests to detect Ebola virus disease, as there were no tests previously cleared for this specific purpose. DoD received the first Emergency Use Authorization on August 5, 2014, for its Ebola diagnostic test, which military-certified laboratories and more than 25 CDC Laboratory Response Network public health laboratories are using. More broadly, CDC has developed, revised, and currently maintains processes to facilitate timely and widespread access to medical countermeasures for other public health threats. These processes include the Pre-Emergency Use Authorization (submitted for FDA review prior to an emergency to expedite the review process) and the Emergency Use Authorization (submitted for FDA review during an emergency) request submissions.

Effective use of technology in disaster response relies on the public sector's ability to adapt to the growing use of mobile communication technology, implement effective processes for technological applications, and maintain necessary knowledge and expertise among system users and operators.

Recent events demonstrated the importance of the response community's ability to adapt to new technologies, such as mobile devices and social media platforms, as the public grows less reliant on traditional communication systems. For

example, in May 2014, San Diego County was unable to send emergency notifications quickly to the public during its wildfire response because the AlertSanDiego System was pre-loaded with only landline telephone numbers. The system can send alerts to mobile devices, but a subscriber must first voluntarily enroll with the system. Subsequent to the wildfire, the county noted a pressing need to increase mobile and Internet-based telephone registrations.

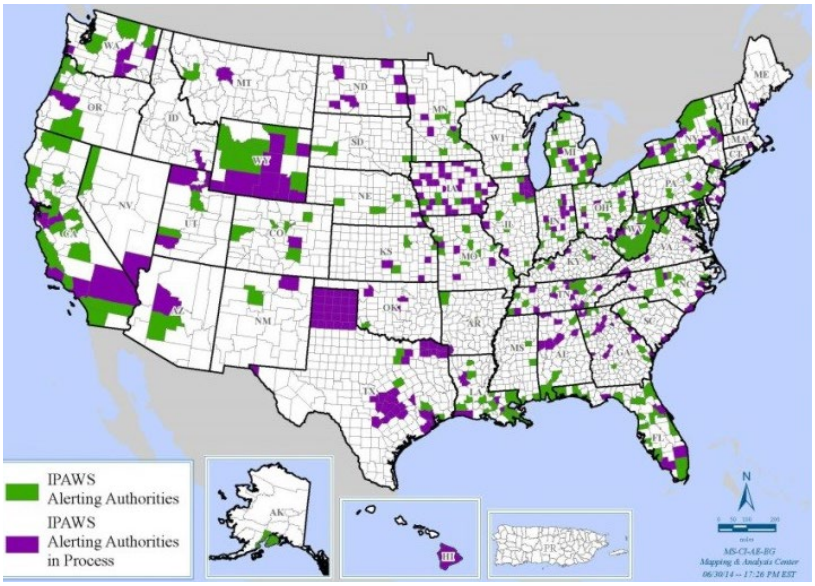


Figure 10. Alerting authorities for the Integrated Public Alert and Warning System (IPAWS) exist in almost every state and territory. These are entities that have completed the necessary authentication steps to use IPAWS.

Increasing use of mobile technology and social media provides emergency responders with more channels to communicate with the public. In 2014, FEMA worked with Federal, state, local, territorial, and tribal alerting authorities to extend the Integrated Public Alert and Warning System to 49 states, Puerto Rico, and the District of Columbia, an increase from 42 in 2013. Over 400 distinct emergency response entities have become alerting authorities (see Figure 10), an increase from 250 authorities in 2013. Since the program's inception in 2011, the National Center for Missing & Exploited Children has directly attributed the recovery of 15 children to the distribution of AMBER Alerts released through the Integrated Public Alert and Warning System. Since June 2012, the National Weather Service has used the system to distribute more than 11,000 imminent weather threat warnings, notifying citizens of tornados, flash floods, dust storms, and other extreme weather events.

Maximizing the effectiveness of technology in disaster response also requires effective processes for implementing such technology, as well as knowledgeable and skilled system users and operators. The Virtual Social Media Working Group and DHS First Responders Group report, *Using Social Media for Enhanced Situational Awareness and Decision Support*, identified several challenges to the effective implementation of technological solutions in disaster response. These include: (1) information application; (2) privacy, legal, and security issues; (3) data and open standards; and (4) technology development. Lessons learned from the national Capstone Exercise 2014 and the 2013 Colorado floods underscore the importance of providing training to users and ensuring their proficiency with response technologies. Specifically, the lack of familiarity and training with incident management tools and systems remains a prevailing gap among disaster responders.

A major cyber vulnerability prompted the Federal Government to establish new guidelines on the roles and responsibilities of Federal cyber response assets to increase the speed of response activities in government Internet domains and alerts to the public.

On April 7, 2014, the Federal Government learned of Heartbleed, a cyber vulnerability in the encryption software used to protect roughly two-thirds of the Internet. Heartbleed could allow attackers to track private keys and decrypt encrypted traffic, exposing sensitive information (e.g., passwords). Within 24 hours of learning about the vulnerability, DHS's National Cybersecurity and Communications Integration Center began working with DoD, DOJ, and the private sector to alert the public, identify vulnerabilities, and patch afflicted systems.

Cyber incident: An occurrence that actually or potentially results in adverse consequences to an information system or the data processed, stored, or transmitted by an information system

Cyber vulnerability: A characteristic or specific weakness that renders an information system open to exploitation by a given threat or hazard

Although the Federal Government's major public networks were not exposed, the unclear and overlapping roles and responsibilities in Federal cyber response delayed DHS's ability to scan government networks for the vulnerability. In response, the Office of Management and Budget issued new guidelines in October 2014 that empower DHS to conduct regular, proactive scans of Federal domain systems, enabling stronger system security and faster, more comprehensive responses to future cybersecurity incidents. The new guidelines helped to increase the number of systems that DHS proactively scans from 32 to 68 in fiscal year 2014, with efforts underway to scan approximately 120 systems by the end of fiscal year 2015. DHS also increased how often it can conduct scans by automating the process to develop and distribute post-scan summary reports.

In fiscal year 2014, the Office of Cybersecurity and Communications identified 297 cyber incidents on Federal Government networks, including Heartbleed and other high-profile cyber attacks on the White House, the U.S. Department of State, the U.S. Postal Service, and NOAA. The U.S. Computer Emergency Readiness Team took an average of 18 minutes to notify impacted agencies and sent 86 percent of agency notifications within 30 minutes. Over the same period, the team validated 87 percent of system-generated cybersecurity alerts as legitimate. The Industrial Control Systems Cyber Emergency Response Team, which works to reduce cybersecurity risk across critical infrastructure, responded to 245 incidents and 149 reported cyber vulnerabilities in fiscal year 2014.

Cybersecurity

While the Protection mission area focuses on securing the cyber environment and infrastructure from unauthorized or malicious access, use, or exploitation (see page 32 for more details), the Response mission area guides activities to save lives, protect property, and preserve vital systems after a successful cyber attack occurs.

Increases in mass shooting incidents have prompted whole community partners to conduct additional training and to revise their plans and procedures to bolster response capabilities and resources.

In 2014, FBI, in consultation with Texas State University, completed a study that found an increase in both the number and severity of active shooter events in recent years. Among the 160 active shooter events since 2000, 115 incidents (72 percent) have occurred in the last seven years. In addition, the violence and severity of active shooter events have risen sharply; for example, the average number of casualties per year has more than tripled from 35 individuals between 2000 and 2006, to 114 individuals between 2007 and 2013.

Increased concerns regarding active shooter events have highlighted the need to revise response training, plans, policies, and procedures. The "Run.Hide.Fight.® Surviving an Active Shooter Event" video—developed by Houston, Texas, with support from Federal grant programs—is a prominent public information and training video on how to survive an active shooter incident. To date, the video has received over three million views in four different languages on the official Ready Houston YouTube™ channel. Federal, state, and local governments, along with other members of the whole community, have also widely adopted the video as a tool for active shooter response training. In addition, efforts continued in 2014 to implement recommendations from "Now is the Time: The President's Plan to Protect our Children and our Communities by Reducing Gun Violence," a joint effort by the U.S. Secret Service, FBI, DHS Office of Intelligence and Analysis, and the U.S. Department of Education. Funding for "Now is the Time" expanded by $115 million to increase youth access to mental health treatment and services, a key initiative in the plan.

Recently, HHS, in collaboration with FEMA and FBI, also developed *Incorporating Active Shooter Incident Planning into Health Care Facility Emergency Operations Plans*, which offers best practices and issues for consideration to healthcare

facilities on how to plan for an active shooter incident. In February 2014, DHS OHA held a two-day meeting in which subject-matter experts and the first responder community discussed ways to improve survivability of victims and first responders in active shooter and improvised explosive device incidents. Moreover, an OHA-led interagency group is developing survivability guidance that addresses hemorrhage control, protective equipment, and response and incident management. More broadly, DHS and FBI coordinate a wide range of training and public outreach initiatives for active shooter response, in collaboration with interagency partners, first responders, and community and private-sector organizations.

The law enforcement community also began implementing lessons learned from past active shooter events. In March 2014, the Police Executive Research Forum released *Police Response to Active Shooter Incidents*, which identified recommendations based on previous active shooter incidents. The report recommended that police agencies develop dedicated active shooter response procedures, with a principal focus on immediately subduing the active shooter(s) using teams of officers. This recommended tactic encourages responding officers to engage the shooter(s), rather than waiting for Special Weapons and Tactics teams. The report also recommended that police agencies provide officers with specialized training for engaging active shooters and providing on-scene emergency medical triage. Lessons learned from the 2012 theater shooting in Aurora, Colorado, supported this recommendation, as a responding police officer with paramedic training provided initial medical triage to wounded survivors.

Joint Counterterrorism Awareness Workshop Series

The Joint Counterterrorism Awareness Workshop Series is a partnership among FEMA, the National Counterterrorism Center, and FBI to increase law enforcement preparedness for responding to and resolving terrorist attacks. The series of tabletop exercises, which are tailored to each host city, depicts a scenario similar to the 2008 Mumbai, India, terrorist attack to examine crisis response plans and law enforcement capabilities. In 2014, four workshops occurred. The workshops identified the need to: (1) integrate plans among local government and Federal, state, territorial, and tribal crisis response and emergency management responders; and (2) conduct joint training and exercises for first responders to ensure an efficient and unified response.

Agencies across all levels of government have updated emergency response plans to include the access and functional needs of individuals with and without disabilities, but implementation challenges remain.

Across the Nation, states have made progress in incorporating access and functional needs support into response planning. CDC's State Disability and Health Programs have supported 18 states in this effort, providing subject-matter experts in accessibility and response planning, who have facilitated 63 training sessions, 25 workshops, and 15 exercises. FEMA also added Disability Integration Advisors to its National Incident Management Assistance Teams, which coordinate operational planning for incident response and recovery. Disability Integration Advisors engage with and facilitate the involvement of whole community partners, including state and local disability services agencies and advocacy groups. In 2014, 37 Disability Integration Advisors deployed to 88 incidents.

While whole community partners have made incremental progress in incorporating access and functional needs into emergency response planning, barriers to implementation

remain. For example, a May 2014 National Council on Disability report documented numerous barriers to effective communication with persons with access and functional needs during an emergency. These barriers include inaccessible emergency notification systems, inaccessible evacuation maps, emergency shelters without staff able to communicate with people who are deaf or hard of hearing, and websites with emergency information that is not suited to screen-reading software applications. To address these barriers, the Federal Government and state, local, tribal, and territorial jurisdictions have increased training, modified response plans, and enhanced collaboration with disability advocates.

Accessibility Issues

Accessibility requirements are not limited to emergency response. Reports such as *Effective Communications for People with Disabilities: Before, During, and After Emergencies* emphasize the need to address physical, programmatic, and effective communication accessibility in all phases of emergency management, including mitigation and recovery. This includes ensuring that emergency management agencies understand the demographics of their community to better meet anticipated needs and address the accessibility of actionable information to access recovery programs and services such as temporary housing. Broader accessibility issues also exist, such as the availability of accessible housing for individuals after a disaster. For example, in May 2014, the U.S. Access Board—the Federal agency that promotes equality for people with disabilities and establishes formal guidelines—clarified accessibility standards for emergency mobile housing units.

While Federal agencies were able to quickly expand their capacity to transport, shelter, and care for the increase in arrivals of unaccompanied children across the U.S.-Mexico border in 2014, the response prompted Federal actions that will more seamlessly provide resources and services in the future.

In fiscal year 2014, CBP referred more than 57,000 unaccompanied children entering the country across the U.S.-Mexico border to the care and custody of the Office of Refugee Resettlement within ACF. This increase in arrivals strained both DHS's and HHS's capacities to process and care for these children, ultimately requiring temporary housing assistance for the increase. DoD temporarily housed approximately 7,700 unaccompanied children on three military installations. In addition to processing and tracking these children through appropriate systems, the Federal Government's response included expanding capacities to: transport these children; medically evaluate and treat, shelter, and care for them; and place them in the least restrictive environment with families, legal guardians, or foster care in the United States, or repatriate them to their home countries. This also included hiring additional case management staff, particularly staff fluent in Spanish.

While interagency efforts quickly expanded the Nation's capacity to manage the situation involving unaccompanied children in 2014, the Federal response revealed an underlying need for greater programmatic agility to quickly open facilities to shelter and care for these children, as existing HHS shelters and CBP temporary holding facilities were rapidly overwhelmed. In response, ACF significantly expanded national shelter capacity for unaccompanied children. Moreover, the Executive Branch has enhanced the Federal Government's capabilities and coordination mechanisms for managing this case load. On June 2, 2014, the President launched an initiative to unify efforts among Federal agencies for addressing the situation. Specifically, this initiative directed the DHS Secretary to establish an interagency Unified Coordination Group to assist the coordination and use of response assets from across the Federal Government, including ongoing Federal planning to manage future situations involving unaccompanied children.

Government and whole community partners continue to implement lessons learned and develop innovative approaches for improving response capacities in lifeline sectors, particularly the energy and transportation sectors.

The Nation continued to make progress toward sustainment and rapid restoration of lifeline sector services for disaster response. These lifeline sector services—primarily energy, water, transportation, and communications—underpin the operation of nearly every business sector, community, and government agency.

Recent Federal, state, and private-sector initiatives in the energy sector include the following:

- In June 2014, DOE established the Northeast Gasoline Supply Reserve. The reserve holds one million barrels of gasoline and can help mitigate the impacts of sudden, unexpected supply interruptions. Similarly, the New York State gasoline reserve, launched in October 2014, is the first state-based strategic gasoline reserve and serves as an emergency stockpile to provide replacement supplies when gasoline supplies are interrupted.
- GridEx II, conducted November 2013, is the largest and most comprehensive energy grid security exercise to date. The after-action report for the exercise, published in March 2014, recommended that energy-sector stakeholders continue to enhance information sharing, improve incident coordination, and clarify roles and responsibilities for developing situational awareness.
- The Environment for Analysis of Geo-Located Energy Information, a web-based tool developed by DOE, enables real-time sharing of power and natural gas infrastructure statuses during emergencies. The tool now covers 72 percent of all domestic electricity customers, and more than 20 Federal agencies and 14 Federal Emergency Operations Centers use the tool to monitor energy infrastructure to better coordinate emergency response and recovery.

Notable Shale Crude Oil Incidents in 2014

- January 2014, New Augusta, Mississippi: A train transporting crude oil from North Alberta, Canada, to a Gulf Coast refinery derailed, spilling 50,000 gallons of product.
- February 2014, Mississippi River: A barge collision spilled over 30,000 gallons and closed 65 miles of river.
- April 2014, Lynchburg, Virginia: A train derailment in the downtown area caused an explosion and resulted in a 17-mile oil slick on the James River, a major tributary of the Chesapeake Bay.

In the transportation sector, production of domestic shale crude oil continues to increase demands on rail transportation. Quantities of shale crude oil transported by rail surpassed one million barrels per day in 2014. For comparison, U.S. railroads moved only 9,500 cars of shale crude oil in 2008, but more than 200,000 in the first seven months of 2014 alone—more than eight percent of the country's oil production. The possibility of train derailment, crude-related transportation incidents, and oil spills poses not only a threat to transportation-sector reliability, but also to the safety, health, and environmental wellbeing of the communities those railcars traverse.

In response, government and private-sector partners are continuing to develop and conduct emergency response training and exercise programs specific to shale crude oil. FEMA's National Exercise Division held planning meetings

Crude by Rail Emergency Response Training

An agreement between DOT and the American Association of Railroads requires rail carriers to subsidize the training course on responding to rail incidents involving shipments of crude oil. In 2014, more than 1,500 first responders completed the three-day course, which takes place in a field-based setting. The course provides practical training using rail cars and addresses response tactics, including firefighting foam application, and the environmental impact of crude oil-related incidents.

and conducted research and development of an exercise toolkit focused on crude-oil rail incidents. The toolkit—named "Operation Safe Delivery" and developed by DOT in collaboration with other Federal departments and agencies—will debut through a series of exercises in early 2015. To support training, the U.S. Fire Administration also reached out to over 400,000 firefighters through electronic mailing lists and social media to share best practices and safety information for responding to oil-related incidents. Additionally, the National Response Team, a multi-agency Federal coordination entity under the National Oil and Hazardous Substances Pollution Contingency Plan, worked with Canadian partners and delivered Bakken Crude Oil First Responder Awareness training to more than 300 responders at all levels of government. In May 2014, Federal Railroad Authority issued an emergency order requiring rail carriers to provide State Emergency Response Commissions with information on the number of trains, descriptions of products, emergency response information, and routing data for trains carrying more than one million gallons of shale crude oil. Finally, the private sector is actively striving to improve rail safety for oil transportation. Training initiatives include the Safety Train and Crude by Rail training programs, which began in May and July 2014, respectively.

While the transition to Next Generation 9-1-1 will augment emergency response capabilities, the uneven implementation of adopted standards and best practices for Next Generation 9-1-1 threatens its reliability.

Next Generation 9-1-1 is an Internet Protocol–based system that offers several benefits over traditional 9-1-1 systems, including the ability to transmit digital information (e.g., text, photo, and video) and receive real-time location information from mobile devices. Next Generation 9-1-1 also offers more resiliency and redundancy than traditional 9-1-1 systems. Given the ubiquity of Internet Protocol technology—as well as migration of emergency responders to broadband networks—Next Generation 9-1-1 is increasingly important for effective emergency response. As the Nation continues to transition to Next Generation 9-1-1, the Federal Communications Commission (FCC) noted that a seamless transition requires a broad understanding among all stakeholders on the status of Next Generation 9-1-1 deployment.

Next Generation 9-1-1 offers significant long-term benefits, but the transition carries significant risks. These risks are attributable to jurisdictions' lack of experience with the types of procurements necessary to operate Next Generation 9-1-1 systems, evolving governance structures, unstable 9-1-1 funding, high costs associated with transitioning to Next Generation 9-1-1 systems, and the need to coordinate with larger and different groups of public and private stakeholders. In January 2014, DOT's National Highway Traffic Safety Administration identified and reviewed Next Generation 9-1-1 standards and found limited coordination among Next Generation 9-1-1 stakeholders for developing and adopting such standards. For example, while the National Emergency Number Association provides functional, interface, and cybersecurity standards for next generation systems, gaps remain in identifying best practices among next generation system stakeholders and in the adequacy of reliability and security standards associated with evolving network threats.

FCC Adopted Rules to Increase Next Generation 9-1-1 Reliability

- December 2013: Adopted rules requiring 9-1-1 service providers to certify annual implementation of industry-backed best practices or acceptable alternative measures
- November 2014: Adopted rules requiring 9-1-1 service providers to report major disruptions to 9-1-1 operators within 30 minutes of discovering an outage
- November 2014: Approved notice of proposed rulemaking to expand 9-1-1 provider certification rules and create a group of lead 9-1-1 providers with coordination responsibilities in the event of an outage

Another challenge with Next Generation 9-1-1 is that integration with legacy systems can result in incompatibilities, compromising emergency response efforts. A multistate 9-1-1 outage in April 2014 demonstrated this risk. As critical 9-1-1 functions from two locations were combined, a software coding error at the consolidated Next Generation 9-1-1 call-routing facility in Colorado stopped the system from directing calls to 81 9-1-1 call centers across seven states. This led to interruptions in services to over 100 million people for up to six hours. This outage affected significantly more

people than a traditional 9-1-1 system outage would. In November 2014, FCC launched a proceeding to address gaps in 9-1-1 and Next Generation 9-1-1 governance. FCC has also adopted additional rules to ensure industry adherence to network best practices in efforts to support Next Generation 9-1-1 implementation and improve 9-1-1 system reliability and resiliency.

The First Responder Network Authority (FirstNet) continues to make progress in establishing a dedicated nationwide public safety broadband network, though challenges remain.

The *Middle Class Tax Relief and Job Creation Act of 2012* established FirstNet as an independent authority within the National Telecommunications and Information Administration to ensure the building, deployment, and operation of a nationwide, high-speed network dedicated to public safety. During disasters, this broadband network will enable responders at local, state, regional, and Federal levels to communicate and exchange data.

Numerous challenges exist for implementing the first-ever nationwide public safety broadband network, including its long-term financial self-sustainability. Although FirstNet will likely receive the full $7 billion congressional allocation provided in the *Middle Class Tax Relief and Job Creation Act of 2012*, the cost of deploying the network is expected to significantly exceed this initial funding. FirstNet intends to partner with entities to help offset the costs of constructing and operating the nationwide public safety broadband network, and can lease excess network capacity and collect user fees to help sustain the network.

In 2014, FirstNet made progress in planning for the deployment of the nationwide public safety broadband network. It issued its first public notice addressing key statutory issues and initiated a consultation process aimed at informing FirstNet's plans for deployment of the network. *The Middle Class Tax Relief and Job Creation Act of 2012* requires FirstNet to develop plans for each state and territory for the deployment of the network, as informed, in part, by ongoing consultations. As of February 25, 2015, FirstNet had submitted initial state consulting packages to all 56 states and territories; held pre-consultation conference calls with 52 states and territories; received initial consultation checklists from 47 states and territories; and completed 15 state consultations. In Spring 2015, FirstNet management will release a Special Notice requesting comments on draft request for proposal documents that detail key terms, as part of its ongoing consultation efforts and market research with industry. A final solicitation is targeted for late 2015/early 2016. Additionally, DHS Office of Emergency Communications has worked with states and territories to incorporate broadband planning into their strategic plans for enhancing interoperable and emergency communications by offering technical assistance and helping states and territories identify near- and long-term plans for preparing for the nationwide public safety broadband network.

Mission Area Overview

Recovery

Focused on a timely restoration, strengthening, and revitalization of the infrastructure; housing; a sustainable economy; and the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident

Highlights

- Federal agencies are improving their ability to support recovery under the *National Disaster Recovery Framework,* but staff awareness and abilities for conducting collateral duties remain challenges. (p. 67)
- The Housing and Infrastructure Systems core capabilities have experienced limited progress and remain national areas for improvement. (p. 69, 71)
- The Federal Government modernized its process for reviewing environmental and historic preservation requirements for large-scale projects addressing infrastructure recovery. (p. 72)
- Whole community partners are developing new information-sharing tools to support community recovery. (p. 74)

Frameworks in Action

The *National Disaster Recovery Framework* (the Recovery Framework) identifies the process for jurisdictions affected by disaster to achieve effective and timely recovery. The Recovery Framework includes 90 pre- and post-disaster activities. Nine core principles guide the Recovery Framework. These principles are: individual and family empowerment; leadership and local primacy; pre-disaster recovery planning; partnerships and inclusiveness; public information; unity of effort; timeliness and flexibility; resilience and sustainability; and psychological and emotional recovery.

Colorado adopted three core principles from the Recovery Framework—pre-disaster recovery planning; resilience and sustainability; and psychological and emotional recovery—to successfully recover from historic flooding that occurred in September 2013. Approximately 17 inches of rainfall resulted in the most severe flooding disaster in decades for the central and eastern regions of Colorado. Despite the extensive scale and scope of the damage, local officials were prepared to manage the disaster recovery effort. Prior to the flood, Colorado had developed a statewide Disaster Recovery Framework that pre-identified 13 recovery functions along with the state agencies that coordinated each function. This planning effort—modeled after the Recovery Framework—identified stakeholders' roles and responsibilities, and short- and long-term recovery strategies. When the disaster occurred, state agencies were able to coordinate quickly with Federal and local counterparts to implement recovery support in the field.

Core Capabilities in the Recovery Mission Area

- Economic Recovery
- Health and Social Services
- Housing
- Infrastructure Systems
- Natural and Cultural Resources
- Operational Coordination
- Planning
- Public Information and Warning

Colorado's recovery efforts also emphasized the Recovery Framework's core principle of resilience and sustainability. The Colorado *Recovery Support Strategy*—developed by Federal, state, and local partners—included hazard mitigation activities to help local communities become more resilient to future disasters. These longer-term activities included floodplain management, riverbank realignment, and resilient infrastructure and housing construction.

The psychological and emotional recovery core principle has appeared since the beginning of Colorado's recovery activities. The 2013 flood damaged more than 17,000 homes and affected thousands of livelihoods. Recognizing that disasters have more than physical consequences, Colorado officials, with support from FEMA and HHS's Substance Abuse and Mental Health Services Administration (SAMHSA), provided counseling and disaster case-management programs to address the mental health needs of affected communities. For example, Colorado and SAMHSA activated disaster-related distress helplines that provided immediate crisis counseling to survivors. In Boulder County, the local flood-recovery group distributed a bilingual resource guide to survivors on flood recovery that highlighted available mental health services and resources. For individuals with financial limitations, the group implemented a voucher program to help flood survivors receive mental health and counseling services. By summer 2014, the group distributed more than 200 vouchers to families and individuals in the community. These core recovery principles are helping to facilitate a lasting, holistic recovery for the affected communities.

By the Numbers

$80 million — In 2014, the U.S. Department of Commerce's (DOC's) Economic Development Administration (EDA) invested nearly $80 million for economic-development activities related to recovery and resilience.

6,248 loans — In fiscal year 2014, SBA approved 6,248 loans totaling $333 million to help businesses, homeowners, and renters recover from disasters.

930 museums and collections institutions — From 2007 to 2014, the Western States and Territories Preservation Assistance Service helped 930 museums and collections institutions develop disaster preparedness and recovery plans.

Resilience Innovations

- FEMA, HHS, and the DHS Coastal Hazards Center of Excellence collaborated with the University of North Carolina to develop a tool that tracks disaster recovery progress based on 79 metrics.
- EPA added an improved user interface and other features to I-WASTE, a secure web-based tool that helps communities manage waste resulting from natural and manmade disasters, including chemical, biological, radiological, and nuclear incidents.
- DoD developed the Tactical Dynamic Operational Guided Sampling tool, which reduces the time required to characterize a hazard area and recover from a biological event in an urban area by mapping data from sampling teams and tracking laboratory results in near real time.
- USGS developed new tools to assess disaster consequences and facilitate recovery and rebuilding strategies along coastal communities, including developing monitoring networks for storm surge, tracking contaminant dispersion, and determining the impacts of wetland inundation.

Whole Community Accomplishments

Rockefeller Foundation The Rockefeller Foundation selected six additional U.S. cities—Boston, Chicago, Dallas, Pittsburgh, Tulsa, and St. Louis—to join its 100 Resilient Cities Challenge, an initiative aimed at making major cities more resilient and better able to recover from disasters. The foundation provides support to selected cities to create a strategic plan, develop local leadership, and access innovative tools and networks.

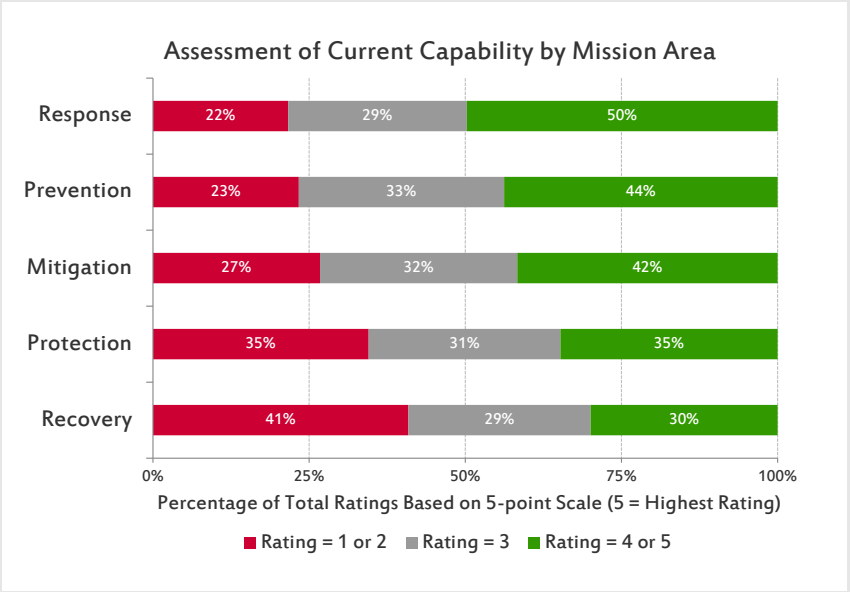
American Red Cross After the March 2014 mudslide tore through a neighborhood in Snohomish County, Washington, the American Red Cross deployed more than 500 volunteers, opened emergency shelters, and provided food and other assistance to survivors. The American Red Cross has pledged hundreds of thousands of dollars for emergency relief, recovery support, and preparedness efforts in the affected communities—including funds for local nonprofit organizations. This funding is supporting mental health services; a food bank; repairs to the damaged community center; an emergency preparedness program for local schools; and casework efforts to assist survivors with health and social services, and housing.

Libraries, Museums, and Other Collections Institutions Over 4,300 cultural and civic institutions have used dPlan—an online toolkit for disaster planning supported by the Institute of Museum and Library Services—to create emergency preparedness and recovery plans.

State Perspectives on Preparedness

2014 State Preparedness Report Results

- States and territories reported some of the lowest levels of capability in the Recovery mission area. Economic Recovery, Housing, and Natural and Cultural Resources were among the bottom-five of all 31 core capabilities.
- Twenty-one states and territories reported not having complete or up-to-date plans for any Recovery core capability. Seven states and territories do not have a plan or annexes for Housing and Natural and Cultural Resources.
- Fourteen states and territories reported that they have not exercised the Housing core capability in the past five years and 15 states and territories have not exercised the Natural and Cultural Resources core capability in the same timeframe.



Notes: The chart and statements do not include contributions from the three common core capabilities—Planning, Operational Coordination, and Public Information and Warning. Due to rounding, some percentages may total slightly more or slightly less than 100 percent.

Recovery Mission Area

Key Findings

Federal agencies have yet to adequately familiarize their personnel on the Recovery Framework, but some are taking steps to address challenges in coordinating and delivering recovery support.

The Recovery Framework seeks to optimally engage existing Federal resources and authorities to better assist disaster-affected communities. In practice, this centers on how Federal agencies can adapt, pivot, and apply their existing programmatic resources (e.g., funding, technical assistance, staff time) for disaster recovery, which in turn relies on the ability of their personnel to facilitate these transitions effectively.

An initial challenge is familiarizing personnel with the roles, responsibilities, and coordinating mechanisms of the Recovery Framework. Without this awareness, staff assigned to coordinate multi-agency efforts may struggle to comprehend the full scope of their mission and only consider solutions from the perspective of their specific agency's equities and not those of other organizations. Moreover, shifting personnel from daily operations to support recovery operations may require agencies to identify agency-specific competencies for recovery, which can be challenging due to the inherent variability of disasters. The absence of identified competencies hinders the ability to pre-identify appropriate staff, even in cases in which doing so would be beneficial. For example, agencies such as FEMA, USACE, DOC, SBA, and USDA currently rely on existing permanent staff at the regional- or district-level to support long-term recovery. However, these staff members possess uneven levels of awareness and experience in supporting and applying their resources for disaster recovery. Without personnel adequately prepared with a working knowledge of the Recovery Framework and capable of conducting specific collateral duties, agencies limit their ability to plan ahead and risk exacerbating disruptions to daily operations while supporting recovery operations.

This issue becomes particularly pronounced when staff members are called to perform key leadership positions as a Recovery Support Function coordinating agency. A recent recovery-focused exercise highlighted a distinct advantage of staff that had prior experience and expertise in leading and coordinating recovery activities. This observation further impresses the need among Recovery Support Function coordinating agencies to investigate steps to ensure staff leading recovery activities are effectively prepared to fully implement recovery missions and engage the whole community.

Federal agencies are continuing to familiarize staff that serve key coordinating roles with the Recovery Framework and are exploring flexibility within their programs to better support recovery activities when needed. Examples include the following:

- SBA formally established a Disaster Preparedness and Operations Team in 2014 to provide training for district offices, as well as connections to trained, headquarters-based personnel to help communities with the multifaceted recovery of

small businesses affected by disaster. This is distinct from SBA's longstanding reserve force, which is maintained by the Office of Disaster Assistance and is trained specifically to provide disaster assistance loans (often a key first step in homeowner and small business recovery).

- In 2014, USACE developed and delivered training to all USACE field coordinators on their roles, responsibilities, and associated tasks during a recovery deployment.
- DOC is developing a cadre of trained professionals based on its executive development and professional development programs.
- The National Weather Service trained its first cadre of hydrologists to provide meteorological and hydrological expertise in support of landscape recovery following wildfires, and dispatched these specialists to support several incidents in 2014.
- HHS has five permanent, headquarters-based coordinators who can provide guidance and direction remotely, but who are also pre-designated to deploy to assigned geographic regions to staff Health and Social Services Recovery Support Function activations, if necessary.
- FEMA trained and appointed permanent Federal Disaster Recovery Coordinators in all 10 of its regional offices in 2014, establishing a permanent recovery support network nationwide for the first time.

Despite these advances, effectively managing staff resources to pivot from daily operations to long-term recovery operations for a major disaster remains a challenge.

The Federal Government developed new guidance and policies to more effectively define and deliver recovery support, but a major recovery exercise identified several remaining areas for improvement.

The Federal Government made progress throughout 2014 in formalizing coordinating structures and internal guidance to help communities recover from disasters. In February 2014, Federal agencies approved a charter for the Recovery Support Function Leadership Group, the senior-level entity that coordinates responsibilities and resolves operational, resource, and preparedness issues relating to interagency recovery activities at a national level. The charter formalized recovery coordinating processes and designated lead officials from each agency to streamline the group's decision-making authority. In addition, HHS released two concepts of operations for disaster behavioral health and human services in 2014. These documents provide detailed guidance on how agencies will work together to support state and local recovery efforts.

In 2014, FEMA also revised formal guidance on the timeframes for mission assignments to more accurately reflect the longer operational periods typically needed for recovery. FEMA uses mission assignments to reimburse other Federal agencies for supporting disaster response and recovery activities during a presidentially declared disaster. The new guidelines extend the timeframe necessary to complete mission assignments to up to two years, permitting agencies to undertake longer-term recovery support activities more easily. FEMA also updated its Donated Resources Policy in 2014 for Public Assistance Emergency Work, significantly expanding the resources that count toward the requirement for grant recipients to match up to 25 percent of grant dollars by allowing donated resources and services from voluntary organizations to be included.

Although post-incident activations of Recovery Support Functions continue to be the primary manner in which state and local leaders practically apply the principles in the Recovery Framework, Federal efforts to familiarize states with the Recovery Framework are expanding. FEMA redesigned the format for its National Disaster Recovery Framework Leadership Workshop to convene local-, state-, and regional-level Federal staff in a collaborative, seminar-style learning environment. Two of the 10 FEMA Regions held the workshop in 2014. Additionally, six states received briefings from FEMA on the Recovery Framework in 2014. Other training resources targeting state, local, tribal, and territorial levels

include two courses offered by the Emergency Management Institute to better prepare state and local recovery planners. While training efforts focused on the Recovery Framework have expanded, limited technical assistance exists to help state and local jurisdictions address recovery planning and capability gaps.

Silver Phoenix, a participant-led tabletop exercise that was part of the National Exercise Program Capstone Exercise 2014 series, helped Federal partners identify several ways to strengthen recovery support. For example, Health and Social Services Recovery Support Function agencies prioritized activities for maintaining services to displaced populations and re-establishing critical health and social services facilities. The exercise also highlighted additional Federal programs that might be beneficial for recovery, prompting a discussion of pre-disaster coordination. Additional coordination challenges identified during Silver Phoenix include using supplemental appropriations efficiently and effectively in tandem with existing budgets and authorities, and improving collaboration among all levels of government to accurately share information on ongoing recovery operations.

Structural challenges have prevented the whole community from making more progress in comprehensively addressing housing needs of disaster survivors.

Disaster housing has been an acknowledged area for improvement since Hurricane Katrina in 2005. While performance has improved since then, Hurricane Ike in 2008 revealed continued coordination difficulties, and a specific recommendation from the Hurricane Sandy Rebuilding Task Force four years later indicate that room for progress remains. As outlined in Table 4, numerous structural challenges continue to hinder the ability of whole community partners to fully address the housing needs of disaster survivors from response through long-term recovery.

Challenge	Description
Transitions across housing phases	A variety of Federal agencies and whole community partners lead distinct phases in housing recovery, but transitions between these phases and their associated programs are not well defined. The American Red Cross and other nonprofit organizations often provide immediate sheltering assistance prior to the arrival of Federal support. If needed and requested by a state, FEMA's Transitional Shelter Assistance Program can provide support between temporary shelter and interim housing. Once authorized, FEMA can also provide temporary housing to eligible individuals and households for up to 18 months, which can be extended under extraordinary circumstances. After this period, displaced individuals must find long-term housing solutions, which may take many years to fully address, due to obstacles such as a lack of affordable rental units.
Funding variability	HUD uses supplemental funds that Congress approves as needed for the Community Development Block Grant Disaster Recovery Program to support disaster housing. The approval processes and disbursement of these funds can unfold over several years, and the amount of supplemental funds can vary greatly from one disaster to the next. These funds do not always address the full range of housing needs, which sometimes require disaster survivors to seek further support from other programs or resources.
Influence of early decisions	Given the complex legal, administrative, and logistical requirements of different housing options, decisions made in early phases of a disaster response can affect available housing options in subsequent phases. As a result, some housing solutions may not be viable in later stages.
State capabilities, resources, and competing priorities	Many states lack the resources and expertise necessary to manage and implement a large-scale disaster housing operation, particularly one that stretches over a long period. State leaders may also have other recovery priorities, limiting resources for federally recommended planning and assessment efforts after a disaster. For example, some states do not appoint state-led disaster housing task forces to coordinate state, Federal, and private-sector efforts.

Table 4. Structural issues impede progress in meeting housing needs of disaster survivors.

Reflecting these challenges, 2014 State Preparedness Report results indicate that the Housing core capability remains among the lowest-scoring core capabilities for the fourth year in a row. Only 26 percent of responses fell into the top-two rating categories (i.e., a 4 or 5). Sixty percent of states and territories reported low levels of training for the Housing core capability (see Figure 11). In addition, more than half of responses from states and territories identified addressing housing shortages (57 percent), conducting housing assessments (57 percent), and rehabilitating damaged housing (52 percent) as remaining gaps for the Housing core capability. Forty-two percent of states and territories believed that the responsibility for addressing remaining capability gaps in Housing was mostly or entirely Federal, which was second-highest among all 31 core capabilities.

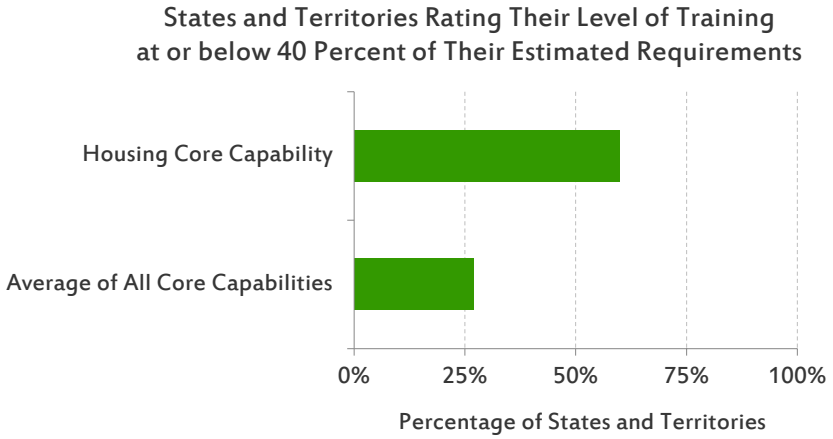


Figure 11. More than twice as many states and territories reported low levels of training proficiency for Housing than the average for all 31 core capabilities.

Federal efforts to address persistent gaps in disaster housing have been modest. Limited formal training courses in disaster housing exist for state and local officials. To date, the most comprehensive disaster housing guidance available is the Catastrophic Housing Annex to the *2012 Federal Interagency Operational Plan – Hurricane*. FEMA began updating the annex in 2014 so that whole community partners could apply the processes, options, and programs it describes to other hazards. FEMA also developed templates to assist states in creating state-level housing plans and disaster housing strategies. These documents help states identify key information, such as building codes or zoning laws, that Federal agencies need from states to develop housing assistance options. In August 2013, the Sandy Rebuilding Task Force directed Federal agencies involved in disaster housing to provide new policy recommendations for improving disaster housing coordination from response through long-term recovery. These efforts are still in progress.

Preparedness Case Study:

Disaster Housing Prototype for Urban Areas

Limited housing stock and land availability can complicate the provision of post-disaster housing for survivors in large metropolitan areas. A New York City pilot program of a new manufactured home design addresses disaster housing limitations in densely populated urban areas. The prototype can accommodate several families in a single, multi-story building. USACE provided support for the assembly of the prototype in Brooklyn, New York, in April 2014 and will leave it in place for one year to learn more about the logistical and administrative challenges of rapidly deploying manufactured housing units inside the city.

Limited investment capacity among the whole community hinders progress in strengthening the resilience of the Nation's infrastructure systems.

The ability of communities to recover quickly from a disaster depends, in part, on the resilience of their critical infrastructure, particularly lifeline sectors such as transportation and drinking water systems. Recent assessments identify significant investment demands to maintain and improve these systems:

- In February 2015, DOT publicly released a draft of *Beyond Traffic: Trends and Choices 2045*, which notes that current public revenues to support transportation are insufficient to address the rising costs of maintaining existing infrastructure and adding new capacity to meet future transportation needs.
- In 2013, EPA's *Drinking Water Infrastructure Needs Survey and Assessment* reported that the Nation needs more than $384 billion in infrastructure projects from 2011 to 2030 for water systems to continue to provide safe drinking water to the public.
- The 2013 *Report Card for America's Infrastructure*, the latest installment of a national assessment of infrastructure that the American Society of Civil Engineers publishes every four years, gave the Nation's transportation and drinking-water infrastructure "Mediocre" and "Poor" ratings, respectively.

The Federal Government has a difficult challenge in prioritizing and optimizing limited public resources to bolster infrastructure capacity. The costs to repair or replace large-scale infrastructure typically exceed the capacity of any one stakeholder. For example, DOT estimates that an annual investment of between $85 and $177 billion is necessary to strengthen the Nation's transportation sector; the low end of the range would prevent further degradation of the infrastructure, but would result in little or no improvement. Improvement would require investments closer to the upper estimate.

Federal partners are exploring public-private partnerships and innovative monitoring capabilities to help increase the resilience of infrastructure. In September 2014, the White House hosted the Infrastructure Investment Summit to advance public-private partnerships. The summit brought together over 100 government and private-sector leaders who announced their intent to commit more than $50 billion for U.S. infrastructure over the next five years. Additionally, NIST showcased innovative infrastructure-monitoring technologies from academia and the private sector in March 2014. Examples included self-powering, wireless sensors that continuously monitor bridge integrity, and unmanned aircraft systems that provide high-quality structural surveillance. Through improvements in monitoring infrastructure, the whole community can better identify and prioritize needed maintenance and repairs and make more efficient use of resources.

The Federal Government has established new approaches to coordinate large-scale infrastructure recovery projects and modernize Federal review processes.

In 2014, the Federal Government pioneered a new approach for managing large-scale infrastructure projects in the Sandy-affected region by establishing the Sandy Regional Infrastructure Resilience Coordination Group (Coordination Group). This group is enhancing regional resilience by coordinating more than $18 billion in Federal infrastructure investments appropriated under the *Disaster Relief Appropriations Act, 2013* across more than 400 projects. To help manage this effort, the Coordination Group created a repository of key information on these projects in order to promote interagency information sharing. The Coordination Group has used this information to map and identify all projects taking place within particular geographic areas (see Figure 12) and enhance coordination of Federal support and funding. The group also established 10 Technical Coordination Teams of local, state, and Federal officials to facilitate planning, development, and implementation of planned and proposed infrastructure projects in the affected jurisdictions. The teams' success in improving interagency coordination led the Sandy Recovery Office to develop a charter for each team that formalizes its structure and approach, including tools for future large-scale infrastructure recovery and resilience efforts.

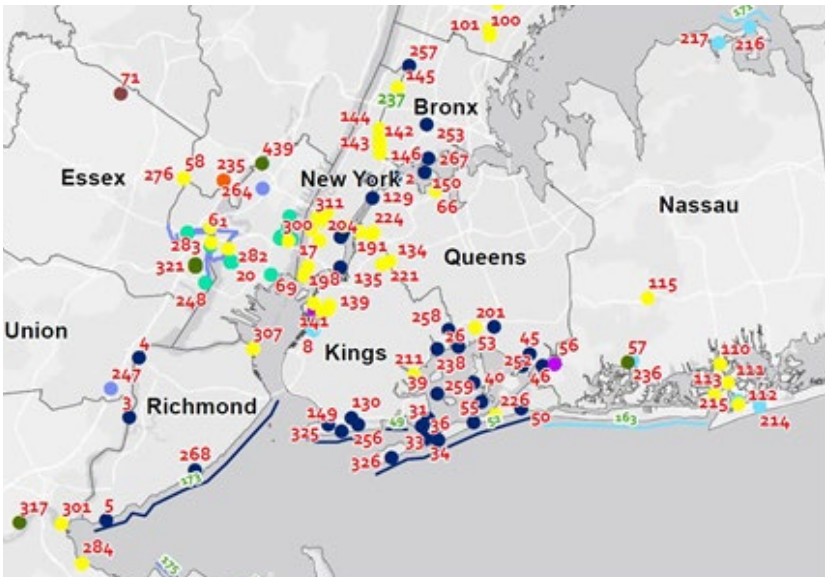
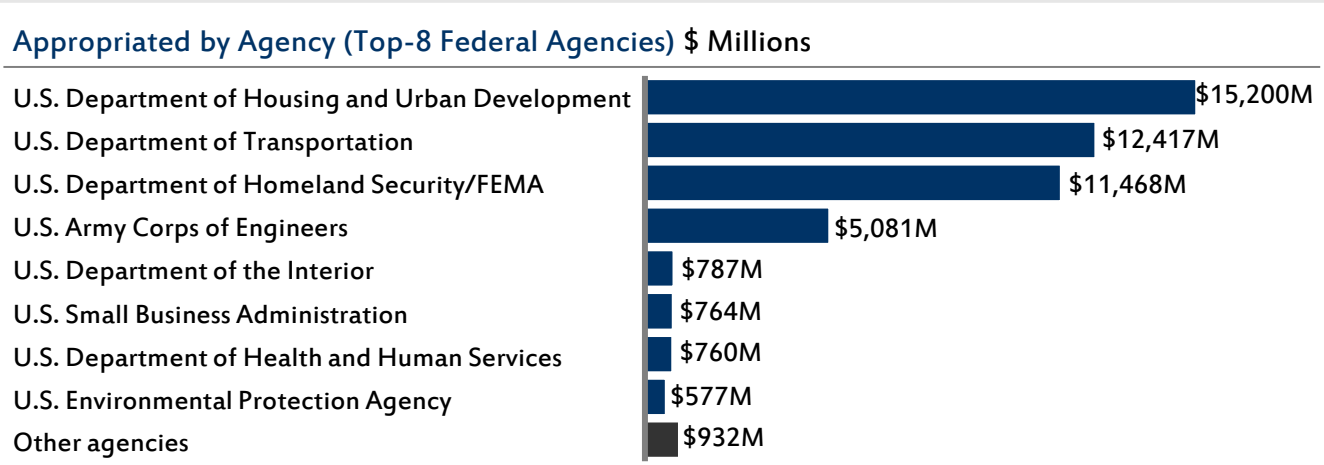


Figure 12. The Sandy Regional Infrastructure Resilience Coordination Group assigns project numbers and color markings to distinguish among the numerous infrastructure projects it monitors in the New York City area.

Federal initiatives are also updating the permitting and compliance review process for disaster recovery projects. Large-scale interagency infrastructure projects can face complex legal reviews to ensure compliance with environmental and historic preservation requirements from multiple Federal agencies. During this process, different agencies may need to review the same data, leading to duplication of effort and project delays. In July 2014, 11 Federal agencies approved the Unified Federal Review process to streamline environmental and historic preservation reviews for disaster recovery projects. FEMA and the U.S. Fish and Wildlife Service implemented an early version of the Unified Federal Review process in New Jersey after Hurricane Sandy. In just 90 days, the two agencies identified 825 project actions that met existing multi-jurisdictional environmental requirements, providing a quick and efficient review of important recovery projects for New Jersey.

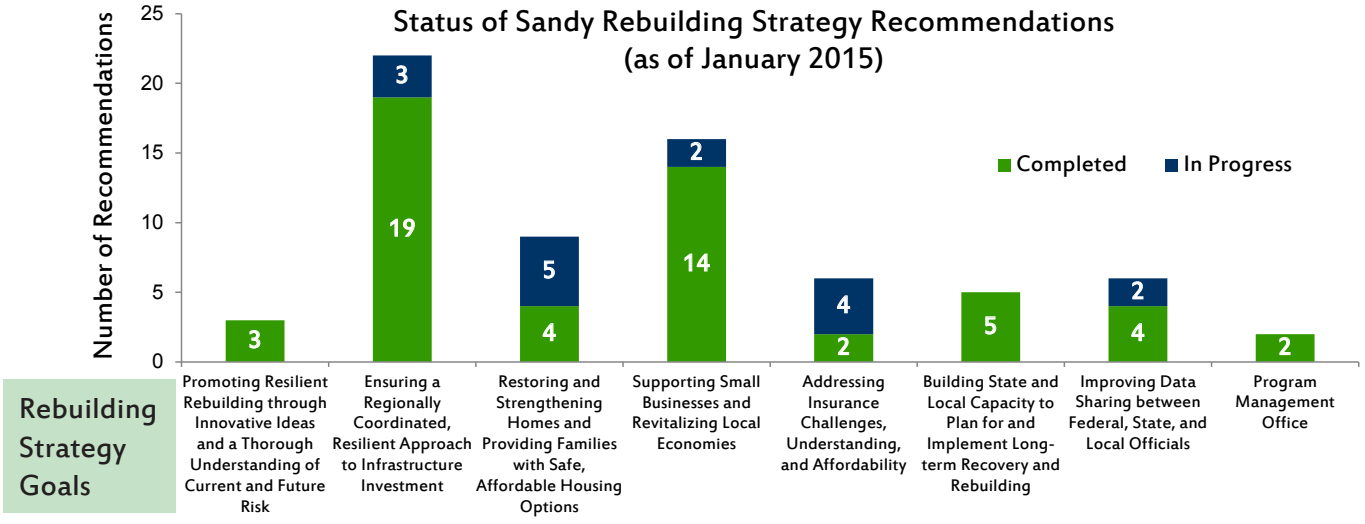
Hurricane Sandy: The First Large-scale Implementation of the Recovery Framework

Congress appropriated more than $47 billion to 19 Federal agencies across more than 65 programs.



Of the 69 recommendations in the *Hurricane Sandy Rebuilding Strategy*, 53 (77 percent) are complete, and 16 are in progress, many of which are long-term by design.

The Sandy Program Management Office served as a centralized source of information on the status of Hurricane Sandy recovery funding. The office developed a new toolkit—including guidance on interagency tracking—to help agencies adapt key functions for future large-scale disasters and cross-agency supplemental appropriations.

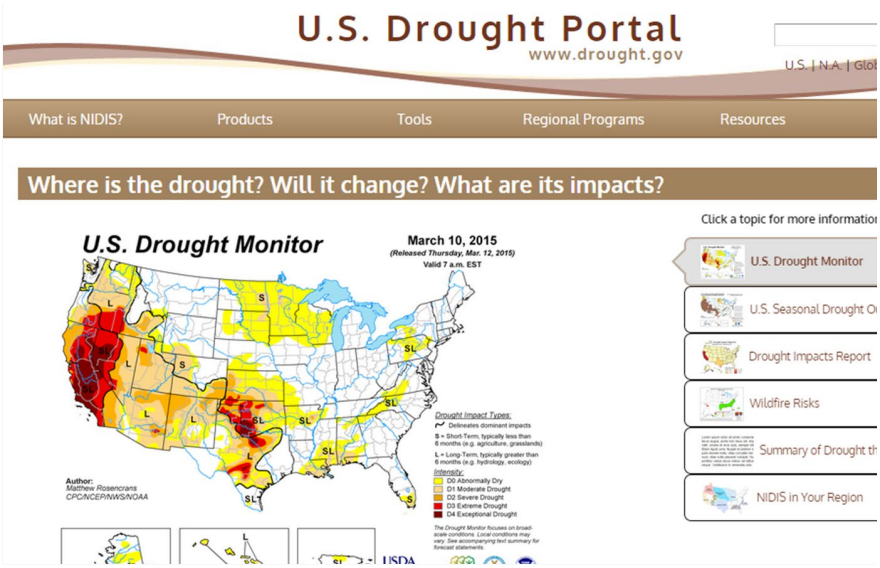


Federal agencies and nongovernmental organizations are developing new information-sharing resources and improving existing systems to facilitate state and local recovery efforts.

Federal and nongovernmental organizations are collaborating to develop new information-sharing resources for recovery efforts. Examples of such innovations include the following:

- **Disaster Assessment and Assistance Dashboard**: An online platform for citizens, businesses, and governments to map nearby environmental hazards, share resources, and access a marketplace of local resources and services that state and local governments can hire to promote local economic recovery while rebuilding after a disaster.
- **American Red Cross's Coordinated Assistance Network**: A cloud-based case-management system that enables the American Red Cross and its partners to share information and better coordinate delivery of recovery resources.
- **Economic Resilience Planning Evaluation Tool**: EDA and FEMA created a tool, first piloted in Colorado following the 2013 floods, to help economic development professionals better determine and define economic resilience activities in practice.

Recognizing the increasing number of these information resources, the Federal Government is also working to consolidate information on Federal recovery assistance in a more publicly accessible and user-friendly format. The U.S. Drought Portal contains a list of drought recovery resources available from eight separate Federal departments and agencies. As of December 2014, the portal had received approximately 280,000 visits. Similarly, EDA supported the development of RestoreYourEconomy.org, a website that consolidates economic recovery resources, technical assistance, and training into one site for use by local officials and economic recovery professionals.



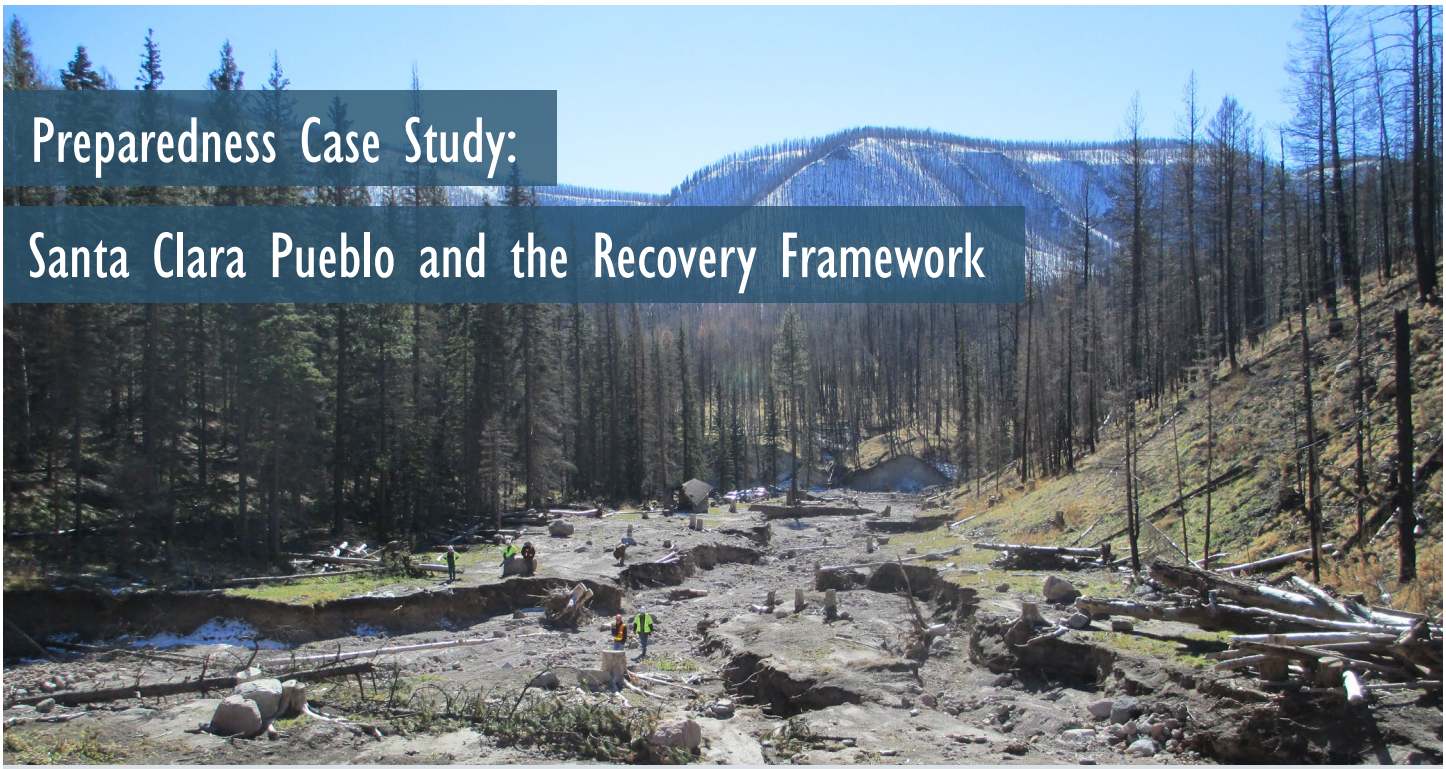
Mission Area Connections

Response

Recovery

Disaster Assessment and Assistance Dashboard

Response	▪ Presents real-time mapping of disaster relief locations and requests for assistance ▪ Provides status updates on roadways ▪ Displays information on hospitals, shelters, and other support facilities
Recovery	▪ Allows citizens, businesses, and governments to share information on Federal aid and how to reopen businesses ▪ Lists job-seekers local to disaster-affected areas available for hire



Preparedness Case Study:

Santa Clara Pueblo and the Recovery Framework

In the last decade, wildfires have destroyed over 80 percent of the Santa Clara Pueblo tribe's forest land. One consequence has been an increased susceptibility to flooding, with five major disaster declarations occurring in the last four years. A July 2013 flood resulted in the most damage, destroying four dams in the Santa Clara Canyon and causing some areas of the Santa Clara Creek to widen nearly ten-fold.

To meet recovery needs, the Santa Clara Pueblo became the first tribe to request and receive direct Federal support under the *National Disaster Recovery Framework* in September 2013. However, the Santa Clara Pueblo faced several challenges in their recovery efforts. Small staff size required tribal officials to serve multiple roles. For example, the sheriff for the tribe also served as the Tribal Coordinating Officer and the Tribal Disaster Recovery Coordinator. The Pueblo also encountered difficulties satisfying Federal cost-sharing requirements associated with obtaining disaster grants. In addition, standard methods of relocating individuals from flood-prone areas were not viable options, as reservation boundaries are not easily adjusted, and Pueblo people have strong cultural ties to the land on which they reside.

The Recovery Framework served as an effective mechanism for coordinating and planning the tribe's disaster recovery efforts. The Tribal Disaster Recovery Coordinator and Federal Disaster Recovery Coordinator facilitated the creation of a Recovery Support Strategy through an existing working group composed of tribal, state, and Federal officials. The strategy enabled the Pueblo to identify critical recovery priorities, secure commitments of Federal resources through the activation of Recovery Support Functions and issuing of Mission Assignments, and provide a timeline for monitoring recovery progress. Moreover, the Federal Coordinating Officer facilitated a consultation between Pueblo leadership, the FEMA Regional Administrator, and state officials that resulted in reduced cost-sharing requirements, enabling high-priority recovery projects to proceed.

A major part of the recovery effort was the tribe's collaboration with Federal agencies, the State of New Mexico, and the philanthropic community to repair and upgrade an early-warning system for floods. The 2013 floods destroyed the system, along with four dams. The Bureau of Indian Affairs offered a portion of Federal funding, and USGS provided technical assistance and updated technology for real-time remote monitoring and automated, community-wide alerts. The tribe received additional financial support from New Mexico and a philanthropic foundation. This effective whole community collaboration enabled the tribe to install an upgraded early-warning system prior to the summer 2014 monsoon season.

Conclusion

The 2015 *National Preparedness Report* provides evidence of the progress that the Nation has made in strengthening national preparedness and identifies remaining areas for improvement. Real-world events, exercises, and assessments highlighted the continued maturation of the National Preparedness System over the past year. The report identified three new core capabilities—Environmental Response/Health and Safety, Intelligence and Information Sharing, and Operational Coordination—as meeting acceptable levels of performance but requiring sustained effort to maintain capability and meet emerging challenges. These capabilities join five others from the 2014 report that future *National Preparedness Reports* will revisit to determine if they are still meeting performance goals.

The 2015 *National Preparedness Report* also highlights key preparedness challenges remaining for the Nation. Three core capabilities—Cybersecurity, Housing, and Infrastructure Systems—have persisted as areas for improvement across all four *National Preparedness Reports*. A fourth core capability, Long-term Vulnerability Reduction, repeats as an area for improvement from last year, due in part to questions surrounding the long-term solvency of the National Flood Insurance Program and nascent national efforts for climate change adaptation and green infrastructure. Preparedness data further revealed that the Federal Government, states, and territories are also struggling to build capacity for the Access Control and Identity Verification and Economic Recovery core capabilities. These areas for improvement are a reminder that preparedness gains are gradual and that solutions to complex challenges will not materialize without sustained support from the whole community.

In addition, the 2015 *National Preparedness Report* identifies four overarching findings with national implications. First, recent events—such as the epidemic of Ebola virus disease and the increase in arrivals of unaccompanied children crossing the U.S.-Mexico border—highlighted response and recovery coordination challenges for complex incidents that do not receive a Stafford Act declaration. Second, businesses and public-private partnerships are increasingly incorporating emergency preparedness into technology platforms. Third, the report found that the Federal Government lacks a mechanism to comprehensively assess the status of corrective actions for high-priority issues with broad implications across multiple Federal agencies, as identified in large-scale exercises and real-world incidents. Finally, states and territories reported current levels of preparedness similar to previous years.

The 2015 *National Preparedness Report* also marks the start of a multi-year analytic agenda, which is based on five issues introduced in the 2014 report:

- Studying **resilience efforts over a multi-year period** to better understand the return on investment for mitigation and recovery initiatives;

Multi-year analytic agenda: A set of issues identified in previous *National Preparedness Reports* as requiring long-term examination to inform the Nation's overall understanding of preparedness

- Examining in greater depth the concepts of **capability maturity and long-term sustainment**, including identifying inputs to help assess maturity, track capability assets from year to year, and better understand the relative contributions of whole community partners;
- Exploring how **dynamic elements within the preparedness environment**—including emerging technology, climate change, aging infrastructure, and legal and policy updates—positively and negatively affect prevention, protection, mitigation, response, and recovery initiatives;
- Partnering with Federal Government and whole community stakeholders to **measure performance** in the core capabilities more effectively **based on the new National Planning Frameworks and Federal Interagency Operational Plans** to explore complementary approaches for visualizing this information; and
- Examining security and resilience efforts that address the **interconnected nature of cyber and physical infrastructure,** including interdependencies across sectors.

These issues informed research topics and findings in the 2015 *National Preparedness Report*. Future reports will use the analytic agenda to track trends in capability over time, support resource-allocation strategies, and enrich the Nation's overall understanding of preparedness.

2015 National Preparedness Report Analytic Agenda

Resilience efforts over a multi-year period

- Federal agencies are expanding initiatives piloted through Hurricane Sandy recovery efforts to increase resilience across the Nation.
- The Sandy Regional Infrastructure Resilience Coordination Group is coordinating more than $18 billion in Federal infrastructure investments across more than 400 projects.

Capability maturity and long-term sustainment

- The Federal Government faces challenges in systematically assessing the implementation of corrective actions from real-world incidents and large-scale exercises.
- This year's report applied selection criteria for identifying capabilities to sustain; criteria included assessments of current preparedness, future trends and drivers influencing preparedness, and other preparedness indicators.

Dynamic elements within the preparedness environment

- Law enforcement strengthened community-based programs to combat violent extremism in response to evolving threats at home and abroad.
- As of October 2014, 38 Federal agencies had updated their climate change adaptation plans.

Measurement of performance based on the Frameworks and Federal Interagency Operational Plans

- The 2015 *National Preparedness Report* organized key findings by the National Planning Frameworks and linked preparedness data to critical tasks to assess performance.

Interconnected nature of cyber and physical infrastructure

- DHS increased engagement across the Federal Government and the private sector to support the response to cyber attacks against critical infrastructure.
- Federal agencies and Sandia National Laboratories are completing the Smart Power Infrastructure Demonstration for Energy Reliability and Security project to allow military bases to continue operating even when the external power grid is disrupted.

Acronym List

ACF	Administration for Children and Families, U.S. Department of Health and Human Services
ASPR	Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services
CBP	U.S. Customs and Border Protection
CDC	Centers for Disease Control and Prevention, U.S. Department of Health and Human Services
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOC	U.S. Department of Commerce
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOI	U.S. Department of the Interior
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
EDA	U.S. Economic Development Administration
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	U.S. Food and Drug Administration, U.S. Department of Health and Human Services
FEMA	Federal Emergency Management Agency
GAO	U.S. Government Accountability Office
HHS	U.S. Department of Health and Human Services
HUD	U.S. Department of Housing and Urban Development
IPAWS	Integrated Public Alert and Warning System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NRC	Nuclear Regulatory Commission
OHA	Office of Health Affairs
SAMHSA	Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services
SBA	U.S. Small Business Administration
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
USACE	U.S. Army Corps of Engineers
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
USGS	U.S. Geological Survey

Appendix A: Grant Case Studies

In 2014, the Federal Emergency Management Agency (FEMA) completed a series of grant case studies to demonstrate how states and urban areas across the country have used Federal homeland security grants to improve preparedness. FEMA partnered with stakeholders to develop case studies in Washington, Colorado, Oklahoma, Louisiana, and Illinois, as well as Houston, Texas. FEMA chose these locations to account for a mix of homeland security non-disaster grant programs, ensure geographical diversity, and link grant investments with recent events.

Washington: At a Glance

Since 2006, Washington has received nearly **$469 million in preparedness grant funding**. Washington implemented a regional approach to managing homeland security investments and improving preparedness. Regions are organized by threats, hazards, and population, and the regional approach provides planning and coordination support for the all-hazards environment. Washington's investment in the Northwest Regional Aviation unit demonstrates the value of the regional approach.

Northwest Regional Aviation Unit

Four Washington regions created the Northwest Regional Aviation Unit in response to the 1999 arrest of an al-Qaeda operative at a Puget Sound port and the 9/11 attacks. The air unit protects regional critical assets and provides search and rescue capabilities to the Puget Sound area. Regional partners used grant funds to purchase two helicopters and train aviation crews. They upgraded equipment through the addition of high-tech video and map interfaces, and integrated law enforcement communications systems. Local governments provided supplemental funding to support the unit's staff, maintenance, and operations.

In March 2014, when a major mudslide engulfed a rural neighborhood in Snohomish County, the Northwest Regional Aviation Unit was the most effective asset for spotting and rescuing survivors in thick, unstable mud up to 75 feet deep. The unit saved 16 people in the first three hours of the response

From 2007–2011, Washington invested $7.4 million of funding from the State Homeland Security Program, Urban Areas Security Initiative, and Port Security Grant Program to support the Northwest Regional Aviation Unit.

Colorado: At a Glance

Colorado has received over **$180 million in Federal homeland security grants** since 2006. Colorado's emergency preparedness initiatives target terrorism prevention and all-hazards disaster response. The Colorado Information Analysis Center plays a critical role in coordinating information sharing and ensuring public safety throughout the state.

Colorado Information Analysis Center

The Colorado Information Analysis Center serves as Colorado's analytic hub for all hazards. The center conducts interstate and intrastate information sharing that assists in investigations. The center and law enforcement partners

established an intelligence cell in the immediate aftermath of the 2012 Aurora theater shooting. The cell searched for accomplices and potential follow-on attacks using the agencies' combined databases, social media, and thousands of public tips.

In 2013, after the assassination of a Colorado Cabinet member, the Colorado Information Analysis Center partnered with the Texas Department of Public Safety Fusion Center to support a criminal manhunt. The Colorado Information Analysis Center distributed a request for information with a description of the suspect's car. Two days later, the Texas Fusion Center reported that a suspect driving a similar car had shot a Texas corrections officer. Through the fusion center, the Colorado Information Analysis Center located the assassin and enabled his arrest, along with the arrest of other individuals planning future assassinations.

Oklahoma: At a Glance

Between 2006 and 2013, Oklahoma received over **$146 million in preparedness grant funding**. Oklahoma faces a diverse set of threats and hazards, including tornados, wildfires, ice storms, and floods. The Alfred P. Murrah Federal Building bombing in 1995 also influenced the state's grant investment strategy. In an effort to protect Oklahoma's geographically dispersed population with limited emergency management resources, the state developed the Regional Response System.

Since 2006, Oklahoma has supported the Regional Response System through $35 million of funding from the State Homeland Security Program, Urban Areas Security Initiative, Law Enforcement Terrorism Prevention Grant Program, and Metropolitan Medical Response System Grant Program.

Regional Response System

Oklahoma has strategically placed Regional Response System assets, including equipment and 117 specialized teams, to ensure that response teams arrive on scene for all hazards within two hours or less in all regions of the state. Investments include nearly $3.5 million to deliver four training courses (in hazardous materials, rescue, incident management, and the National Incident Management System) 1,500 times to over 27,000 responders. Local response organizations maintain Regional Response System assets and contribute trained personnel to operate the equipment. The system has responded to numerous incidents, including tornados, a microburst storm, and a potential animal disease outbreak.

In May 2013, Regional Response System assets were vital to response efforts after an EF5 tornado struck the Oklahoma City metropolitan area. Five Technical Rescue Teams searched for children at two elementary schools. Thirty-three self-sufficient Regional Emergency Medical Services System units—equipped with generator power and tower lights—arrived at the destroyed Moore Medical Center within 10 minutes after the EF5 tornado touched down. During the eight-hour response operation, teams provided generator power to the medical station, lighting for citizens and responders, and medical supplies for patient treatment and transport.

Louisiana: At a Glance

Since 2005, Louisiana has received over **$380 million in Federal homeland security grants**. Louisiana's history of severe hurricanes and flooding, including Hurricanes Katrina and Rita in 2005, has shaped its emergency preparedness and response initiatives. Since 2005, the state has invested in interoperable communications, partnerships to enhance disaster response and recovery, and critical infrastructure protection. Through projects such as the Louisiana Wireless Information Network, Louisiana's investments of Federal preparedness grants aid in their response to hurricanes and large-scale incidents.

Louisiana Wireless Information Network

The Louisiana Wireless Information Network is a statewide interoperable public safety communications network that can link with surrounding states' networks. The network provides 95-percent geographic area radio coverage to over 70,000 users across 500 agencies.

The Louisiana Wireless Information Network provides first responders with interoperable communication capabilities in dense urban areas. New Orleans regularly hosts large-scale events and festivals, requiring significant surge communications capacity. During a large event such as Super Bowl XLVII or during annual events such as Mardi Gras, the Sugar Bowl, and the Jazz Festival, New Orleans' population can surge six-fold to two million people. Urban Areas Security Initiative investments in tower sites, microwave relays, remote equipment monitors, and radio repeaters inside buildings enable comprehensive wireless coverage. The Louisiana Wireless Information Network has decreased busy signals experienced by first responders by over 90 percent, enabling reliable communications capabilities.

Since 2005, Louisiana has invested over $90 million from grants, including funding from the State Homeland Security Program, Community Development Block Grant, Public Safety Interoperable Communications, Interoperable Communications Emergency Planning Grant, and Community Oriented Policing Services to support the Louisiana Wireless Information Network.

The Louisiana Wireless Information Network features multiple layers of redundancies, providing overall system resiliency during large and complex disasters. During Hurricane Isaac in 2012, the network increased communications capacity and handled twice the call volume compared to during Hurricane Gustav in 2008.

Illinois: At a Glance

From 2006 through 2013, Illinois received over **$1 billion in Federal preparedness grant funding**. The state faces a range of threats and hazards, including tornados, severe winter storms, and floods. Chicago is the Nation's third-largest metropolitan area and faces an enduring threat of terrorism. Chicago hosts high-profile public events requiring regional coordination and planning, such as the Chicago Marathon, the 2012 North Atlantic Treaty Organization summit, and major music festivals such as Lollapalooza. The Illinois Emergency Management Agency divides the state into eight regions and provides all regions with access to deployable response teams. Through projects such as the Chicago Fire Department's simulation center, Illinois uses grant awards to address important regional needs with information systems, targeted training, and equipment.

Chicago Fire Department Training and Simulation Center

The Chicago Fire Department's training and simulation center serves as a regional resource for all-hazards training. The center brings together regional partners through regularly offered training courses to enhance collaboration during response operations. More than 12 regional partners train at the center each year, including the U.S. Secret Service, the Federal Bureau of Investigation, Transportation Security Administration, O'Hare Airport, and local hospitals. Training includes courses addressing scenarios for active shooters, courses on emergency medical services, and other

The Chicago Fire Department has used $180,000 in Urban Areas Security Initiative funding to modernize its training and simulation center.

training for public safety operations, such as chemical, biological, radiological, nuclear, and explosive response.

The center's immersive fire and emergency medical services simulation center contributes to a dramatic increase in positive emergency medical outcomes. The center trains over 2,000 responders annually on proper techniques and procedures for emergency medical services. Responders train on state-of-the-art manikins that provide real-time feedback to students and instructors. Modernized training increased cardiac-arrest survival rates ten-fold. Additionally, successful first-attempt tracheal intubations increased by 20 percentage points.

Houston, Texas: At a Glance

From 2006 through 2013, the Houston Urban Area received over **$455 million in preparedness grants**. The Houston Urban Area Working Group and its standing committees collaboratively govern Urban Areas Security Initiative preparedness priorities. The Houston Urban Area funds preparedness initiatives based on relevant threat scenarios, regional risk assessments, and resource gap analysis. Houston used these grant funds to build programs with regional and national-level impact, including the "Run. Hide. Fight.® Surviving an Active Shooter Event" video.

"Run. Hide. Fight.® Surviving an Active Shooter Event" Video

The "Run. Hide. Fight.® Surviving an Active Shooter Event" video provides a realistic depiction of an active shooter incident and clear steps that individuals can take to survive such an event. The video, which Houston released shortly after the 2012 shooting in Aurora, Colorado, was developed to address preparedness gaps revealed during a Joint Counterterrorism Awareness Workshop.

The video was produced and developed with an initial investment from the Regional Catastrophic Preparedness Grant Program. The video has been shared with government agencies, nonprofit organizations, and private-sector entities in the United States and abroad. FEMA currently uses it to train its employees.

The "Run. Hide. Fight.® Surviving an Active Shooter Event" video has received millions of views on YouTube™.

Homeland Security