2017 National Preparedness Report

Homeland Security

Executive Summary

2017 National Preparedness Report

The *National Preparedness Report* summarizes the progress that the Nation has made in becoming more secure and resilient across five mission areas: Prevention, Protection, Mitigation, Response, and Recovery. The report identifies cross-cutting findings that apply across the mission areas, as well as key findings for each individual mission area. The report offers all levels of government, the private and nonprofit sectors, and the public practical insights into preparedness to support decisions about program priorities, resource allocation, and community actions.

What is the *National Preparedness Report*?

The *National Preparedness Report* is an annual requirement of *The Post-Katrina Emergency Management Reform Act of 2006* and a key element of the National Preparedness System. The report evaluates and measures gains that individuals and communities, private and nonprofit sectors, faith-based organizations, and all levels of government have made in preparedness. It also identifies where challenges and opportunities for improvement remain. The 2017 *National Preparedness Report* focuses primarily on preparedness activities undertaken or reported during calendar year 2016 and summarizes progress in building, sustaining, and delivering the 32 core capabilities outlined in the *National Preparedness Goal*.

Cross-Cutting Findings

The *National Preparedness Report* identifies four cross-cutting findings that stretch across the different mission areas. Analysts identified these findings through the evaluation of preparedness indicators—such as training participation and exercise frequency—that apply to all 32 core capabilities; assessments submitted by states and territories; and analysis provided by Federal agencies.

Environmental Response/ Health and Safety, Intelligence and Information Sharing, Operational Communications, Operational Coordination, and Planning are five core capabilities in which the Nation has developed proficiency, but in which it likely faces a future capability gap.

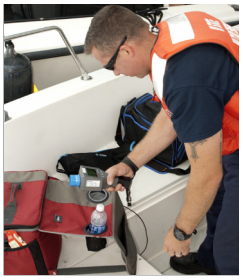
Cybersecurity, Economic Recovery, Housing, Infrastructure Systems, Natural and Cultural Resources, and Supply Chain Integrity and Security remain national areas for improvement. One additional core capability—Risk Management for Protection Programs and Activities—emerged as a new area for improvement in 2016.

States and territories reported similar levels of capability compared to 2015, highlighting that larger-scale preparedness investments are necessary to drive major improvements on an annual basis; since 2012, states and territories reported proficiency increases in the Mitigation mission area, but proficiency decreases in the Prevention, Protection, and Recovery mission areas.

Exercises conducted under the National Exercise Program tested all 32 core capabilities, and especially highlighted improvements and lessons learned for Intelligence and Information Sharing, Public Information and Warning, and Operational Coordination, as well as core capabilities in the Recovery mission area.

Key Findings

The 2017 *National Preparedness Report* offers 30 key findings that highlight successes and challenges across the five mission areas. The key findings are based on the analysis of qualitative and quantitative data from all levels of government and the private and nonprofit sectors. Several criteria contribute to the identification of findings—including quantitative data that show trends over time, demonstrated progress in establishing or implementing national-level strategies and policies, and significant shifts in resources to support preparedness. The sections below highlight selected key findings that address areas that may be of high public interest.



Prevention

The Prevention mission area prepares the Nation to avoid, prevent, or stop an imminent terrorist attack within the United States. In 2016, events such as the June attack at the Pulse nightclub in Orlando, Florida, and the September bombings in New York City and New Jersey highlighted the importance of Prevention capabilities. A key finding in this mission area is:

- *In 2016, the U.S. Department of Homeland Security's Office of Intelligence and Analysis, in collaboration with Federal, state, and local partners, implemented an enhanced process for assessing fusion center performance.*

Protection

The Protection mission area secures the homeland against acts of terrorism and human-induced or natural disasters. Throughout 2016, malicious cyber activities, such as ransomware attacks on critical services, highlighted the need for strengthened Protection capabilities. Selected key findings in this mission area include:

- *Lessons learned from the 2015 Office of Personnel Management data breaches continue to prompt actions to better safeguard sensitive data on government employees and contractors, and to update procedures for background investigations and security clearances.*
- *Among the different measures adopted to address the Zika epidemic, state, territorial, and local governments, as well as Federal agencies, effectively distributed preventative supplies and communicated protection measures.*

Mitigation

The Mitigation mission area reduces loss of life and property by lessening the impact of disasters. Record flooding in areas of Louisiana, Texas, and West Virginia, along with a sixth consecutive year of drought in California, underscored the value of risk-mitigation activities. Selected key findings in this mission area include:

- *Federal departments, the private sector, and industry groups have launched new efforts to improve understanding of the value of stronger building codes and to increase their adoption.*
- *As the costs of wildfire suppression rise, public and private initiatives to fund wildfire risk reduction projects are emerging.*

Response

The Response mission area focuses on saving lives, protecting property and the environment, and meeting basic human needs after an incident. Throughout 2016, a number of events demonstrated the importance of building these capabilities, including Hurricane Matthew—a major hurricane that led to flooding as it traveled up the Southeast coast. Selected key findings in this mission area include:

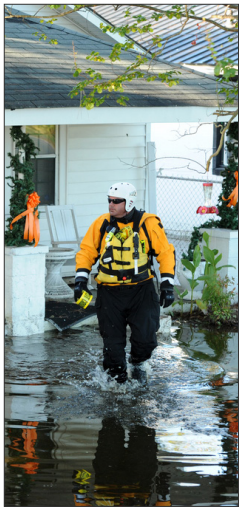
- *Federal agencies demonstrated agility by anticipating and reacting to evolving response needs during Hurricane Matthew.*
- *Public- and private-sector partners are collaborating to advance diagnostics, case monitoring, and case management in response to the Zika virus outbreak.*

Recovery

The Recovery mission area focuses on maintaining and restoring important community assets after an incident, such as housing, infrastructure, businesses, and health and social services, as well as ensures consideration for natural and cultural resources. In 2016, the Flint Michigan Water Contamination was one of several examples that showed how Recovery capabilities help communities coordinate and tackle challenges. Selected key findings in this mission area include:

- *Re-establishing child care services is an important element in helping families to recover, but most child care centers face severe challenges after a disaster.*
- *Recent flooding events highlight ongoing gaps in delivering housing solutions efficiently and effectively after disasters.*

Ongoing Challenges



While the 2017 *National Preparedness Report* highlights numerous achievements toward implementing the *National Preparedness Goal*, it also points to areas where progress has been slow to occur. As identified in this and previous *National Preparedness Reports*, the Nation still faces a number of persistent and emerging challenges. These include:

- *Detecting and preventing attacks by homegrown violent extremists*
- *Balancing competing demands between increasing security and minimizing disruptions to travel and commerce*
- *Inspiring individuals to prepare for emergencies*
- *Improving responder capacity and coordination in catastrophic events*
- *Comprehensively addressing the housing needs of disaster survivors*

These challenges require sustained effort and innovative approaches to overcome. Future reports will continue to monitor and assess our Nation's progress in addressing these and emerging preparedness challenges.

Table of Contents

2017 National Preparedness Report

Introduction

2017 National Preparedness Report

National preparedness actions help to prevent, protect against, mitigate, respond to, and recover from the threats and hazards posing the greatest risk to the Nation's security. Each year, the *National Preparedness Report* presents a Federal assessment of the Nation's progress toward achieving the *National Preparedness Goal* (see below) of a secure and resilient Nation.[1] Because preparedness is a shared responsibility across the entire Nation, the report aims to guide decisions of all preparedness stakeholders—including individuals, families, and communities; private and nonprofit sectors; faith-based organizations; and all levels of government—regarding program priorities, resource allocations, and community actions.[2] The 2017 edition of the *National Preparedness Report* primarily focuses on events that occurred or were reported on in 2016, but also covers a small number of events that occurred in early 2017.

Overview of the National Preparedness Goal & System

The *National Preparedness Goal* ("the Goal") describes what it means for the United States to be prepared for all types of disasters and emergencies, whether these are natural hazards (e.g., earthquakes, hurricanes, infectious diseases), accidental hazards (e.g., chemical spills), or human-induced threats (e.g., terrorism, cyberattacks). The Goal defines a vision for preparedness nationwide, namely:

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

To achieve this vision, preparedness stakeholders collectively need to effectively build, sustain, and deliver 32 "core capabilities" identified in the Goal (see Table 1). The core capabilities are distinct, critical elements needed to achieve the goal of a secure and resilient Nation. They are not exclusive to any single level of government or organization. The core capabilities provide consistent, standard, national-level definitions applicable for use by the whole community. Preparedness stakeholders—including private and nonprofit sectors, faith-based organizations, and all levels of government—can and do use the core capabilities to align their planning, training, exercise, and resourcing efforts.

Within the Goal, the core capabilities are grouped into five mission areas:

- ***Prevention:*** *Preventing, avoiding, or stopping an imminent, threatened, or actual act of terrorism or extremist violence*
- ***Protection:*** *Protecting citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows interests, aspirations, and way of life to thrive*
- ***Mitigation:*** *Mitigating the loss of life and property by lessening the impact of future disasters*
- ***Response:*** *Responding quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an incident*
- ***Recovery:*** *Recovering through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by an incident*

[1] The *National Preparedness Report* addresses several reporting requirements from *The Post-Katrina Emergency Management Reform Act of 2006*, including the Federal Preparedness Report, State Preparedness Report, and Catastrophic Resource Report.

[2] The reader recognizes that the Federal Government may identify products it uses or that have been implemented to support its emergency management efforts. This data is provided for informational purposes only, and the Federal Government does not endorse any non-Federal events, entities, organizations, services, or products.

Mission Areas and Core Capabilities

Table 1. The Goal outlines 32 core capabilities needed for a secure and resilient Nation. Each core capability is associated with one or more of the five mission areas.

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

The 2017 *National Preparedness Report* uses the five mission areas to organize its findings and to aid readers in identifying the sections most relevant to them. While the 32 core capabilities provide a basic nomenclature for describing the Nation's security and resilience posture, the mission areas provide a higher-level structure that is more reflective of the way organizations and individuals view their role in preparedness.

To complement this organizing structure, the National Preparedness System ensures a consistent process for moving forward with achieving the Goal. The National Preparedness System includes six components (see Figure 1):

- ***Identifying and Assessing Risk:*** *Collecting information on existing, potential, and perceived threats and hazards to assess risks*
- ***Estimating Capability Requirements:*** *Identifying the specific capabilities and activities needed to best address risks*
- ***Building and Sustaining Capabilities:*** *Determining the best ways to use limited resources to build and maintain capabilities informed by risk assessments*
- ***Planning to Deliver Capabilities:*** *Coordinating preparedness efforts with all relevant preparedness stakeholders, including individuals, businesses, nonprofits, community and faith-based groups, and all levels of government*
- ***Validating Capabilities:*** *Using exercises and assessments to identify gaps in existing plans/capabilities, and implementing corrective actions to ensure continuous improvement in meeting preparedness goals*
- ***Reviewing and Updating:*** *Performing regular reviews to keep preparedness efforts up-to-date with evolving risks and resources*

Encircling these six components are three concepts critical to successfully implementing the process. **Core Capabilities** identify the distinct critical elements to build, sustain, and deliver through the process. A **Whole Community** focus ensures the National Preparedness System addresses preparedness activities from a broad range of stakeholders, including all levels of government, private and nonprofit sectors, faith-based organizations, communities, and individuals. Finally, the **National Incident Management System (NIMS)** provides whole community partners with shared vocabulary, systems, and processes to help successfully deliver the core capabilities.

As shown in Figure 1, the six components, while forming a cyclic process, are also highly interconnected and interdependent. The *National Preparedness Report* addresses each part of the National Preparedness System, but plays a particularly important role in "Validating Capabilities," where it serves as the principal analysis and reporting product to monitor the Nation's progress in building, sustaining, and delivering the 32 core capabilities.

Figure 1. The National Preparedness System includes six interconnected components. It outlines an organized process for the whole community to move forward in building and sustaining the core capabilities outlined in the Goal, and helps ensure their successful delivery through the shared use of the vocabulary, systems, and processes identified in NIMS.

Report Organization

Following the **Introduction**, the 2017 *National Preparedness Report* continues with the **2016 Year in Review**, which highlights real-world incidents that attracted national headlines in 2016 and serve as the basis for several of the report's key findings. Next, the **Cross-Cutting Findings** section presents four findings that use various preparedness datasets to compare performance among all 32 core capabilities.

The main body of the report is divided into five sections, each based on one of the Goal's five mission areas—Prevention, Protection, Mitigation, Response, and Recovery. Each section begins with a **Mission Area Overview** that contains the following components:

- ***Core Capabilities in Practice:*** *Discusses the core capabilities and how they function, including examples that highlight the connections among core capabilities*
- ***Summary of Progress:*** *Provides a status update on preparedness efforts for core capabilities in the mission area*
- ***By the Numbers:*** *Measures achievements in current programs and initiatives*
- ***Mission Area Snapshots:*** *Provides short accounts of preparedness accomplishments and best practices from across the country*
- ***Preparedness Indicators:*** *Presents measures that demonstrate agency or program performance in the mission areas, for tracking in this and future National Preparedness Reports*

Subsequent to the overviews are the mission area **Key Findings**, each of which is an assessment of a specific area of national preparedness within that mission area. In total, the report includes 30 key findings across the five mission areas.

The report concludes with a section on **Ongoing Challenges**, which identifies persistent or emerging issues that the new Administration will likely face in each of the mission areas.

In addition, the 2017 *National Preparedness Report* includes five appendices:

- ***Appendix A: Acronym List*** *defines the acronyms appearing in the report*
- ***Appendix B: Research Approach*** *describes the steps taken to ensure a comprehensive report and the criteria used to help identify the report's key findings*
- ***Appendix C: 9/11 Retrospective*** *highlights ways in which the Nation has restructured and retooled its preparedness efforts since the 9/11 tragedy*
- ***Appendix D: Capabilities to Sustain Selection Methodology*** *describes the two-part analysis used to identify which of the 32 core capabilities are capabilities to sustain*
- ***Appendix E: Areas for Improvement Selection Methodology*** *describes how national areas for improvement were selected from the 32 core capabilities*

2016 Year in review

2017 National Preparedness Report

Each year, jurisdictions face threats that test their capabilities and reveal where strengths in delivering these capabilities exist and gaps remain. In particular, major disasters and emergencies that stress the Nation's collective abilities and resources play an important role in assessing progress toward achieving the Goal.

This year was no exception. In 2016, the following notable incidents informed several of the report's key findings.

January 16

The City of Flint, Michigan, continues to recover from a public health crisis resulting from contamination of its drinking water supply. Dangerously high levels of lead leached into the public water system after the city switched its primary water supply in April 2014. On January 16, 2016, the State of Michigan received an emergency declaration under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act), which authorizes Federal aid to supplement state and local response efforts under certain conditions. Specifically, the emergency declaration authorized the Federal Emergency Management Agency (FEMA) to provide water, water filters, water testing kits, and related items to Flint residents. In addition, the U.S. Department of Health and Human Services (HHS)—the designated lead agency for coordinating Federal support for response and recovery efforts in Flint—and other Federal agencies have provided assistance under their existing authorities. Their efforts have been addressing not only the ability to access safe water (covered by the emergency declaration), but also a broader suite of response and recovery activities. For additional analyses on these efforts, see page 83.

January 22

A blizzard struck the Mid-Atlantic and southern New England from January 22 to 24, resulting in historic amounts of snowfall and crippling winter storm conditions. The blizzard covered 434,000 square miles and affected approximately 102.8 million people, with almost 24 million people inhabiting areas that received more than 20 inches of snowfall. Governors in 10 states declared states of emergency, and major cities such as New York and Baltimore set all-time snowfall records (27.5 inches and 29.2 inches, respectively). The blizzard highlighted recent improvements in weather forecasting, with forecasters able to predict the weather system responsible for the blizzard a week in advance. In reaction, the Washington Metropolitan Area Transit Authority made the rare decision to shut down bus and rail service in the DC region ahead of the storm. In New York City, the mayor imposed a travel ban, which included shutting down trains and large segments of the subway system. Even so, the storm resulted in more than 30 fatalities, caused heavy flooding along the East Coast, stranded thousands of air travelers, and left thousands without electricity.

April 18

From March to June 2016, Texas experienced several severe storms, resulting in three presidential disaster declarations covering 39 counties. Intense rains on April 18 in the Greater Houston region led the National Weather Service to issue the largest flash-flood warning in at least a decade and required more than 1,200 high-water rescues. Following the city's worst flooding event in 15 years, the Mayor of Houston established a "flood czar" to oversee future flood-prevention efforts.

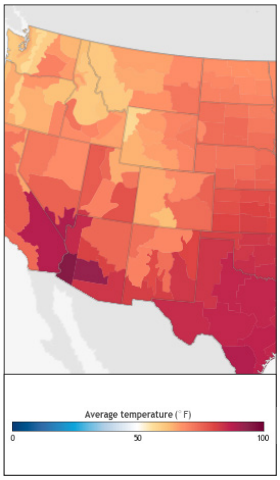
May 9

In 2016, California experienced its sixth consecutive year of drought, prompting the Governor of California to issue an Executive Order on May 9 to further institutionalize California's recent water-conservation efforts (see page 55 for additional details). The dry conditions contributed to wildfires. Through November 26, more than 7,000 wildfires burned nearly 560,815 acres. In addition, California faces an expanding epidemic of trees killed by drought and bark beetles (estimated at more than 102 million trees since 2010), increasing public safety risks such as wildfires. To mitigate these risks, the California Department of Forestry and Fire Protection has been working with Federal, local, and utility partners to remove dead and dying trees; as of November 18, 2016, they have removed more than 423,000 trees that pose the greatest risk. For an analysis of additional wildfire risk-reduction projects, see page 55.

June 12

An armed gunman attacked the Pulse nightclub in Orlando, Florida, resulting in the deadliest mass shooting in U.S. history, with 49 fatalities and 53 injured. Response efforts to the attack provide an example of the change in police tactics toward immediately engaging the shooter and quickly accessing the injured. For example, officers began evacuating victims from the scene, even though the shooter was still barricaded elsewhere in the nightclub. For additional analysis of how recent events are providing new insights into active shooter tactics and needs, see page 75.

June 22



In June, extreme heat struck the southwestern United States. On June 22, the peak of one heatwave, approximately 124 million individuals were under extreme heat warnings. In July, several southern U.S. cities broke monthly temperature records. Extreme heat kills hundreds of individuals in the United States each year and causes many more to become seriously ill. Scientists expect heatwaves to increase in severity, frequency, and duration. To help address this growing hazard, HHS's Centers for Disease Control and Prevention (CDC), the National Oceanic and Atmospheric Administration (NOAA), and other domestic and international partners released the National Integrated Heat Health Information System in May 2016. The system helps build understanding and facilitate communication and collaboration efforts to reduce extreme heat–related fatalities and illnesses. In addition, for the first time, America's PrepareAthon!—which supports grassroots efforts to increase community preparedness and resilience—designated an Extreme Heat Week (from May 23 to 27). During that week, Federal departments and agencies took part in various actions (e.g., webinars, presentations) to raise public awareness and prepare the Nation for extreme heat.

June 23

A band of severe thunderstorms struck West Virginia, resulting in a 1,000-year rainfall event (i.e., a rainfall event that has a 0.1 percent chance of occurring in any given year) that produced one-quarter of the state's annual rainfall in a single day and left thousands stranded, 100 homes badly damaged or destroyed, and 22 dead. The U.S. Small Business Administration (SBA) approved more than $47 million in low-interest disaster loans for affected residents and businesses. Nearly another $40 million of housing and other needs assistance has gone to eligible survivors through FEMA's Individuals and Households Program.

July 29

Zika, a viral infection primarily spread by certain mosquitoes, poses serious health risks to infants born from women infected with the virus during pregnancy. On December 31, 2015, the United States experienced the first of many locally transmitted cases of the Zika virus in the U.S. territory of Puerto Rico. Seven months later, on July 29, 2016, the Florida Department of Health reported the mosquito-borne spread of Zika in a neighborhood of Miami, Florida, marking the first occurrence of locally transmitted Zika in the continental United States. As of December 28, 2016, CDC reported more than 39,700 cases of Zika virus infections in U.S. states and territories, with the highest number of cases reported in Puerto Rico, Florida, and New York. Most cases in the continental United States are travel-related. However, in addition to Puerto Rico and Florida, health officials have reported local Zika transmission in Texas, the U.S. Virgin Islands, and American Samoa. On February 23, 2016, in the absence of supplemental emergency funds, HHS reprogrammed more than $500 million to immediately prepare for and respond to the Zika virus. In September 2016, Congress approved $1.1 billion in Zika emergency funding to control the spread of Zika-carrying mosquitoes, continue development of vaccines and surveillance systems, and improve diagnostic tests. For example, given the major risks of Zika to pregnant women, CDC quickly established pregnancy registries to capture information about pregnant women and their infants with laboratory evidence of Zika. These registries have provided estimates of the risks of Zika and have informed clinical guidance for the evaluation and testing of pregnant women and infants. For additional analysis on U.S. response efforts to address the Zika virus outbreak, see page 64 and 66.

August 11

From August 11 to 13, Louisiana faced its second major flooding event of the year. Portions of the state experienced a 1,000-year rainfall event, causing river levels to exceed record heights and flooding in several areas for the first time. The August Louisiana floods were the worst U.S. natural disaster since Hurricane Sandy, damaging more than 109,000 homes and causing an estimated $8.7 billion in damages. Flood insurance policyholders in Louisiana filed 26,128 claims and received more than $2.26 billion (as of January 31, 2017). More broadly, flood insurance claims nationwide in 2016 exceeded 82,000 claims. In 2016, the National Flood Insurance Program (NFIP) experienced its third most severe loss of record, with losses exceeding $4 billion (due in large part to the August Louisiana floods). For additional analyses of response and recovery efforts for these floods, as well as remaining challenges highlighted by these events, see pages 70, 84, and 87.

September 9

From September 9 to 21, the Colonial Pipeline Company shut down its East Coast gasoline supply pipeline following the discovery of a leak in the pipeline near Helena, Alabama. This pipeline system supplies 2.5 million barrels per day of transportation fuels to locations in the Southeast and along the eastern seaboard (as far north as New York Harbor), and is a critical supply of fuel in many southeastern states. In the weeks following the shutdown, the reduction in gasoline volumes led to shortages in the Southeast, with retail price spikes of more than 20 cents per gallon reported in some markets. A subsequent explosion and fire on October 31 near the site of the original leak forced an additional closure of the pipeline. Federal agencies—including the U.S. Department of Homeland Security (DHS), the U.S. Department of Energy (DOE), and the U.S. Department of Transportation (DOT)—monitored both incidents, with DOE working closely with industry and affected states to conduct modeling and analysis of the regional fuel supply situation and manage information sharing among key stakeholders.

September 17

Two improvised explosive devices (IEDs) detonated (one in New York City and the other in Seaside Park, New Jersey), with one explosion injuring more than 30 people and causing millions of dollars of property damage. Similar to the San Bernardino and Pulse nightclub attacks, the individual involved in these attacks appeared to have been inspired by foreign terrorist ideologies. Moreover, these attacks reiterate the challenges of uncovering plots by lone (or small numbers of) attackers and the need to secure high-risk chemicals that can be used to make IEDs. Federal Bureau of Investigation (FBI) agents had investigated the man accused of planting the New York and New Jersey bombs more than two years earlier, finding no ties to terrorism. Fortunately, increasing awareness of IED threats and the importance of reporting suspicious activity by the public assisted investigators and contributed to finding other unexploded IEDs.

September 20

KrebsonSecurity.com—a popular blog focusing on online crime investigations, cyber threats and cybersecurity, data breaches, and cyber justice—was the target of a distributed denial-of-service (DDoS) attack. DDoS attacks prevent legitimate users from accessing information or services. A botnet allegedly comprising more than 380,000 hacked "Internet of Things" devices—such as routers, network-enabled cameras, and digital video recorders—was responsible for the attack, which was among the largest DDoS attacks on record. For additional information on the growing challenge that the Internet of Things presents to information security and cybersecurity, see page 94.

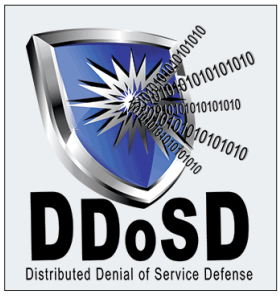
September 22

After investigating a criminal attempt at selling Yahoo! user account information, Yahoo! researchers uncovered a data breach that had gone undetected for two years and compromised more than 500 million user accounts. The Chief Information Security Officer of Yahoo! announced the existence of the breach on September 22. Nearly three months later, Yahoo! disclosed that a separate attack in 2013 compromised more than 1 billion accounts. Even as the Federal Government continues to implement lessons learned from the 2015 U.S. Office of Personnel Management (OPM) breaches (see page 38), these new discoveries and other incidents in 2016 involving critical systems—such as attempted attacks on voter registration systems (see page 37) and holding hospital systems hostage for ransom (see page 37)—continue to raise cybersecurity concerns.

September 30

In an above-normal hurricane season, five named storms made landfall in the United States during 2016, the most since 2008. The strongest and longest-lived of these was Hurricane Matthew, which reached maximum sustained winds of 160 miles per hour and was a major hurricane from September 30 to October 7. Forecasted as passing very near or over the east coast of Florida with potentially disastrous impacts, Hurricane Matthew eventually made landfall in South Carolina on October 8 as a category 1 hurricane. The hurricane's path up the Southeast coast of the United States resulted in storm surge and beach erosion from Florida through North Carolina and caused extensive inland flooding in the Carolinas. Pre-disaster emergency declarations issued October 6 for Florida, Georgia, South Carolina, and North Carolina authorized FEMA to mobilize equipment and resources to anticipated affected areas. For additional analysis of how Federal agencies anticipated and reacted to developing needs during Hurricane Matthew, see page 68.

October 21



Dyn, a major provider of Domain Name System resolution (i.e., the computers that translate website names into Internet protocol addresses), was subject to two large-scale DDoS attacks. As a result, major websites such as Twitter, Netflix, Spotify, Airbnb, and The New York Times were temporarily inaccessible to users. Similar to the September 20 attack on the KrebsonSecurity.com blog website, a significant portion of the attack stemmed from botnets consisting of "Internet of Things" devices, highlighting the cybersecurity vulnerabilities of these devices. Moreover, by targeting critical cyber infrastructure, attackers can cause more harm than attacks on individual sites or organizations.

October 27

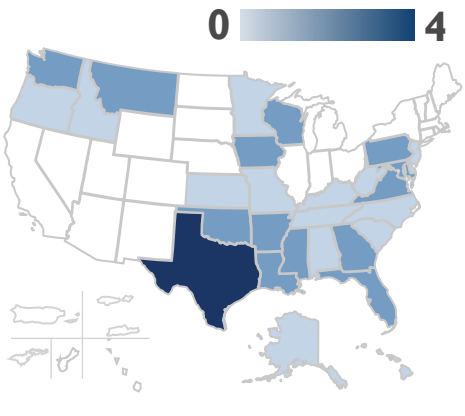
In late October, fake 911 calls inundated several U.S. public safety answering points (PSAPs). A teenage hacker—arrested on October 27 in Maricopa County, Arizona—had created malware to exploit an iPhone vulnerability, forcing iPhones to place fraudulent 911 calls. The malware, promulgated using Twitter, spread and instigated a significant DDoS attack that affected PSAPs in 12 states, including Washington, California, and Arizona.

November 28

Severe drought left the Southeast vulnerable to numerous wildfires in late 2016. At the peak of the drought, more than 16.5 percent of the total area of Kentucky, Tennessee, North Carolina, Georgia, Alabama, and Mississippi was under conditions of exceptional drought (i.e., the most intense level of drought), affecting nearly 6.9 million people. The drought contributed to hundreds of wildfires. For example, a wildfire that ignited near Gatlinburg, Tennessee, in late November grew to become the largest fire in the state in 100 years, resulting in 14 fatalities, at least 180 injured, and more than 2,400 structures damaged or destroyed. Authorities evacuated more than 14,000 people from the city. Tennessee Highway Patrol troopers conducted door-to-door canvassing to assist with notifications and evacuations in addition to the National Guard, which used HHS emPOWER Initiative data to rapidly identify at-risk individuals with access and functional needs.

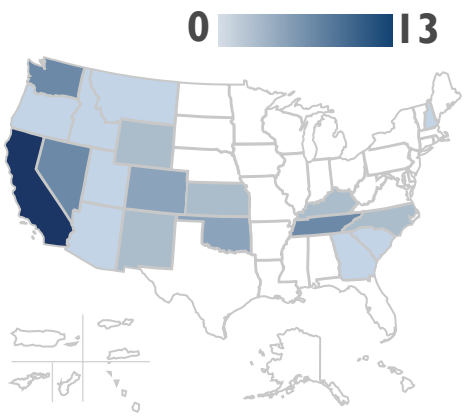
Supporting Disaster Survivors and Capability Development

Major Disaster Declarations



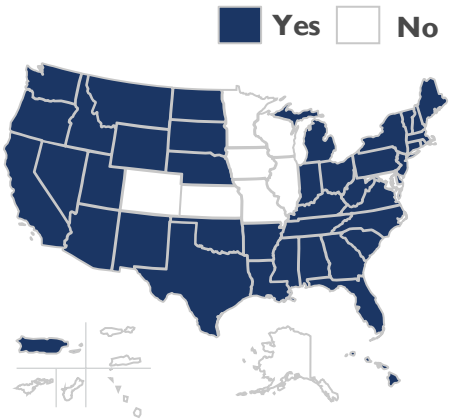
In 2016, Federal agencies assisted in 46 major disaster declarations across 30 states, territories, and tribes.

Fire Management Assistance Declarations



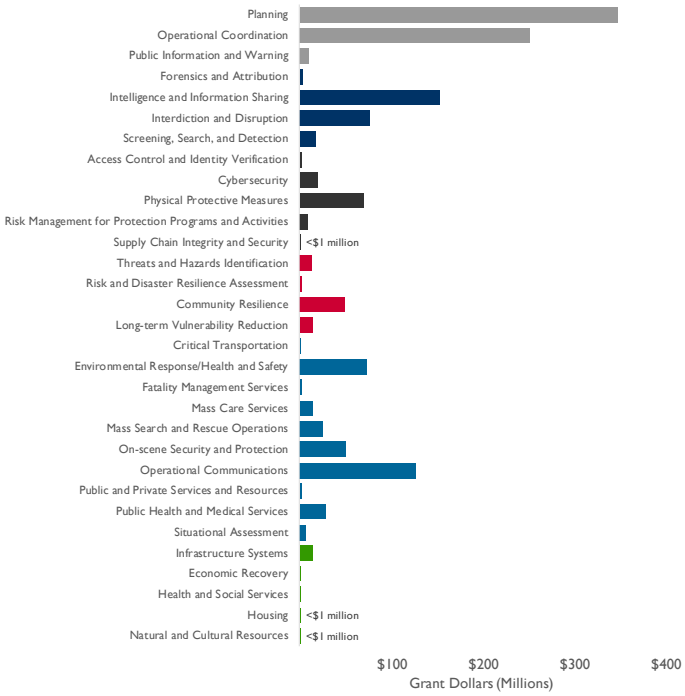
In 2016, Federal agencies assisted with 50 instances of fire management across 19 states.

Drought Designations



In 2016, Federal agencies assisted with USDA-designated drought disasters for 1,025 counties across 42 states and territories.

Distribution of FEMA Preparedness (Non-Disaster) Grants by Core Capability, Fiscal Year 2015



**Grant recipients use the Biannual Strategy Implementation Report (BSIR) to track planned and actual grant expenditures, and categorize expenses into five POETE elements. The BSIR is a snapshot of obligated funding for the given reporting period and do not necessarily reflect grant expenditures.*

In fiscal year 2016, FEMA provided more than $2.3 billion in preparedness grants.

In addition, HHS provided more than $900 million in public health and healthcare system preparedness grants to states and localities.

In fiscal year 2016, FEMA training programs achieved approximately 2.7 million course completions across all core capabilities.

Cross-Cutting Findings

2017 National Preparedness Report

The 2017 *National Preparedness Report* identifies four cross-cutting findings—stretching across the five mission areas—through the evaluation of preparedness indicators (e.g., training participation, exercise frequency) that apply to all 32 core capabilities; assessments submitted by states and territories; and analysis provided by Federal agencies.

Cross-Cutting Finding:

Environmental Response/Health and Safety, Intelligence and Information Sharing, Operational Communications, Operational Coordination, and Planning are five core capabilities in which the Nation has developed proficiency, but in which it likely faces a future capability gap.

Each *National Preparedness Report* identifies a subset of the core capabilities as "capabilities to sustain." To be a capability to sustain, a core capability must satisfy two conditions. First, the Nation must show proficiency in executing that core capability. Second, there must be indications of a potentially growing gap between the demand for and the performance of that core capability in the future.

Consistent with previous reports and with the methodology outlined in Appendix D, the 2017 *National Preparedness Report* identifies the following five core capabilities as capabilities to sustain.

Environmental Response/Health and Safety

This core capability focuses on ensuring the health and safety of the public and workers, as well as the environment, from hazards encountered during response efforts. Extensive amounts of training and exercises occur in this core capability relative to others. Moreover, a broad range of Federal, state, and local assets exist, which support responses to thousands of hazardous materials incidents each year. This national competency is reflected in the 2016 State Preparedness Report results, in which states and territories rated Environmental Response/Health and Safety among the top ten core capabilities in proficiency. Greater demands, however, may occur for this core capability in the future, since more than half of Federal agencies playing key roles in supporting response efforts have identified this core capability as a priority in their latest strategic plans.

Intelligence and Information Sharing

Intelligence and Information Sharing is the capacity for all levels of government and the community to communicate and receive timely and actionable information. More than half of state and territory responses to the 2016 State Preparedness Report indicated proficiency in this capability. In addition, the Nation has developed a number of assets to support this capability, including FBI-led Joint Terrorism Task Forces (JTTFs), state and major urban area fusion centers, and various information-sharing systems (e.g., Homeland Security Information Network [HSIN], TRIPwire). Technological developments, however, require the careful balancing of intelligence collection and privacy protections (see page 39). The emergence and growth of threats also places added demands on public- and private-sector stakeholders to share and exchange information (see page 37). Intelligence and Information Sharing remains critical to states and territories—80 percent of which regard it as a high priority—and the capability is of growing emphasis among Federal agencies in the Prevention and Protection mission areas.

Operational Communications

This Response core capability addresses the ability of emergency responders to communicate during an incident. Fifty-five percent of state and territory responses to the 2016 State Preparedness Report indicate proficiency in carrying out Operational Communications, placing it in the top ten among all core capabilities. Ensuring that responders from multiple jurisdictions and agencies can communicate on interoperable systems, however, requires sustained attention through exercises, planning, and technological acquisitions. For example, Operational Communications is among the top five most commonly assessed core capabilities in FEMA's National Exercise Program (NEP). Moreover, First Responder Network Authority (FirstNet) is engaged in a complex, long-term project to provide a single interoperable broadband network for responders nationwide (see page 72).

Operational Coordination

Operational Coordination spans all mission areas and addresses those actions necessary to establish and maintain a unified and coordinated structure for operations, as well as processes to integrate all appropriate stakeholders. In 2016, response and recovery efforts during real-world incidents (e.g., the Zika virus outbreak) highlighted progress among Federal agencies in improving their coordination for incidents that do not receive a presidential disaster declaration (see page 66). Moreover, states and territories have consistently rated themselves as among the most proficient in carrying out Operational Coordination. While this remained true in 2016, comparisons between 2015 and 2016 State Preparedness Report results show a decline in proficiency by more than five percentage points, signaling an increasing gap in preparedness. Nearly 18 percent of states and territories also selected Operational Coordination as a core capability in greatest danger of future decline (the seventh-highest result for all core capabilities).

Planning

Common to all mission areas, the Planning core capability addresses the need for a systematic process that engages all relevant stakeholders in the development of strategic, operational, and tactical approaches to effectively deliver core capabilities. State and territory self-assessments continue to place Planning among the top ten ranked core capabilities every year, with 58 percent of ratings in the 2016 State Preparedness Report indicating proficiency in Planning. Similar to Operational Coordination, stakeholders nationwide continue to pay significant attention to Planning, as evidenced by relatively high training and exercise participation, as well as Federal preparedness grant investments. In their 2016 State Preparedness Report responses, more states and territories identified Planning as one of their most improved core capabilities than any other. Planning requires ongoing attention as threats remain dynamic. Terrorists continue to refine ways to radicalize individuals (see page 39), new infectious disease outbreaks can require adapting and supplementing existing approaches (see pages 64 and 66), and technology provides new threat vectors and capabilities for adversaries (see page 93).

Cross-Cutting Finding:

Cybersecurity, Economic Recovery, Housing, Infrastructure Systems, Natural and Cultural Resources, and Supply Chain Integrity and Security remain national areas for improvement. One additional core capability—Risk Management for Protection Programs and Activities—emerged as a new area for improvement in 2016.

The *National Preparedness Report* identifies a subset of core capabilities each year as national areas for improvement.

Selection criteria for areas for improvement include the report's key findings on preparedness; State Preparedness Report results; data on the frequency of exercises; funding support; and future trends and drivers affecting preparedness. Appendix E details the approach used for selecting this year's areas for improvement.

The 2017 *National Preparedness Report* identifies seven core capabilities as national areas for improvement. One of these appears as an area for improvement for the first time in the *National Preparedness Report*: Risk Management for Protection Programs and Activities. The remaining six—Cybersecurity, Economic Recovery, Housing, Infrastructure Systems, Natural and Cultural Resources, and Supply Chain Integrity and Security—have appeared in previous *National Preparedness Reports*. For Cybersecurity, Infrastructure Systems, and Housing, this represents their sixth consecutive year as areas for improvement.

Cybersecurity

The Cybersecurity core capability addresses protecting and restoring electronic communications systems (e.g., critical communications infrastructure), information, and services from damage, unauthorized use, and exploitation. Throughout 2016, public- and private-sector organizations suffered malicious cyber activity. Critical services in particular—such as healthcare and law enforcement—saw increases in ransomware attacks, and voter registration systems have come under threat as well. The Federal Government has sought to address cyber threats through policies that improve the coordination of its response and through the application of lessons learned from previous incidents, such as the 2015 OPM breach. The increasing use of the collaboratively developed Cybersecurity Framework (see page 15 for additional details) for managing cybersecurity risks in critical infrastructure, as well as more broadly throughout the economy and society (including by some states and localities), has been a positive development. While states and territories continue to indicate that Cybersecurity is a high priority, more rate themselves as lacking proficiency in it than any other core capability. See pages 37 and 38 for additional information on these issues.

Economic Recovery

This core capability focuses on returning economic and business activities to a healthy state and on developing new business and employment opportunities that result in economically viable communities. States and territories identified Economic Recovery as the second lowest-rated core capability for the second year in a row, and jurisdictions also reported the largest proficiency decreases in Economic Recovery, which dropped by 10 percent from 2012–2016.

Housing

This core capability focuses on implementing affordable and accessible housing solutions that effectively support the needs of the whole community and contribute to its sustainability and resilience. Flooding events in 2016, such as historic summer flooding that occurred in Louisiana, underscored the longstanding challenges the Nation has faced in meeting the housing needs of survivors, including survivors with disabilities and others with access and functional needs. Assistance to renters continues to be a challenge, as does the availability and rapid deployment of manufactured housing units, and the time and additional resources that may be required to build back housing more resiliently to better prepare for the next storm. Federal agencies have taken actions to strengthen the Housing core capability, such as the creation of updated housing doctrine and a toolkit to help recovery stakeholders support people who may be disproportionately affected by disasters (e.g., people with disabilities and individuals and families at risk of homelessness), but difficulties persist. Few training

opportunities and exercises address housing, and in 2016, Housing remained among the lowest-rated core capabilities—as states and territories reported the third-lowest levels of proficiency. See pages 87, 89, and 97 for additional information on these issues.

Infrastructure Systems

The focus of Infrastructure Systems is on stabilizing critical infrastructure functions, minimizing health and safety threats, and efficiently restoring and revitalizing systems and services to support a viable, resilient community. While Federal departments and agencies took steps to address challenges to this core capability, as detailed on page 89, limited evidence exists demonstrating that the Nation has made significant progress in this area. Aging infrastructure in many sectors presents growing risks, as well as decreases resilience. For example, the Flint Michigan Water Contamination highlights the growing threat to national public health from deteriorating water-line infrastructure. States and territories identified this core capability as exhibiting below-average levels of proficiency in 2016.

Natural and Cultural Resources

Natural and Cultural Resources focuses on protecting natural and cultural resources and historic properties through appropriate actions that preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices. While governmental and nongovernmental organizations sponsored forums and training events to bring greater attention to this capability, states and territories collectively rated it as the lowest priority across all capabilities. They also reported the fourth-lowest levels of proficiency, ahead of only Housing, Economic Recovery, and Cybersecurity. In addition, state and local jurisdictions continue to infrequently exercise this capability. Despite the current NEP cycle's emphasis on Recovery core capabilities (see page 18), only seven NEP exercises (out of 167) addressed this core capability (see Figure 2).

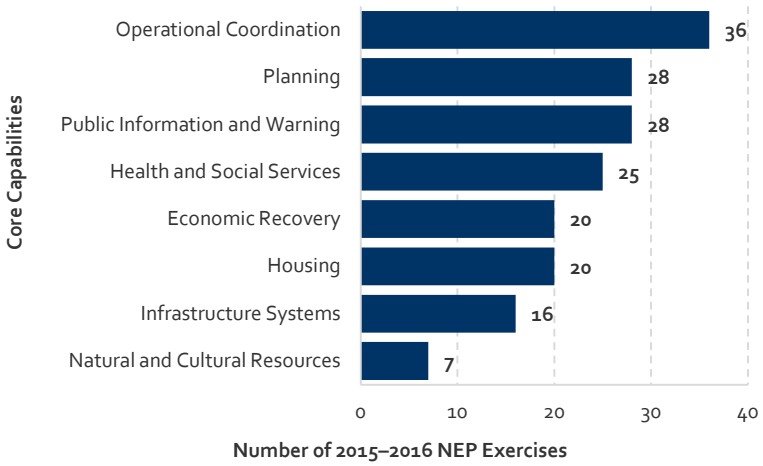


Figure 2. In the 2015–2016 NEP exercise cycle, 69 NEP exercises addressed one or more Recovery core capabilities. *(Note: Counts for Operational Coordination, Planning, and Public Information and Warning are specific to the Recovery mission area)*

Risk Management for Protection Programs and Activities

This core capability covers the identification, assessment, and prioritization of risks to inform protection activities, which include continuity planning. Its first appearance as an area for improvement in the *National Preparedness Report* is driven by state and territorial self-assessments of proficiency. The percentage of non-proficient ratings for this capability was the fifth-highest across all core capabilities. Risk Management for Protection Programs and Activities also fell in the bottom 25 percent of capabilities that state and local jurisdictions reported exercising in the past five years, and few NEP events tested the capability in 2016. Moreover, there was little evidence that the Nation has made progress toward validating and evaluating progress in this capability over the past year. One exception is the growing use of the Cybersecurity Framework.

Cross-Cutting Case Study: Cybersecurity Risk Management

Since its publication in February 2014, the Cybersecurity Framework has become the leading management tool in the United States for assessing cyber risks and prioritizing appropriate policies and actions. The Framework—developed out of a year-long collaborative process led by the National Institute of Standards and Technology (NIST), with the active involvement of thousands of experts from the private sector, DHS, and many others—identifies existing cybersecurity standards, guidelines, frameworks, and best practices that increase cybersecurity across all sectors and industry types. It provides a flexible, repeatable, and cost-effective risk-based approach to implementing security practices. According to Gartner (an information technology [IT] research company), 30 percent of U.S. organizations have used the Cybersecurity Framework in the first two years since its release, with that number projected to increase to 50 percent by 2020.

Supply Chain Integrity and Security

This core capability deals with strengthening the security and resilience of the supply chain. States and territories reported relatively low levels of proficiency for this capability, with more than a third of all State Preparedness Report ratings indicating that respondents are not able, or minimally able, to meet their performance targets. In addition, the capability fell in the bottom 25 percent of capabilities that were included in 2016 NEP exercises. State and local jurisdictions also completed relatively few FEMA-sponsored in-person training courses focused on Supply Chain Integrity and Security. Use of larger, more-complex networks of global suppliers, as well as growing dependence on IT systems, places some supply chains at increasing physical (e.g., counterfeit parts) and cyber (e.g., malware) risk.

Cross-Cutting Finding:

States and territories reported similar levels of capability compared to 2015, highlighting that larger-scale preparedness investments are necessary to drive major improvements on an annual basis; since 2012, states and territories reported proficiency increases in the Mitigation mission area, but proficiency decreases in the Prevention, Protection, and Recovery mission areas.

Each year, through the State Preparedness Report, states and territories self-assess their ability to achieve targets they establish for each core capability through an annual risk assessment process. In the State Preparedness Report, they use a 5-point rating scale—with a 5 being the highest—to assess each of these core capabilities in five areas: Planning, Organization, Equipment, Training, and Exercises. Capabilities change slowly over time; therefore, year-over-year changes in capability ratings are typically small. In 2016, states and territories reported their strongest proficiency ratings (indicated by the percentage of 4 and 5 ratings) in the cross-cutting core capabilities (i.e., Planning, Operational Coordination, and Public Information and Warning) and Response mission area and their lowest proficiency ratings in the Recovery and Protection mission areas. State and territory capability levels for each mission area remained consistent with prior years, including with 2015 results (see Figure 3).

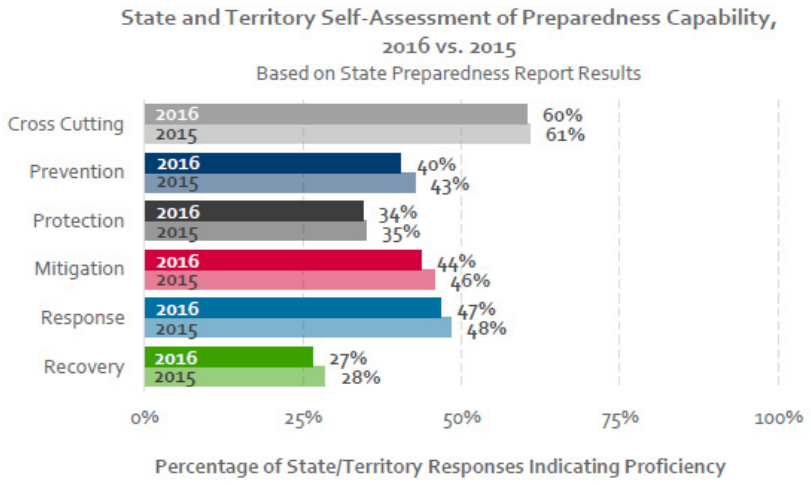


Figure 3. States and territories reported the highest capability ratings in the cross-cutting core capabilities and those within the Response mission area.

Figure 4 shows the breakdown of proficiency scores by core capability. Jurisdictions generally identified the same core capabilities as strengths and weaknesses as they did last year. Modest changes from 2015 include:

- ***Capability Strengths:*** *Fire Management and Suppression replaced Threats and Hazards Identification in the top ten capabilities with the highest proficiency ratings.*
- ***Capability Weaknesses:*** *Infrastructure Systems and Forensics and Attribution replaced Supply Chain Integrity and Security and Physical Protective Measures in the bottom ten capabilities with the lowest proficiency ratings.*

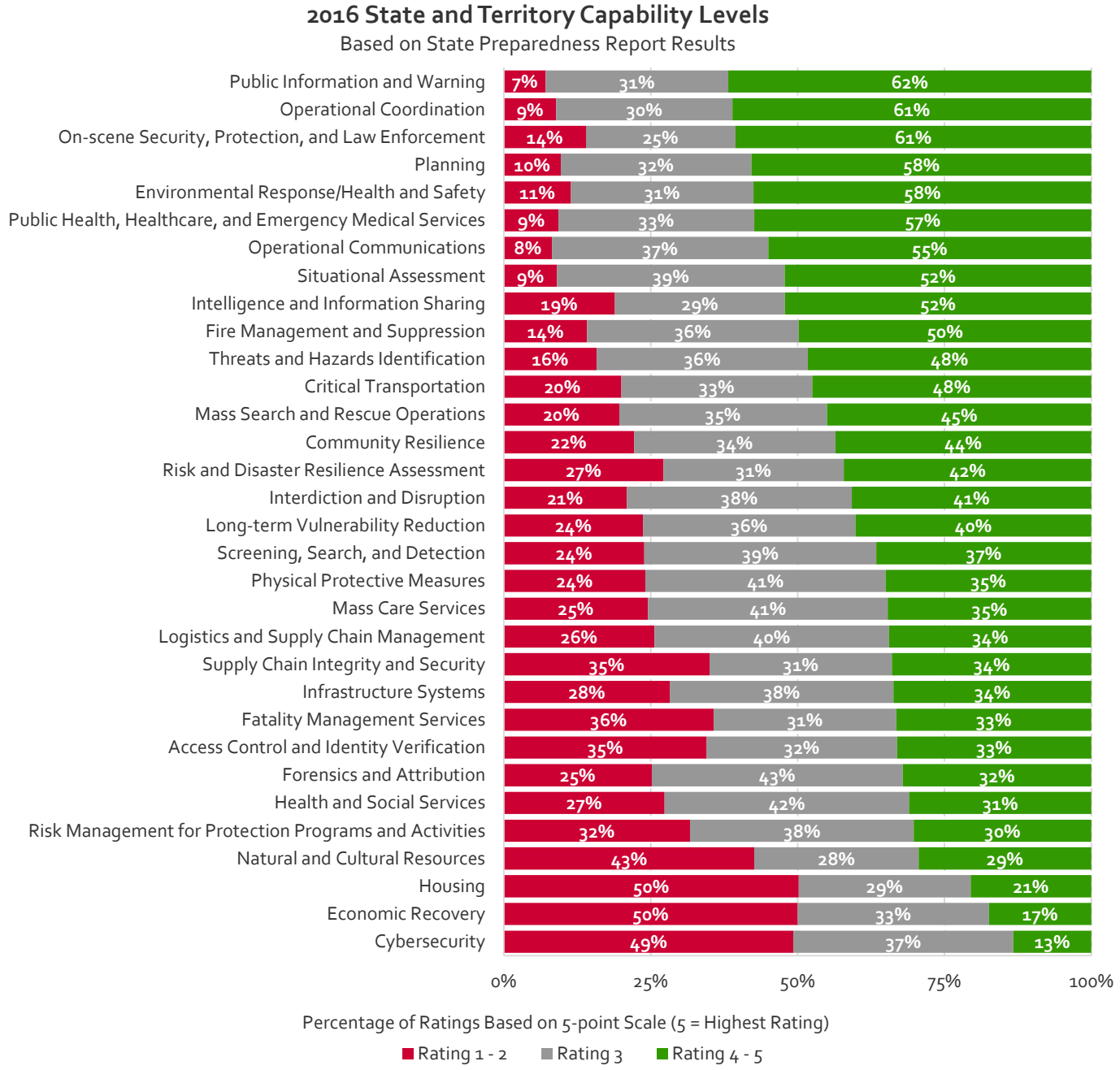


Figure 4. States and territories reported the highest capability ratings in Public Information and Warning and the lowest capability ratings in Cybersecurity and Economic Recovery.

Since 2012,states and territories have reported proficiency increases in the cross-cutting capabilities and the Mitigation mission area. They have reported proficiency decreases in the Protection, Prevention, and Recovery mission areas. The Response mission area ratings have remained essentially unchanged. At the core capability level (see Figure 5), jurisdictions have reported the largest proficiency increases in Public Information and Warning (11 percent since 2012) and Environmental Response/Health and Safety (eight percent since 2012). Jurisdictions reported the largest proficiency decreases during this period in Economic Recovery, which dropped by 10 percent, and Forensics and Attribution, which dropped by eight percent.

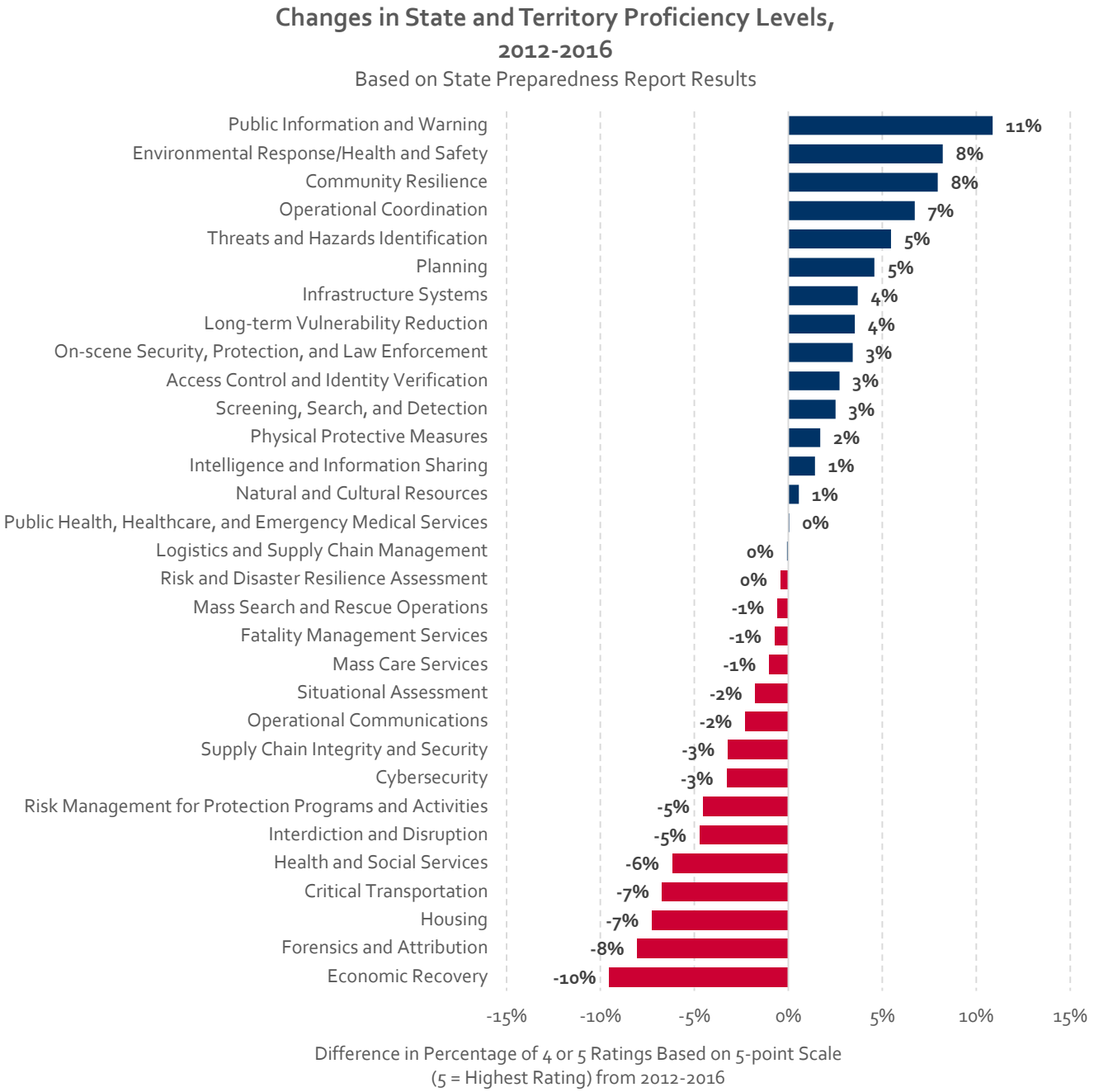


Figure 5. Since 2012, states and territories have reported rating increases in 15 core capabilities and rating decreases in 16 core capabilities.

Cross-Cutting Finding:

Exercises conducted under NEP tested all 32 core capabilities, and especially highlighted improvements and lessons learned for Intelligence and Information Sharing, Public Information and Warning, and Operational Coordination, as well as core capabilities in the Recovery mission area.

FEMA's NEP serves as the Nation's principal mechanism for testing national preparedness through exercises. Operating in two-year cycles, the program features a progressive series of exercises that culminates in a full-scale, national-level, capstone exercise. Each cycle focuses on testing a particular set of strategic priorities, providing a consistent method to validate the capabilities of Federal and non-Federal partners, and gauge progress toward reaching the Goal.

National Exercise Program Capstone Exercise 2016

From April 25 to May 17, 2016, Federal agencies and partner organizations conducted the National Exercise Program Capstone Exercise 2016 ("Capstone 2016"), the culminating exercise for the 2015–2016 NEP cycle. Capstone 2016 examined the ability of senior Federal leaders and key partners to share and act upon information to achieve common and accurate situational awareness, inform crisis action planning, and establish priorities for life-saving and life-sustaining operations in response to a credible threat. Federal departments and agencies organized large-scale activities to defend the homeland and save lives in the face of a weapon-of-mass-destruction (WMD) threat to the Nation's capital, but confronted challenges in situational awareness, public communications, and operational coordination. Federal agencies as a whole lacked consistent situational awareness. At times, the full intelligence and threat picture needed for adequate interagency coordination was known only by a limited number of executive branch leadership and staff. As the Federal Government coordinated its strategic, operational, and tactical activities to respond to the WMD threat, a lack of pre-designated authorities hindered communications with the public and the Federal workforce. Overall, Capstone 2016 reinforced the need to build mechanisms for shared situational awareness in a complex threat environment and for continued comprehensive government-wide planning to strengthen interagency operational coordination.

While the Response mission area remained the most frequently exercised mission area, the other mission areas received increased attention in the 2015–2016 exercise cycle. For example, 41 percent of NEP exercises addressed one or more core capabilities in the Recovery mission area, compared to 27 percent in the 2013–2014 cycle. In 2016, NEP conducted 98 exercises across the country (see Figure 6), which in total tested all 32 core capabilities.

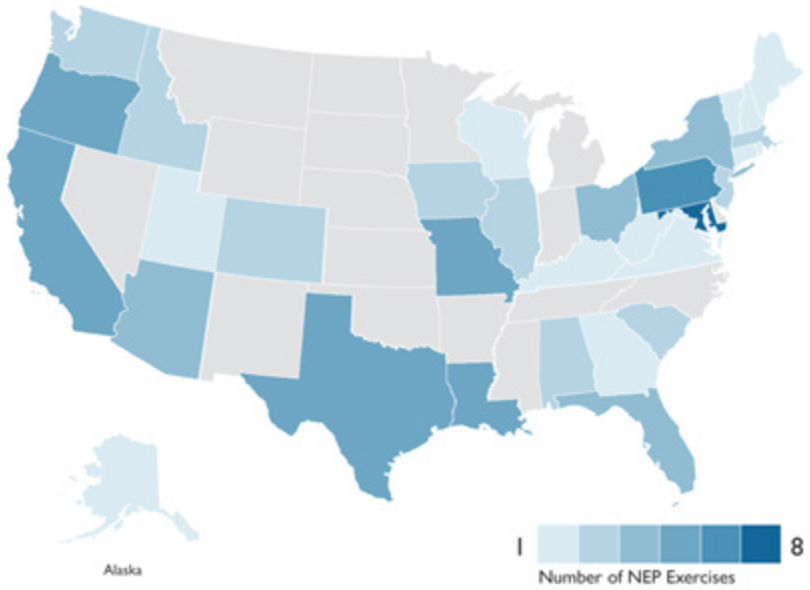


Figure 6. In 2016, NEP exercises across the country tested all 32 core capabilities and addressed a variety of threats and hazards, including active shooter situations, cyber-attacks, and natural disasters.

Based on 2016 exercises, NEP identified 12 findings associated with the current cycle's strategic priorities, each of which aligns to one or more core capabilities (see Table 2).

Table 2. Based on 98 exercises conducted in 2016, NEP identified 12 findings that align to the current cycle's strategic priorities.

Relevant Core Capabilities	Findings
Priority 1: Exchange intelligence, information, data, or knowledge to enable timely and informed decision-making prior to and during an incident that threatens the security of the Nation.	
Intelligence and Information Sharing	▪ Increased understanding of information sharing protocols and procedures across jurisdictions and with whole community stakeholders remains an outstanding need, particularly for classified or sensitive information. ▪ Pre-existing relationships and networks effectively strengthened prevention and mitigation efforts during an incident.
Priority 2: Identify threats and hazards and share prompt, reliable, and actionable risk information with the public, including actions to be taken and assistance made available during the onset of any hazard that threatens the security of the Nation.	
Public Information and Warning	▪ Bringing together a broad range of stakeholders prior to an incident to discuss public messaging methods helps ensure the development of more accessible and actionable messages to the whole community, such as messages that are linguistically and culturally appropriate. ▪ By designating a single agency as responsible for developing and disseminating coordinated messaging, law enforcement and emergency response agencies were able to disseminate consistent and regular messaging to dispel public fear.
Priority 3: Establish and maintain a unified and coordinated operational structure and process, capable of identifying, prioritizing, and delivering resources across all hazards and lead-Federal agency authorities, including catastrophic incidents where a Stafford Act declaration is not likely and domestic response to foreign nations overwhelmed by a disaster.	
Operational Coordination	▪ Insufficient understanding exists among state and local governments, tribal nations, and Federal agencies regarding roles and responsibilities during non-Stafford Act incidents. ▪ Responders have difficulty establishing unified command and coordinating an effective interagency response. ▪ Responders and incident commanders need further training in using the Incident Command System. ▪ State and local responders are not adequately trained to operate key situational awareness systems and software platforms during incident response. ▪ Threat- and hazard-specific response plans are beneficial, and emergency managers and responders should familiarize themselves with these plans. ▪ An effective incident response is tied to effective operational communications.
Priority 4: Establish and maintain plans, authorities, responsibilities, and coordination capabilities that support the recovery of local communities affected by catastrophic disasters.	
Recovery Core Capabilities	▪ NEP exercises reinforced the value of engaging and integrating whole community stakeholders in pre-incident planning. ▪ Increased representation of faith-based, nonprofit, and private sector partners in preparedness activities (e.g., pre-incident planning efforts, training, exercises) is desirable, as emergency managers rely heavily on these partners to supplement government efforts to engage with individuals with disabilities and others with access and functional needs, and ensure support reaches all affected survivors.

Prevention

Mission Area Overview

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

Core Capabilities in Practice

The Prevention mission area focuses on ensuring the Nation is prepared to avoid, prevent, or stop an imminent terrorist attack within the United States. The *National Prevention Framework* ("Prevention Framework") describes seven Prevention core capabilities, including how they interact during an imminent threat.

Being prepared to prevent a terrorist attack in the United States begins with **Intelligence and Information Sharing**, which is the ability to develop situational awareness on the actor(s), method(s), means, weapon(s), or target(s) related to an imminent terrorist threat within the United States. Once an imminent threat has been identified, local, state, tribal, territorial, and Federal partners conduct **Planning** activities to develop appropriate courses of action to prevent the attack. Actions include **Screening, Search, and Detection** operations to effectively identify and locate terrorists and their means, methods, and weapons, as well as subsequent **Interdiction and Disruption** operations to help thwart emerging or developing terrorist plots and neutralize terrorist cells, operatives, and operations. While executing these operations, law enforcement officials use **Operational Coordination** to establish and maintain a unified and coordinated operational structure and process that integrates all relevant stakeholders. Law enforcement officials also conduct their activities in a manner that preserves evidence and the Federal Government's ability to prosecute those who violate the law. **Forensics and Attribution** activities are essential to identify terrorist actors, co-conspirators, and sponsors, and prevent initial or follow-on attacks. Throughout the entire sequence of activities, officials provide **Public Information and Warnings** to share prompt and actionable information with the public and other stakeholders, as appropriate.

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

While much of the work in the Prevention mission area is classified in nature, the following examples highlight publicly shareable actions taken in 2016 to improve preparedness that demonstrate the relationship among select core capabilities in the Prevention Framework:

Forensics and Attribution

The DHS Science and Technology Directorate, in collaboration with the Massachusetts Institute of Technology, developed video forensic tools that enhance the ability of law enforcement and security personnel to rapidly analyze video feeds to conduct unique and specific security assessments for threat indicators and other suspicious behaviors. Amtrak and the Washington Metropolitan Transit Authority are currently testing the tools. The DHS Science and Technology Directorate plans to provide the suite of tools as part of a layered and integrated capability to detect and mitigate threats to surface transportation from explosives.

To improve forensics and attribution capabilities of first responders in cyber-related cases, the FBI's Cyber Division, in collaboration with the International Association of Chiefs of Police and Carnegie Mellon University, developed the Cyber Investigator Certificate Program. Since its inception in October 2015, thousands of law enforcement personnel have received training under this program, which includes modules on recognizing potential sources of digital

evidence, securing digital devices, and documenting digital evidence.

- Planning and Operational Coordination

  In 2016, the Federal Experts Security Advisory Panel (FESAP) comprehensively reviewed biosafety and biosecurity practices for federally funded activities and provided specific recommendations to strengthen these practices. In parallel, the National Science and Technology Council established a committee to seek input from stakeholders into how Select Agent Regulations have affected science, technology, and national security in the United States. Based on stakeholder feedback, the committee developed recommendations on ways to improve the regulatory process and address perceived gaps in the regulations. The Federal Government is currently implementing both sets of recommendations, which address the accounting, security, and physical protection of biological materials. The recommendations include actions, regulatory changes, and guidance to improve biosafety and biosecurity, as well as measures to increase material accountability and oversight, to strengthen security-awareness education and the culture of responsibility, and to optimize inspection processes and incident reporting.

- Interdiction and Disruption and Screening, Search, and Detection

  In fiscal year 2016, DHS's National Counter-IED Capabilities Assessment Database program assessed the capabilities of 415 teams—including bomb squads and Special Weapons and Tactics (SWAT) teams—on their ability to counter IEDs. The program facilitates state and local planning, coordination, and risk assessment efforts and focuses on preparing for IED incidents. In addition, the DHS National Protection and Programs Directorate Office of Infrastructure Protection (IP) delivered 385 courses on counter-IED principles, policies, and programs to more than 8,105 participants in fiscal year 2016. The DHS Office for Bombing Prevention (OBP) also developed three new bomb-threat resources: (1) an instructional video, created with the University of Central Florida, which addresses actions to take when facing a bomb threat; (2) updated planning guidance from DHS and FBI for facilities prone to bomb threats; and (3) a website, "What to Do - Bomb Threat," on DHS.gov that makes bomb threat information and resources more accessible.

- Planning and Operational Coordination

  DOE's National Nuclear Security Administration, in collaboration with FBI, led and conducted the "Atomic Thunder" exercise on December 14, 2016, at the Rhode Island Nuclear Science Center. During the exercise, Federal, state, and local government partners developed plans in response to a hypothetical terrorist threat involving the theft and use of radioactive materials. Throughout the exercise, participants developed methods to communicate and coordinate operational roles when responding to such situations.

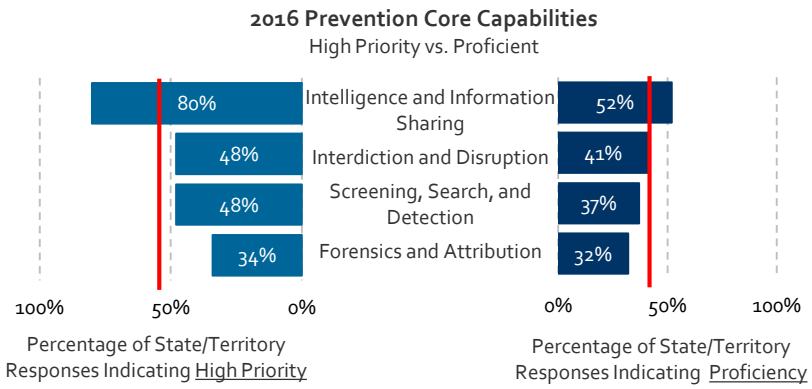
- Screening, Search, and Detection and Intelligence and Information Sharing

  The DHS BioWatch Program, which detects and provides early warning of bioterrorism incidents, continues to support preparedness activities (e.g., pre-event planning and exercises) and screening and detection operations at a number of large-scale events—including Super Bowl 50, and the Republican and Democratic National Conventions. In 2016, the BioWatch Program established a formalized process for quickly notifying its network of Federal, state, and local partners when detection of a biological agent occurs. The process supports greater collaboration and situational awareness across the network of partners and was successfully used in a detection incident in May 2016. More broadly, Biowatch is only one of multiple biosurveillance efforts that help protect the population from emerging infectious diseases.

Summary of Progress

The Nation continues to demonstrate varying levels of capability in and attention to the core capabilities in the Prevention mission area. Key findings in this section describe incremental progress in **Forensics and Attribution**, **Interdiction and Disruption**, and **Screening, Search, and Detection**. This progress is balanced by 2016 State Preparedness Report results, which showed that states and territories rated themselves as less proficient in every Prevention core capability except **Screening, Search, and Detection** compared to 2015.

Prevention core capabilities with higher priority ratings had higher proficiency ratings. Only 32 percent of state and territorial responses to the 2016 State Preparedness Report identified their performance in **Forensics and Attribution** as proficient, placing this core capability in the bottom 10 among all core capabilities (see Figure 7). Moreover, only 34 percent of states and territories rated it as a high priority; states and territories selected nearly all other core capabilities as high priority with greater frequency. In contrast, 52 percent of state and territorial responses reported proficient performance



Notes: Vertical red lines (|) indicate the average ratings for all core capabilities. The chart and statements do not include contributions from the three cross-cutting core capabilities—Planning, Operational Coordination, and Public Information and Warning

Figure 7. In their 2016 State Preparedness Report responses, states and territories provided information on their high priority core capabilities, as well as ratings on core capability proficiency.

in **Intelligence and Information Sharing** capabilities. While a slight decrease from 2015, this is the only core capability not specific to the Response mission area that was among the top ten core capabilities by proficiency. Approximately 80 percent of states and territories also identified it as a high priority (fourth highest). In addition to state and territorial efforts, Federal agencies took modest steps to strengthen **Screening, Search, and Detection** capabilities for radiological materials (see page 28).

Table 3 lists the most frequently identified "functional area" gap for each Prevention core capability, as selected by states and territories in their 2016 State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from an analysis of the Goal, the Prevention Framework, and other national-level preparedness doctrine. **Forensics and Attribution** and **Interdiction and Disruption** were two of the five core capabilities for which states and territories most frequently indicated it was primarily the responsibility of the Federal Government to address gaps.

Table 3. In their 2016 State Preparedness Report responses, states and territories identified remaining gaps in their ability to accomplish various functions associated with each Prevention core capability.

Most Frequently Identified Functional Area Gap in Each Prevention Capability	
Core Capability*	Gap
Forensics and Attribution	Assessing terrorist capabilities
Intelligence and Information Sharing	Gathering intelligence
Interdiction and Disruption	Anti-terrorism operations
Operational Coordination**	Command, control, and coordination
	Establishing a common operating picture
Planning	Whole community involvement and cooperation
Public Information and Warning	New communication tools and technologies
Screening, Search, and Detection	Screening

*For core capabilities that cut across two or more mission areas, the 2016 State Preparedness Report did not include separate data requests that were specific to each mission area. Gaps identified for these core capabilities are identical for the different mission areas.
**The top-two functional area gaps for Operational Coordination were equal in frequency of selection.

The 2017 *National Preparedness Report* identifies **Intelligence and Information Sharing** as a capability to sustain (see page 11). While several indicators (e.g., exercise frequency and State Preparedness Report results) identify this capability as an area of strength, recent declines in proficiency and Federal preparedness grant funding for this capability increase the potential for future gaps to arise. The 2017 *National Preparedness Report* does not identify any Prevention-specific core capabilities as areas for improvement.

By the Numbers

New York State carried out over 600 counterterrorism exercises

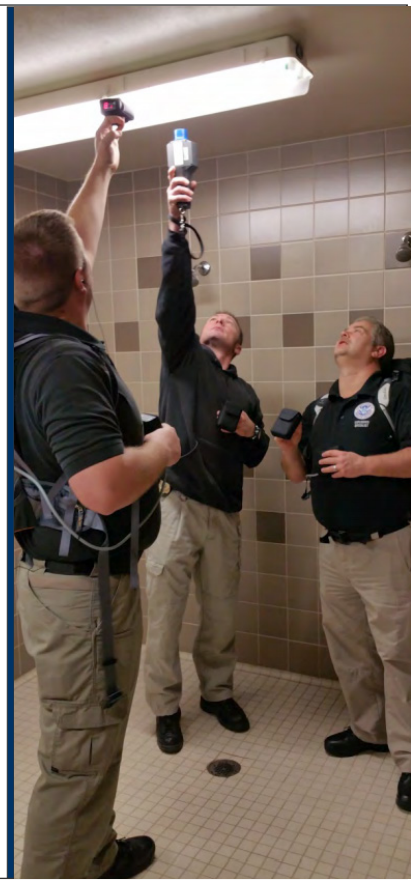
New York State's Division of Homeland Security and Emergency Services—along with New York State Police, the Joint Terrorism Task Force, and local law enforcement—conducted over 600 counterterrorism exercises in 2016 at businesses and organizations across the state to test their suspicious activity reporting programs and counterterrorism plans. In total, nearly 100 law enforcement agencies and 300 personnel supported these unannounced exercises.

The Secret Service trained 1,640 individuals

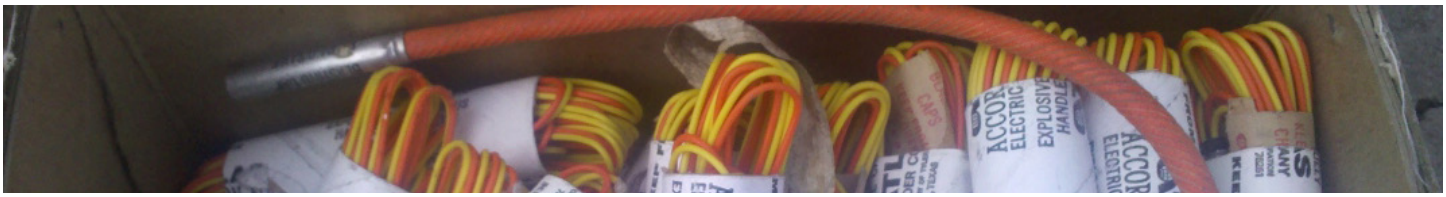
The U.S. Secret Service provided 54 presentations on terrorism trends and tactics to 1,640 total participants—including law enforcement, military, civilian security personnel, first responders, legal officials, and U.S. Secret Service personnel across the country—to better prepare them to prevent and respond to evolving terrorist threats.

The DHS Domestic Nuclear Detection Office conducted 110 deployments

To support state and local security and terrorism prevention capabilities during National Security Special Events (e.g., the Democratic and Republican National Conventions), the DHS Domestic Nuclear Detection Office (DNDO) deployed its six Mobile Detection Deployment Units 110 times in 2016 (compared to 81 times in 2015). These units, which contain radiation detection equipment and staff trained to use it, supplement the radiological and nuclear detection capabilities of local first responders and enhance preparedness against radiological and nuclear threats.



Prevention Snapshots



Bomb-Making Materials Awareness Program

In 2016, the OBP began transitioning implementation of its Bomb-Making Materials Awareness Program to a state-led model. This program helps interdict plots involving bombs at the point-of-sale of explosive precursors. OBP's move to decentralize the program increases training capacity and gives states greater ownership of the training content, enabling them to tailor it to meet their specific needs. OBP has already transitioned control of the program in Texas and Arizona, and a number of states—including Georgia, Tennessee, Florida, North Carolina, and Minnesota—will complete their training for transitioning by July 2017. As each state completes the training, OBP identifies lessons learned to share with other states.

Louisville, Kentucky

The Louisville Metropolitan Police Department established a one-hour training session that seeks to improve officer awareness about IEDs and outlines actions for officers to take following the discovery of such a device. The department requires all police officers to attend the session as a part of recurring mandatory training. Moreover, the city is extending the requirement to all of its emergency services.

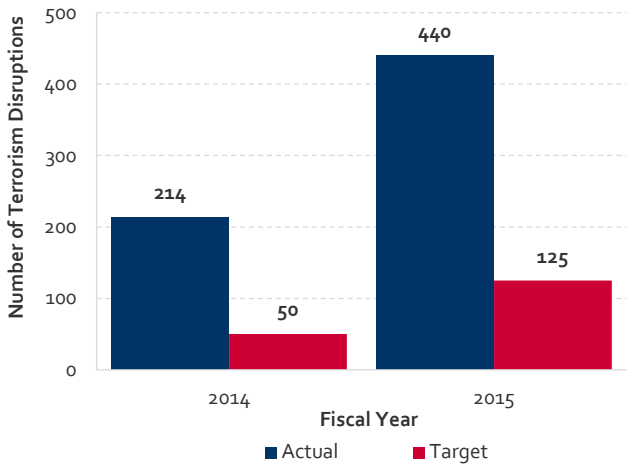
Columbia, South Carolina

On August 1, the South Carolina Department of Public Safety hosted a free anti-terrorism training seminar entitled "Recognizing and Mitigating Suicide Bomber Threats" for Federal, state, and local law enforcement. The seminar included a session on tools for early identification of a suicide bomber suspect and offered best practices based on field experience to enable effective incident response.

PREPAREDNESS INDICATORS

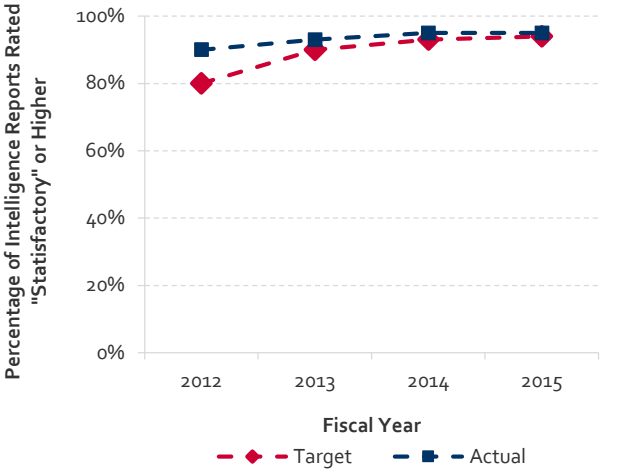
Number of terrorism disruptions by the U.S. Department of Justice (DOJ), primarily by FBI

Preventing and disrupting imminent terrorist attacks is the primary focus of the Prevention mission area. FBI defines a "disruption" as inhibiting or interrupting a threat actor from engaging in criminal or national security-related activity. In fiscal year 2015, DOJ achieved 440 terrorism "disruptions," an increase from 214 disruptions in fiscal year 2014. The fiscal year target values (shown in the figure) represent projections that DOJ determines based on estimated future threats.



Percentage of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to understand the threat

Timely intelligence and information is necessary to keep the homeland safe in a constantly changing threat environment. This measure gauges the extent to which DHS intelligence programs have satisfied their Federal, state, and local customers by producing reports that improve awareness and understanding of potential threats. Specifically, the measure aggregates customer ratings of the relevance, timeliness, and usefulness of these reports. Since fiscal year 2012, DHS has consistently exceeded its targets for this measure.



Prevention

Key Findings

Key Finding:

Federal departments improved their ability to detect insider threats by employing new records-management systems and requiring cleared contractors to maintain formal programs to detect insider threats.

In 2016, DHS and the U.S. Department of Defense (DoD) employed new records-management systems for insider threats to comply with Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" (October 2011). The E.O. directs Federal departments and agencies to establish, implement, monitor, and report on their insider threat-detection and -prevention programs.

DHS began using a database in March 2016 to better manage and investigate the unauthorized disclosure of classified information. In fiscal year 2016, DHS recorded 53 insider threat notifications. The system also helps DHS track its notifications of suspected insider threats to external partners. DoD began using a similar database in October 2016. In addition to meeting E.O. 13587 requirements, the system addresses DoD's need for a "centralized hub" for insider threat data. DoD uses the system to analyze, monitor, and audit information that insider threats may pose to DoD and to other resources.

DoD also changed national industrial security standards to strengthen detection capabilities for insider threats among cleared contractors working for the Executive Branch. Specifically, DoD requires these contractors to maintain an insider threat program consistent with E.O. 13587. This change applies to the approximately 13,000 contractor facilities that are cleared for access to classified information. Cleared contractors must brief all cleared staff on the program before granting them access to classified information. Further, cleared contractors must report information on an insider threat to a designated agency (such as DHS, DoD, or DOE). To help industry comply with this change, agencies have provided Federal and industry representatives with their procedures to help cleared contractors implement compliant insider threat programs.

Prevention Case Study: Transportation Security Administration (TSA) Actions to Improve Its Insider Threat Detection Capabilities

The ability of airport workers to circumvent perimeter and access control security measures and smuggle weapons into restricted areas of airports and onto passenger planes presents a vulnerability for potential terrorist exploitation. DHS, TSA, and FBI consider insider threat to be one of aviation security's most pressing concerns. To address this and other airport perimeter and access control concerns, TSA has enhanced its employee screening practices and capabilities. TSA reported in January 2017 that it increased airport employee screenings, which include physical searches and security background checks, by 43 percent—from 16.9 million in 2015 to 24.2 million in 2016. In addition, TSA conducted a pilot incorporating risk-based scheduling and deployments of security personnel when screening airport employees. The pilot methodology incorporates key requirements defined in the *Federal Aviation Administration (FAA) Extension, Safety, and Security Act of 2016*, including random and unpredictable deployments using game theory and scientific algorithms. TSA also conducted a 90-day pilot test of FBI's Rap Back service (which provides continuous criminal history monitoring) for TSA workers at two major U.S. airports and employees of one commercial airline company. This pilot involved 5,600 individuals covered by the Rap Back service and resulted in 56 notifications of criminal activity and two revoked secure-area access badges. TSA is coordinating with airports and aircraft operators to incorporate the service into their operations. TSA plans to expand the Rap Back service to all U.S. airports by the end of fiscal year 2017. According to TSA, these and other actions taken over the past few years have reinforced layers of security already in place to stop a potential terrorist attack.

Key Finding:

In 2016, DHS's Office of Intelligence and Analysis (I&A), in collaboration with Federal, state, and local partners, implemented an enhanced process for assessing fusion center performance.

The National Network of Fusion Centers reached maturity in 2015, achieving the full capability to integrate resources among and between individual fusion centers and share intelligence across all levels of government. To further assess the network's performance and help fusion centers mitigate capability gaps, DHS I&A piloted an enhanced assessment process in 2016 that includes 18 performance measures. Specifically, these measures characterize how fusion centers in the network improve Federal, state, local, tribal, and territorial understanding of threat information, and the impact of the network's analytical products and support activities on law enforcement and counterterrorism operations. The enhanced assessment will facilitate improvements in fusion center performance by identifying potential areas in which additional resources should be dedicated.

In 2016, the enhanced assessment measured fusion center outputs in several areas. For example, fusion centers vetted 76,743 tips and leads by fusion centers. Of those, fusion centers provided 39,472 to other Federal, state, local, tribal, and territorial agencies for follow up action. In addition, DHS found that the fusion centers played a direct role in responding to 52 public safety incidents in 2016.

The 77 fusion centers that participated in the pilot assessment (out of 78 total in the network) also demonstrated strong performance in the following areas:

- ***Alignment with Intelligence Community (IC) Needs:*** *Fusion centers made improvements in meeting the demand for intelligence products that address specific IC needs as a result of increased collocation and collaboration within the network. The percentage of Intelligence Information Reports (IIRs) published by DHS I&A that originated from fusion center information and met the specific needs of the IC increased from 90 percent in 2015 to 100 percent in 2016. In addition, 53 percent of fusion distributable center analytic products addressed a specific IC need.*
- ***Usability of Intelligence Products:*** *In addition to increasingly meeting intelligence product demands, the percentage of Federal IIRs originating from fusion center information that the IC used in performing its mission—such as addressing critical intelligence gaps, corroborating existing information, or helping to define an issue or target—increased from 86 percent in 2015 to 98 percent in 2016.*

PREVENTION CASE STUDY: HSIN EXCHANGE

DHS in collaboration with the Terrorist Screening Center (TSC), implemented HSIN Exchange in September 2016 to strengthen information sharing capabilities within and across the National Network of Fusion Centers, and with the TSC. HSIN Exchange builds off of HSIN, an information platform fusion center partners use to share sensitive but unclassified information. HSIN Exchange enhances information and intelligence sharing capabilities within the network by providing two main advantages:

- *HSIN Exchange increases the speed and efficiency of sharing information between fusion centers, as well as with the TSC, because it is a centralized information request management system that replaces multiple, often duplicative individual management systems.*
- *HSIN Exchange uses a standardized process that allows requests for information to be easily tracked from initiation through closeout. These requests for information, which are an essential part of the information sharing and collaboration support among fusion centers and their partners, involve providing analytical assistance or information that could help identify emerging criminal or terrorist activity, and support emergency management operations.*

Key Finding:

The Federal Government has taken steps to improve the security of radioactive materials and enhance its detection capabilities for radiological and nuclear materials.

Radioactive materials serve beneficial purposes, but can pose serious threats in the wrong hands, such as a terrorist seeking to construct a dirty bomb. U.S. Government Accountability Office (GAO) evaluations have previously revealed radioactive

material security vulnerabilities, such as weaknesses in Nuclear Regulatory Commission (NRC) and "Agreement State"[3] procedures for issuing licenses to possess radioactive materials. To improve the security of radioactive materials, NRC has taken several steps. For example:

- *NRC and state working groups are implementing modifications to guidance that NRC provides to states for evaluating license applicants and verifying licenses.*
- *NRC has conducted training on licensing processes and guidance for NRC and Agreement State officials and will continue to provide new and updated training to ensure adequate implementation of licensing practices. As part of this training, NRC has emphasized, among other things, the need for greater scrutiny when conducting site visits of applicants' facilities.*
- *NRC currently requires on-site security reviews for higher-level quantities of radioactive materials, and is considering extending such on-site reviews to cover smaller sources as well.*

The NRC has also formed an NRC-Agreement State working group to evaluate whether existing regulations and processes governing source protection and accountability for lower-level quantities of radioactive material (namely, Category 3 quantities[4]) continue to ensure adequate protection of public health and safety. The working group will consider numerous items, including potential changes to methods for license verification and source tracking for lower-level quantities of radioactive material based on consideration of the vulnerability of such materials, the risk posed by the materials, and the current threat environment. The working group's recommendations will be provided to the Commission for consideration in August 2017. These are a sample of the initiatives NRC has undertaken and continues to undertake to ensure the safety and security of radioactive materials used for beneficial commercial, academic, and medical applications in the United States. Other notable initiatives include:

- *The NRC leads the Radiation Source Protection and Security Task Force, which was established by the Energy Policy Act of 2005. The task force evaluates the security of radiation sources in the United States from potential terrorist threats, including acts of sabotage, theft, or use of a radiation source in a radiological dispersal device or a radiological exposure device. The task force comprises independent experts from 14 Federal agencies and one state organization, and is chaired by NRC. The task force meets routinely to discuss matters pertaining to radioactive materials security and provides reports on its efforts to the U.S. President and Congress every four years, with the next report planned for completion in 2018.*
- *The NRC completed an evaluation of the regulation for the security of risk-significant radioactive material, 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," in 2016. As a result of the review, NRC concluded that the rule is effective in protecting risk-significant radioactive material from theft or diversion. The results of the review were reported to Congress in December 2016, and recommendations developed during the review are being used to enhance licensee implementation of security measures for the protection of risk-significant radioactive material currently in use in the United States.*

DoD, through its Defense Advanced Research Projects Agency (DARPA), has taken steps to enhance detection capabilities for nuclear and radiological materials. In 2016, working with the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism, DARPA sponsored two tests of its SIGMA program. SIGMA was launched to develop and test low-cost, high-efficiency radiation sensors networked via smartphones to provide Federal, state, and local

[3] The Atomic Energy Act authorizes the NRC to enter into agreements with states in which it relinquishes its regulatory authority over specified radioactive materials. These Agreement States can grant licenses to possess and use radioactive materials and sealed sources and are responsible for conducting regular inspections of licensees.

[4] Thresholds for radioactive material quantities (e.g., Category 1, 2, 3) are included both in the International Atomic Energy Agency Code of Conduct on the Safety and Security of Radioactive Sources and in 10 CFR Part 37. "Risk-significant" quantities of radioactive material are defined as those meeting the thresholds for Category 1 and Category 2.

officials with real-time awareness of potential nuclear and radiological threats. A 1,000-sensor deployment in Washington, D.C. in October demonstrated the program's ability to provide minute-to-minute information concerning radiological and nuclear threats. DARPA plans to continue testing SIGMA on city and regional scales; achieve the ability to continuously monitor large geographic areas in 2017; and transition the system to Federal, state, and local entities in 2018.

Prevention Case Study: 2016 Nuclear Security Summit Outcomes

For decades, the Federal Government has devoted attention to the security of other countries' fissile materials to prevent their use by hostile actors, either abroad or within the United States. The Nuclear Security Summit, first held in 2010, is a world summit aimed at securing nuclear materials and preventing nuclear terrorism. In April, following the March 2016 Nuclear Security Summit, the Federal Government announced measures that the United States will take to support these efforts. These include strengthening other countries' nuclear forensics capabilities and hosting exercises, workshops, and other activities to build partner nations' nuclear security capabilities.

Protection

Mission Area Overview

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

Core Capabilities in Practice

The Protection mission area aims to secure the homeland against acts of terrorism and human-induced or natural disasters. The *National Protection Framework* ("Protection Framework") describes 11 Protection core capabilities, including how they operate together to safeguard the Nation against all hazards.

Protecting the Nation requires understanding the threat environment. This understanding is accomplished through **Intelligence and Information Sharing** (i.e., the collection and distribution of timely, accurate, and actionable data), including sharing intelligence and information between the public and private sectors. Through a process of **Risk Management for Protection Programs and Activities**, officials evaluate the likelihood of, vulnerability to, and consequences of different threats against an asset, individual, or event. Once a possible threat vector is identified and its risk is understood, emergency managers disseminate **Public Information and Warning**, as needed. Steady-state protection operations—those conducted regardless of knowledge of an imminent attack, including **Screening, Search, and Detection**, and **Interdiction and Disruption** activities—are routinely informed by the intelligence and risk-management cycles. These operations are conducted using **Operational Coordination** structures to integrate all relevant stakeholders.

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

Public and private stakeholders apply the remaining steady-state core capability measures, as appropriate. **Access Control and Identity Verification**, for example, controls admittance to critical locations and systems, and is essential for both **Cybersecurity** and **Physical Protective Measures**. **Supply Chain Integrity and Security** helps strengthen the resilience of the Nation's critical supply chains from intentional disruptions or natural hazards. Government officials and private and nonprofit organizations implement all the above capabilities aligned with procedures identified during the **Planning** process, which are then tested and refined during relevant exercises.

The following are examples of actions taken in 2016 to improve preparedness that highlight the relationship among select core capabilities in the Protection Framework:

- Planning and Risk Management for Protection Programs and Activities

  Through the Hometown Security Initiative, IP conducts outreach with businesses and faith-based organizations and provides expert advice and recommendations about measures they can implement to protect facilities, public-gathering sites, and special-event venues. As of January 2017, DHS Protective Security Advisors have shared information and provided technical assistance in more than 2,800 engagements. For example, DHS encourages businesses to take four steps—connect, plan, train, and report—in advance of an incident to better prepare their employees to think about their role in ensuring the safety and security of their businesses and communities. DHS

has also established a "Hometown Security" website to make it easier for the public to find community tools and resources about protective measures. Similarly, the DHS Center for Faith-based & Neighborhood Partnerships worked with FEMA to establish a website, "Resources to Protect Your House of Worship," to make it easier for faith-based organizations to find tools, resources, and partners to help them meet their unique needs.

- Screening, Search, and Detection

  In 2016, U.S. Customs and Border Protection (CBP) began implementing new biometric screening technologies at major U.S. airports to enhance the collection and verification of entry and exit data. Among other benefits, this data helps officials determine whether individuals suspected of terrorism involvement have left the United States. For example, CBP deployed facial comparison technology at select U.S. airports. This technology takes photos of passengers and compares them to the image in the ePassport that they present. CBP discards photos taken of American citizens upon verification. CBP also began using mobile fingerprint collection devices to collect biometric data for outbound operations at 10 international airports and plans to expand these efforts. At the Hartsfield-Jackson Atlanta International Airport, CBP tested and implemented a new departure information system to identify improved, cost-effective real-time photo-matching capabilities that can be deployed at exit points nationwide.

  CBP also tested new biometric data collection technology at a land-based departure point. In May 2016, CBP completed the first test on facial and iris identification technology at a U.S. land border crossing—Otay Mesa, California. The results of this test will help CBP determine whether the technology improves identification of visa overstays and persons of law enforcement or national security interest.

Summary of Progress

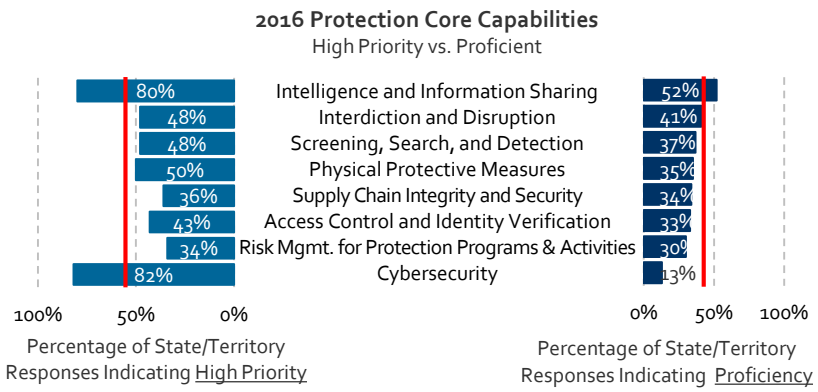
Despite evidence of progress in this year's key findings, the Nation remains less proficient in delivering some capabilities in the Protection mission area. Key findings and 2016 State Preparedness Report results identify progress in **Access Control and Identity Verification** and **Screening, Search, and Detection**. Of the 10 capabilities that states and territories rated themselves as having low proficiency in, however, four are in Protection. The 2017 *National Preparedness Report* identifies **Supply Chain Integrity and Security**, **Risk Management for Protection Programs and Activities**, and **Cybersecurity** as national areas for improvement (see page 12). One Protection capability—**Intelligence and Information Sharing**—is a capability to sustain in this year's report (see page 11).

Real-world incidents in 2016 underscore the mixture of progress and remaining challenges occurring across the Protection mission area. For example, even as **Access Control and Identity Verification** continues to improve following the 2015 OPM breaches (see page 38), the Nation continues to face numerous **Cybersecurity** challenges. These challenges include increased malicious cyber activity directed at public and private services (see page 37), voter registration systems (see page 37), and cyber infrastructure (see page 9). Despite a high degree of interest in **Cybersecurity**—82 percent of states and territories selected it as a high priority (third among all core capabilities)—the capability remained both the lowest rated core capability in proficiency and the capability in greatest danger of decline.

More broadly, State Preparedness Report data reflects both positive and negative changes in capability across the Protection space.[5] Between 2015 and 2016, states and territories reported proficiency gains of approximately three percent in **Supply Chain Integrity and Security** and **Access Control and Identity Verification**—representing the third and fourth largest increases among all core capabilities. Both, however, remain below average among all core capabilities as ranked by proficiency (see Figure 8). In contrast, **Risk Management for Protection Programs and Activities** declined in proficiency by four percent and **Intelligence and Information Sharing** declined by five percent. Nevertheless, **Intelligence and Information Sharing** remained the only Protection capability for which more than half of states and territories rated themselves as proficient. When looking towards the future, states and territories only expressed increasing concern for **Access Control and Identity Verification** as a Protection core capability in greatest danger of decline.

In addition to proficiency, states and territories also exhibited variable views on the importance they placed on various Protection core capabilities. **Cybersecurity** and **Intelligence and Information Sharing** ranked in the top five in terms of

[5] Unless otherwise noted, figures and statements do not include contributions from the three core capabilities common to all mission areas—i.e., Planning, Operational Coordination, and Public Information and Warning.



Notes: Vertical red lines (|) indicate the average ratings for all core capabilities. The chart and statements do not include contributions from the three cross-cutting core capabilities—Planning, Operational Coordination, and Public Information and Warning

Figure 8. In their 2016 State Preparedness Report responses, states and territories provided information on their high priority core capabilities, as well as ratings on core capability proficiency.

priority, whereas **Risk Management for Protection Programs and Activities** ranked in the bottom five. Proficiency rankings often aligned to priority rankings, with **Cybersecurity** the most notable exception. In more recent years, fewer states and territories have identified Protection core capabilities as high priority. Between 2015 and 2016, the average number of states and territories identifying each Protection core capability as high priority decreased by an average of five states and territories. Moreover, with the exception of **Cybersecurity**, **Intelligence and Information Sharing**, and **Interdiction and Disruption**, Protection core capabilities have experienced consecutive years of decreasing priority anywhere from two to four years.

Table 4 lists the most frequently identified "functional area" gap for each Protection core capability, as selected by states and territories in their 2016 State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from an analysis of the Goal, the Protection Framework, and other national-level preparedness doctrine.

Table 4. In their 2016 State Preparedness Report responses, states and territories identified remaining gaps in their ability to accomplish various functions associated with each Protection core capability.

Most Frequently Identified Functional Area Gap in Each Protection Capability	
Core Capability*	Gap
Access Control and Identity Verification	Verifying identity
Cybersecurity	Continuity of operations for information technology systems and networks
Intelligence and Information Sharing	Gathering intelligence
Interdiction and Disruption	Anti-terrorism operations
Operational Coordination**	Command, control, and coordination
	Establishing a common operating picture
Physical Protective Measures	Site-specific and process-specific risk assessments
Planning	Whole community involvement and cooperation
Public Information and Warning	New communication tools and technologies
Risk Management for Protection Programs and Activities	Risk assessment
Screening, Search, and Detection	Screening
Supply Chain Integrity and Security	Analysis of supply chain dependencies

* For core capabilities that cut across two or more mission areas, the 2016 State Preparedness Report did not include separate data requests that were specific to each mission area. Gaps identified for these core capabilities are identical for the different mission areas.
** The top-two functional area gaps for Operational Coordination were tied in terms of how frequently they were selected.

By the Numbers

DOE has provided Cybersecurity Capability Maturity Model (C2M2) toolkits to 921 recipients

In 2016, DOE worked with energy sector partners to expand participation in its C2M2 program, as well as update and enhance C2M2 tools to better account for evolving cyber threats. The program offers several tools to help electricity, oil, and natural gas utilities evaluate the maturity of their cybersecurity programs, and identify and prioritize ways to enhance their cybersecurity posture. Since the program's launch in June 2012, 921 organizations have requested and received the C2M2 toolkit (as of the end of 2016).

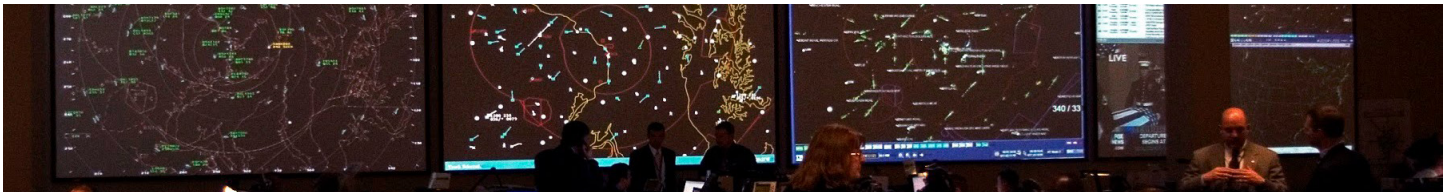
DHS identified eight coordinating activities for the Protection core capabilities

In August 2016, DHS published the first edition of the *Protection Federal Interagency Operational Plan* (Protection FIOP). The Protection FIOP describes eight coordinating activities (e.g., Border Security, Critical Infrastructure Security and Resilience) that are the primary, but not exclusive, Federal coordinating mechanisms for building, sustaining, and delivering the Protection core capabilities.

The DHS Office of Cybersecurity and Communications issued 12,187 Cyber Hygiene Reports

In fiscal year 2016, the DHS Office of Cybersecurity and Communications National Cybersecurity Assessments and Technical Services team conducted vulnerability scans of public, Internet-connected information systems for hundreds of Federal, state, local, tribal, and territorial government stakeholders, producing 12,187 Cyber Hygiene Reports. These reports include recommendations for addressing identified vulnerabilities, enhancing the ability of stakeholders to protect against potential exploitation by malicious actors.

Protection Snapshots



City of Los Angeles Supply Chain

In 2016, The Los Angeles Emergency Management Department, in partnership with FEMA's National Integration Center, conducted an assessment of the resilience of the city's supply chains to a major earthquake scenario. The assessment found areas for improvement in logistics planning for six critical supply lines: water, food, pharmaceuticals, medical goods, fuel, and transportation. One notable finding is the lack of redundancies among pharmaceutical distributors. Only three companies circulate up to 90 percent of pharmaceuticals in the city.

PhotoDNA

In May 2016, Microsoft announced it would provide support to computer scientists at Dartmouth College to use its PhotoDNA program to track terrorist content on social media. The software develops a digital fingerprint for images that can be tracked across the Internet, enabling social media platforms to quickly detect and remove previously flagged content. In December 2016, Facebook, Microsoft, Twitter, and YouTube announced a collaborative effort to better share the fingerprints of terrorist media, such as those generated by PhotoDNA, in order to counter the proliferation of violent extremist content on their sites.

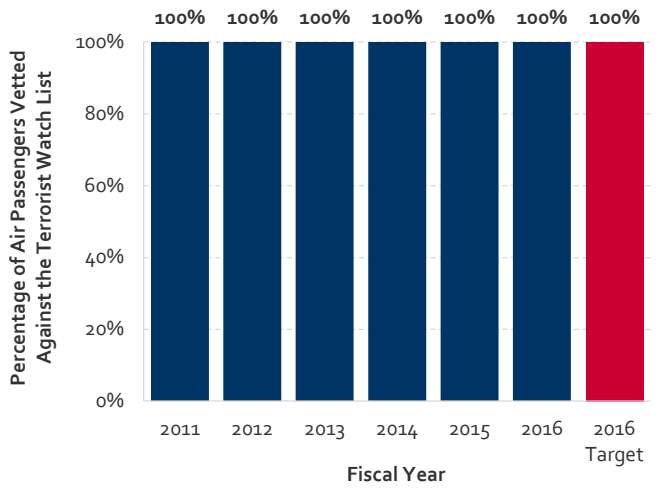
TSA Airport Operations Center (AOC)

In spring 2016, TSA established the AOC, a public-private partnership with the airline industry to address the increase in passengers for the 2016 summer travel season. The AOC tracks daily screening operations and reassigns officers, canines, and other resources to meet demand in advance of predicted passenger volume. These efforts improved TSA's ability to deploy resources to screen the record number of passengers during the summer months.

Preparedness Indicators

Percentage of international air passengers vetted against the terrorist watchlist through Secure Flight

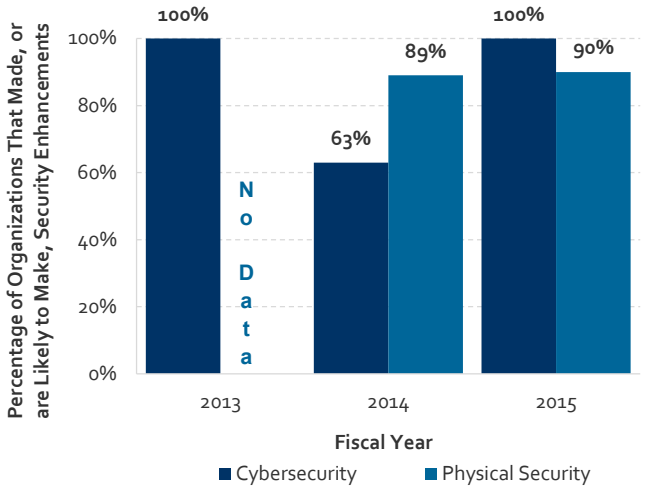
Screening travelers reduces the likelihood of terrorists entering the country. Secure Flight is a risk-based passenger prescreening program that TSA uses to identify low- and high-risk passengers before they arrive at the airport by matching their names against trusted traveler lists and a watchlist. Specifically, this measure tracks the percentage of air passengers traveling in and out of the United States who are screened against the Terrorist Screening Database, the U.S. Government's consolidated database of individuals who are known or reasonably suspected of being involved in terrorist activities. Over the past six years, TSA has met its target goal of screening 100 percent of these international travelers.



Cybersecurity: Percentage of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey

Physical Security: Percentage of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements

Vulnerability assessments enable critical infrastructure owners and operators to tailor protective measures to their needs. The first measure tracks the extent to which organizations have changed their cybersecurity policies and procedures after DHS cyber assessments. The second measure tracks the percentage of facilities that are likely to inform their security and resilience enhancements using information from DHS vulnerability assessments focusing on physical security. Results suggest that these assessments are prompting critical infrastructure owners and operators to take additional protective actions. In fiscal year 2015, the percentage of organizations incorporating an enhancement based on cyber assessments was 100 percent. The percentage of facilities likely to incorporate an enhancement based on a physical security-oriented assessment was 90 percent.



Protection

Key Findings

Key Finding:

A rise in ransomware (a form of malware) attacks threatens the delivery and continuity of critical services, such as healthcare services.

Ransomware attacks, which lock users out of data files, rose in 2016, threatening critical services such as healthcare and law enforcement. Attacks increased by 300 percent over the first several months of 2016, from an average of 1,000 to 4,000 attacks daily. Victims in the United States paid more than $209 million in ransom payments during the first quarter of 2016, compared to $25 million in all of 2015. One report found that up to three-quarters of healthcare entities may have been victims of ransomware attacks over a 12-month period (starting in 2015). An April 2016 survey of 61 healthcare technology officers found that more than half had reported their facility as being a victim of ransomware attacks in the previous 12 months. Rising rates of ransomware attacks have also affected government networks and services, including law enforcement. Since 2013, ransomware attacks have affected police in at least seven states.

Throughout 2016, Federal departments and agencies took actions to address the challenges of ransomware. For example, the Federal Government published guidance and best practices to private industry and state and local partners to discourage victims from making ransomware payments. The FBI issued two alerts and one notification, which included information on indications of compromised systems and aimed to raise awareness of the threat. HHS alerted healthcare executives to the threat, presented at webinars and industry conferences, published technical assistance resources, and is supporting a task force that is developing recommendations for Congress on steps to improve cybersecurity within the healthcare industry. HHS also published guidance on best practices in the prevention of and response to ransomware attacks. Non-Federal partners supplemented these efforts. For example, the Center for Internet Security—in partnership with FBI, the U.S. Secret Service, and relevant industry information-sharing organizations—conducted a 14-city awareness campaign in 2016 to educate over 4,000 corporate executives on ransomware threats.

Key Finding:

Malicious cyber activities targeting voter registration systems prompted local, state, and Federal government agencies to increase collaboration in order to secure election systems.

Attacks on voter registration systems in 2016 contributed to concerns about the vulnerability of election results to cyberattacks. Arizona and Illinois confirmed attempted attacks on voter registration systems in the summer, and FBI reported that other states were likely targeted by malicious actors. However, while voter registration systems faced threats, several factors make other types of voting systems resilient to cyberattacks. For example, machines used to cast votes are not connected to the Internet. Attempts to alter voting systems to affect election outcomes would require large-scale, coordinated physical and cyber manipulation of thousands of individual ballot boxes. Moreover, elections are decentralized across thousands of local jurisdictions using a range of software and hardware, reducing the number of common vulnerabilities nationwide. Variation across voting systems, however, means that the Federal Government faces challenges in issuing standardized assistance to state and local jurisdictions.

To better understand these challenges, DHS collaborated with the National Association of Secretaries of State in August to

establish the Election Infrastructure Cybersecurity Working Group. The group collected data on election-related cyber threats and disseminated best practices. DHS also encouraged state and local election agencies to leverage the department's risk and vulnerability assessments. To further promote best practices in the lead-up to the election, the U.S. Election Assistance Commission circulated a checklist and resources on securing voters' data. Prior to the election, 49 state and local election agencies sought cybersecurity assistance from DHS. Such assistance included scanning systems connected to the Internet and conducting risk and vulnerability assessments for important networks, such as those responsible for online voter registration and reporting votes on election night.

In January 2017, DHS designated election infrastructure as a subsector of Government Facilities—one of 16 critical infrastructure[6] sectors. The new designation enables DHS to more easily prioritize cybersecurity assistance to state and local election officials. State and local governments maintain control over the administration of elections in their jurisdictions, though they may request additional aid from the Federal Government to help strengthen, secure, and maintain voting or polling systems.

PROTECTION CASE STUDY: VOTER REGISTRATION SYSTEM BREACHES

Malicious actors target voter registration systems either to extract personal details for identity theft or to disrupt election processes. In the one public case where voter registration data was accessed (Illinois), state election officials reported that malicious actors viewed as many as 90,000 records, exposing information such as names, dates of birth, and driver's license numbers. However, no evidence exists that these actors attempted to modify voter data. In all cases, including those in which details are not available to the public, the IC found no evidence that attacks inhibited voters' ability to cast ballots in the election or targeted vote counting systems.

Key Finding:

Lessons learned from the 2015 OPM data breaches continue to prompt actions to better safeguard sensitive data on government employees and contractors, and to update procedures for background investigations and security clearances.

Protecting personal information housed by the Federal Government against malicious cyber activity remains a longstanding challenge. Attacks on these systems can jeopardize preparedness, exposing data on individuals with background investigations and security clearances and slowing the clearance process. In response to the 2015 OPM breaches, the Federal Chief Information Officer issued guidance in January 2016 to enhance the security and effectiveness of background investigations, including phasing out vulnerable systems. Additionally, the Federal Government created the National Background Investigations Bureau (NBIB) to process the one million annual requests for investigations from Federal agencies in an effort to provide renewed oversight and guidance. NBIB's leadership includes a dedicated senior official for privacy to further ensure the safety of personal data. To better safeguard sensitive data on government employees and contractors, DoD is working with OPM to improve the security of their network.

The Federal Government has also adopted procedural changes to how it safeguards the issuance, maintenance, and protection of background investigations and security clearances. OPM has also increased the frequency with which its

[6] The *Critical Infrastructure Protection Act of 2001* defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

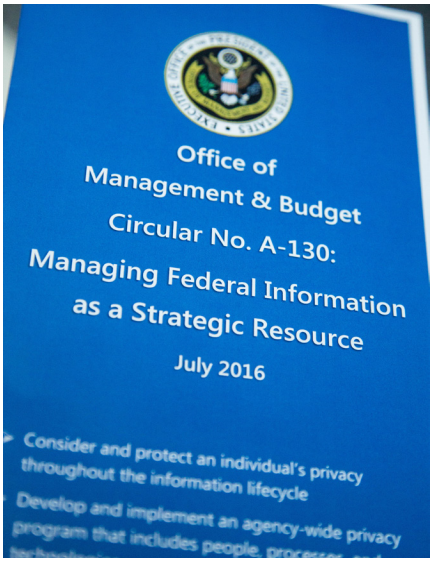
networks are scanned for evidence of tampering or intrusion to better detect vulnerabilities on Federal systems related to background investigations. Additionally, the White House and OPM continued to pursue a wider series of changes to the background investigation process enacted after the 2015 breaches. OPM is launching programs to ensure that employees' needs for security clearances are continuously reassessed in relation to their duties and that all clearance holders undergo more frequent reinvestigations.

The White House is focusing continued attention on ensuring that users on government systems are who they say they are, which will carry cybersecurity benefits across Federal networks and operations. This is also true of Federal systems accessed by constituents. NIST is in the process of a major update to Special Publication 800-63, "Digital Identity Guidelines," to modernize the types of authenticators acceptable to government and better allow agencies to adopt market innovations. Additionally, the document updates approaches to identity proofing and provides guidelines for agencies to accept commercially provided credentials for access to government services.

Key Finding:

The IC and Federal oversight groups have enhanced privacy protections for intelligence-related information collection.

The Federal departments and agencies that compose the IC took steps to improve U.S. citizen and lawful permanent resident privacy protections and the transparency of intelligence collection and information sharing. These steps are consistent with legal requirements to protect these individuals' privacy rights, while accomplishing important national security missions. The National Security Agency (NSA) found that the IC continued to strengthen privacy protections of personal information through various means, such as training and internal policies. The agency's *Intelligence Reform 2016 Progress Report* noted that the IC continued to enhance and institutionalize transparency through public engagement. In addition, a May 2016 DHS Office of the Inspector General report, *Office of Intelligence and Analysis Can Improve Transparency and Privacy*, found that DHS I&A has made progress in protecting privacy by centralizing oversight of privacy and civil liberties and by working to meet the requirements of legislation, regulations, directives, and guidance. DHS I&A also conducted specialized training for employees on privacy and civil liberties safeguards.



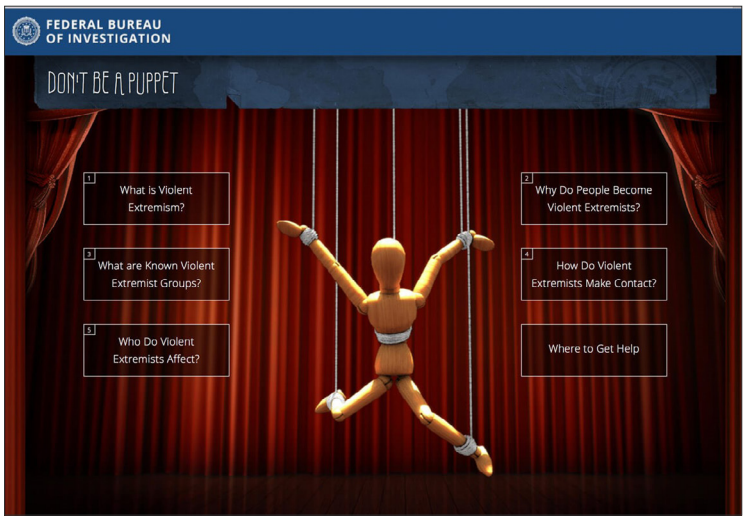
In July, the Office of Management and Budget updated the Federal Government's governing document for establishing how departments and agencies should manage their information resources to account for the dramatic changes in IT, data governance, and security that have occurred since 2000, when the document was last updated. The updated document establishes minimum requirements for Federal privacy programs for the first time, replaces outdated privacy and information-security requirements with new ones, and outlines practices that agencies should incorporate when managing information resources that involve personally identifiable information (PII). In addition, E.O. 13719 (issued in February 2016) established the Federal Privacy Council as the principal interagency forum for improving the privacy practices of Federal agencies and entities acting on their behalf. Over 350 privacy professionals from across the Federal Government participated in the council's Federal Privacy Summit in November, which addressed privacy issues such as encryption, privacy risk assessment, and health privacy.

Key Finding:

Government, academic, and private-sector partners continue to take steps to counter violent extremism through domestic education and other initiatives, including countering terrorist use of social media.

In 2016, the Federal Government continued to build both infrastructure and capacity for countering violent extremism (CVE) activities. In January, DHS and DOJ announced the Countering Violent Extremism Task Force to manage the synchronization

and integration of CVE initiatives across the Federal Government. The task force regularly convenes partners to coordinate and share U.S. Government–funded CVE research and analysis. The National Counterterrorism Center (NCTC) also holds quarterly interagency CVE roundtables, which provide the only classified forum for analysts and policymakers to discuss recent IC products and policy developments. DOJ increased its CVE staff from one attorney with collateral responsibilities to four full-time staff members. Additionally, in October, the White House released an updated *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* that calls for strengthening collaboration with the private sector and academia to pursue CVE-relevant communications tools and capabilities. Also in October, DHS released *Department of Homeland Security Strategy for Countering Violent Extremism*, which outlines its approach to CVE and aligns with the White House's strategic implementation plan.



The Federal Government has also continued to pursue community engagement to support CVE efforts. In 2016, FBI and its partners broadened outreach campaigns to counter violent extremism among young people, whom violent extremist groups target for recruitment through the Internet and social media. The FBI published a guide for preventing radicalization to violence in high schools to help these institutions better understand the topic of violent radicalization and identify warning signs. The FBI also launched an interactive website, "Don't Be a Puppet," which combines videos and interactive activities to deliver narratives counter to messages that target teenagers and promote radicalization to violence. In the first eight months since its launch, the website received over 280,000 page views. Among other efforts, the DHS Office for Civil Rights and Civil Liberties delivered Community Awareness Briefings to community stakeholders and law enforcement officers nationwide. Community Awareness Briefings share unclassified information with communities regarding the threat of radicalization to violence. In addition, Federal agencies have sought to expand their outreach through train-the-presenter efforts. The NCTC has trained dozens of local partners to present Community Awareness Briefings and the DHS Office of Civil Rights and Civil Liberties is developing a program to train local law enforcement officials to deliver awareness briefings to their fellow officers.

Students from around the country, with support from Federal and non-Federal partners, also developed their own outreach initiatives. In 2015, DHS worked with DoD, NCTC, and the Department of State to develop the Peer to Peer Challenging Extremism contest. The contest, which challenges educational institutions to develop innovative social media campaigns for countering violent extremism, has expanded from 23 universities to more than 130 around the world in 2016. Under the program, students compete to design, implement, and measure the success of a product or tool that counters violent extremist messages. In June 2016, a team of students from the Rochester Institute of Technology won first place for their "It's Time: ExOut Extremism" social media campaign. The campaign seeks to counter violent extremist narratives by informing Internet users about their possible exposure to violent extremist content when surfing the web or using social media platforms. It also identifies ways in which users can protect themselves by avoiding violent extremist messaging on the Internet and contribute to positive narratives against online violent extremist messaging.

Private technology companies have also contributed to CVE efforts. For example, Google's technology incubator company, Jigsaw, developed a pilot project with other companies to redirect online users susceptible to ISIS's message to YouTube videos that debunk ISIS recruiting themes and strategies. During the tool's pilot test, which lasted eight weeks, 320,000 individuals watched over half-a-million minutes of 116 videos discrediting ISIS recruitment themes. Twitter has also sought to counter terrorists' use of social media to radicalize and recruit followers. As of August 2016, daily suspensions on Twitter of terrorist-linked accounts were up over 80 percent from the previous year. Since mid-2015, the company has suspended at least 360,000 accounts connected to terrorist groups.

Key Finding:

Among the different measures adopted to address the Zika epidemic, states, territorial, and local governments, as well as Federal agencies, effectively distributed preventative supplies and communicated protection measures.

Zika emerged in the Americas in late 2015 and has spread throughout the Western Hemisphere. While infected adults can experience no to mild, flu-like symptoms, Zika infection during pregnancy can cause serious birth defects. Protecting infants from congenital Zika syndrome defects is the driving motivation for U.S. Government efforts.

Zika virus disease primarily spreads through infected mosquitoes, but can also be transmitted through sexual contact and transfusion of infected blood products. A pregnant woman can pass the Zika virus to her fetus during pregnancy or around the time of birth. An analysis presented in the April 7, 2017, edition of the CDC's *Morbidity and Mortality Weekly Report* found that 10 percent of pregnancies with laboratory-confirmed Zika virus infection resulted in Zika virus–associated birth defects. Because a Zika vaccine has yet to be fully tested and licensed, the best way to protect oneself from the Zika virus is by taking steps to prevent mosquito bites and the spread of the virus through sexual intercourse. The CDC has developed resources to help all levels of government communicate personal protective measures for preventing Zika virus infection. To help communities promote public awareness of personal protective measures, CDC issued guidance documents in 2016 to inform all levels of government on best practices for Zika virus outreach:

- *The* Zika CDC Interim Response Plan *outlines communication and community education activities to prepare state and local jurisdictions where local mosquito-borne transmission is possible.*
- *The* Zika Communication Planning Guide for States *provides states with the resources to develop their own tailored communication strategies and includes sample public outreach products, as well as clinical communication products and deliverables.*
- *The Zika Community Action Response Toolkit (Z-CART) provides a template for state, local, and tribal agencies to develop strategies in the event of a local mosquito-borne transmission of the virus.*
- Interim Recommendations for Zika Vector Control in the Continental U.S. *provides guidance for states to update mosquito-control programs that have focused on West Nile virus transmission.*

Zika Virus Vaccine Development

Vaccines for the Zika virus are under development and some are in clinical trials to test whether they are safe and effective. A licensed Zika vaccine will likely not be available for several years. As part of an overall strategy to support the response to Zika in 2016, the Biomedical Advanced Research and Development Authority (BARDA; which exists within the Office of the Assistant Secretary for Preparedness and Response [ASPR] in HHS), HHS's National Institute of Allergy and Infectious Diseases, and DoD's Walter Reed Army Institute of Research are supporting a diverse portfolio of Zika vaccine candidates, investing in multiple technological platforms to improve the chances of having a successful vaccine. As of December 2016, early phase clinical trials were underway to assess vaccine candidates for their safety, tolerability, and ability to provoke a beneficial immune response. Zika vaccine development represents a crucial step toward protecting infants from Zika virus disease and is one component of an overall Zika medical countermeasure response, which also includes the development of diagnostic tools and blood screening and pathogen reduction technologies.

State and territorial governments, along with non-Federal partners, also developed and implemented their own Zika-prevention programs, focusing on risk communication and outreach to communities. For example, Maryland's state government organized a "Zika Virus Awareness Week" in April 2016 to encourage residents to take actions to reduce their risk of infection. Similarly, the New York City Department of Health and Mental Hygiene sponsored a "Zika Day of Action" in June 2016, deploying outreach teams to subway stations to hand out educational materials on mosquito prevention and testing. In Puerto Rico, where the virus has infected more than 33,000 people (as of December 15, 2016) since the first

case was reported on the island in December 2015, the Puerto Rico Department of Health worked with CDC and private-sector partners to carry out public awareness and education campaigns. In June 2016, The Home Depot and the Puerto Rico Department of Health initiated the campaign by hosting more than 800 community members at an event that included a health fair and workshops on Zika prevention. In May 2016, the National Association of Chain Drug Stores Foundation launched a Zika-education initiative in Puerto Rico to encourage pregnant women to consult their pharmacists and doctors on protecting themselves and their unborn children from the Zika virus. The foundation also partnered with CDC to create outreach materials for store displays. HHS's Administration for Children and Families (ACF), with support from CDC, developed and distributed fact sheets in both Spanish and English on Zika for Head Start and child care providers, and parents. ACF programs also provided Puerto Rico with technical assistance on how it could use ACF program waivers and flexibilities to support Zika prevention efforts. Partnership programs across levels of government also provided support in communicating Zika protection measures. From January to October 2016, volunteer health professionals of the Medical Reserve Corps of Puerto Rico—a program supported by HHS's ASPR and administered by the Puerto Rico Department of Health—conducted educational workshops for community members on Zika. During this period, 144 volunteers educated more than 16,000 residents in Puerto Rico on the Zika virus and prevention measures.

Federal, state, local, tribal, and territorial partners have implemented mechanisms to control mosquito populations and distributed protective supplies to prevent the spread of the virus. ASPR led an interagency working group to identify and respond to potential supply shortages for mosquito control products in coordination with manufacturers and distributors. The CDC provided states and territories that have confirmed outbreaks of Zika with immediate services to control mosquito populations, as well as Zika Prevention Kits. In addition, the Strategic National Stockpile (SNS) supported the establishment and implementation of mosquito population-control contracts, which provide access to spraying and other mosquito-control support, for 10 state and local governments (as of December 12, 2016). Building on its experience from Ebola response efforts, CDC used partnerships with its nonprofit foundation and private companies to receive, assemble, and distribute more than 30,000 Zika Prevention Kits through the SNS. The CDC also collaborated with the National Association of Chain Drug Stores, which created Zika prevention messaging, set up store displays about Zika, and began distributing Zika prevention items (e.g. insect repellent) for purchase through local pharmacies and drug stores. However, these efforts may have begun too late in Puerto Rico; by July 7, 2016, the Zika virus was widespread in Puerto Rico, and Zika-infected patients resided in 99 percent of municipalities in the territory.

Protection Case Study: Texas A&M Develops App to Track Mosquito Populations

To facilitate mosquito control efforts, researchers at Texas A&M University developed a mobile application that tracks sites with standing water that might serve as places where the primary carrier and transmitter of the Zika virus, the *Aedes* mosquito species, lays eggs. *Aedes aegypti* and *Aedes albopictus* mosquitoes often lay eggs in containers of standing water, such as old tires, buckets, and bird baths. Through the app, users can document containers that could potentially be places for mosquito eggs and larvae, along with their locations. The app makes mapped data available to local health officials to use when prioritizing mosquito-control measures.

CBP Cargo and Port Security Programs

The Container Security Initiative **operates in**

58
Ports

and **pre-screens**

80%
inbound cargo prescreened

coming to the United States **from five continents**

Through the Container Security Initiative (CSI), CBP works collaboratively with foreign governments to prescreen cargo bound for the United States by ship. This initiative helps prevent terrorists from using cargo shipments to smuggle individuals or dangerous materials to the United States, securing the Nation's borders and addressing possible threats away from U.S. soil.

The Freight Security Initiative adds an additional layer of security at select ports by scanning 100 percent of all U.S. bound cargo containers for radiation.

In 2016, CBP added the Port of Aqaba, Jordan, to the list of ports conducting radiation scanning under the Freight Security Initiative.

Increasing Screening Efficiency

For shipments arriving at U.S. points of entry from abroad, CBP uses Radiation Portal Monitors to scan the cargo. This program provides another layer of defense against potential attempts to smuggle radioactive materials into the United States that could be used for weapons such as dirty bombs.

One major problem is **FALSE ALARMS**. From 2002 to May 2016, CBP scanned more than 1.2 billion conveyances for radiological contraband. This resulted in **millions of false alarms** that the agency had to investigate, **drawing resources away from other high priority law enforcement duties**. Efforts by CBP and DNDO to modify the setting these monitors operate at have resulted in major improvements, reducing false alarms by 78 percent at sea ports and 44 percent at land crossings.

Improvements have **reduced false alarms** by **200,000** each year

Mitigation

Mission Area Overview

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

Core Capabilities in Practice

The National Mitigation Framework ("Mitigation Framework") describes seven core capabilities, including how they interact to reduce loss of life and property and increase community resilience.

To effectively mitigate risks, a community begins with **Threats and Hazards Identification**, which includes understanding their frequency and magnitude. Next, **Risk and Disaster Resilience Assessments** help communities understand the consequences that these threats and hazards would have if they occurred. Based on this knowledge, community officials can begin **Planning** efforts to manage the risk, as well as provide **Public Information and Warnings** to residents. Once implemented, these plans enable **Long-term Vulnerability Reduction** to disasters through one or more of the following strategies:

- Risk avoidance – *Preventing exposure to an event (e.g., using zoning rules to prevent home construction in high-risk areas)*
- Risk reduction – *Minimizing vulnerabilities (e.g., retrofitting buildings to be more resistant to earthquakes)*
- Risk transfer – *Eliminating or limiting liability for harm, without reducing vulnerability (e.g., purchasing insurance)*

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 Hazards Identification

Since a community can rarely avoid risks completely, the Mitigation Framework encourages leadership, collaboration, partnership building, education, and skill building before an event through **Community Resilience**, with the goal of supporting other capabilities and building resilience. The Mitigation Framework also encourages communities to build and sustain capability in **Operational Coordination** in order to integrate critical stakeholders to support efforts during and after an incident.

The following are examples of actions taken in 2016 to improve preparedness that highlight the relationship among select core capabilities in the Mitigation Framework.

Community Resilience and Long-term Vulnerability Reduction

More than 1,100 community members from three towns in Massachusetts and two in New Hampshire started a project to restore native sand dunes. Sand dunes are a natural barrier to coastal winds, flooding, and erosion. Another benefit of this project, spearheaded by the University of New Hampshire, has been the establishment of a beachgrass community garden in Hampton, New Hampshire. The garden provides coastal homeowners in Hampton with free plants that they can transplant to their properties to protect against coastal storms.

Risk and Disaster Resilience Assessment and Community Resilience

The Rhode Island Division of Planning partnered with the Environmental Protection Agency (EPA) to create a framework to help communities assess their economic vulnerability to extreme weather events and improve their economic resilience. The framework is flexible and easy to use. Communities of varying size and resources can use

it to identify threats from extreme weather events and assess the economic impacts. The framework also helps the business community develop creative solutions to enhance their resilience. One community in Rhode Island, North Kingstown, has already pilot-tested and provided refinements to the framework.

- Planning and Long-term Vulnerability Reduction

  St. Tammany Parish, Louisiana, adopted an ordinance to address risks from storm surges. Floodwaters from heavy rains frequently trap residents and prevent emergency vehicle access. To address this vulnerability, parish officials approved an ordinance requiring roads constructed in new developments to be a minimum of six feet above sea level. Officials based the higher elevation on historical surge data and carefully weighed the benefits and costs to the environment and businesses. They determined that adopting the higher elevation requirement will reduce long-term maintenance costs in new coastal subdivisions and improve emergency response capabilities.

- Risk and Disaster Resilience Assessment and Threats and Hazards Identification

  NOAA, the U.S. Geological Survey (USGS), and other Federal partners supported a project in California's Sonoma and Mendocino Counties to develop a flood mapping and information tool, "Our Coast, Our Future." The tool enables local decision-makers to identify, understand, and visualize anticipated vulnerabilities resulting from sea level rise and coastal storms (such as increased flooding, shoreline erosion, and degraded salmon habitats). The interactive map feature allows users to view wave heights and flood potentials in their geographic area.

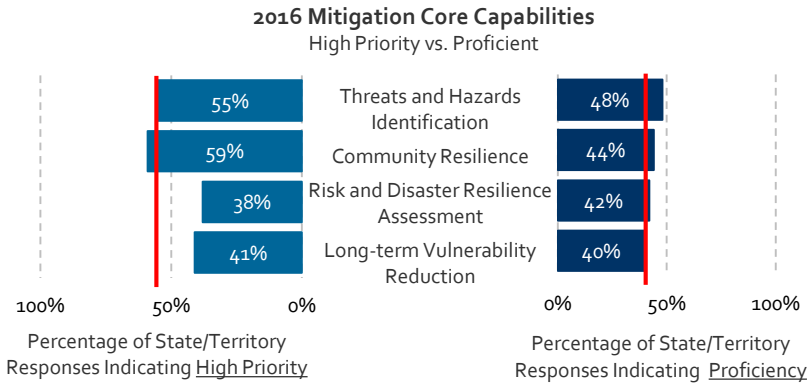
Summary of Progress

The Mitigation mission area continues to show progress in meeting the challenges posed by increasingly severe natural hazards. Scientific research and data collection, enhanced by advancements in technology, have improved the Nation's ability to understand natural hazards and to avoid, reduce, and transfer the risks they pose. In 2016, states and territories reported the second-highest overall proficiency ratings for capabilities in the Mitigation mission area, and since 2012, they have reported a greater increase in proficiency for Mitigation core capabilities than those in any other mission area. However, 2016 is the first year that states and territories reported lower State Preparedness Report proficiency ratings in Mitigation than the previous year.

The key findings in this section explain how the Nation is building upon its Mitigation capabilities to address specific hazards. The persistence of drought conditions in the West, the rise of human-induced earthquakes in the central United States, and the nationwide threat of flooding have tested the **Threats and Hazards Identification** and **Risk and Disaster Resilience Assessment** core capabilities. Innovations in both of these capabilities, such as development of water forecast tools and flood maps, have helped refine estimates of the risks these natural hazards pose, as well as enhance early warning systems and inform mitigation efforts. However, the number of states and territories that consider themselves proficient in **Threats and Hazards Identification** has decreased more than any other core capability since 2015. **Risk and Disaster Resilience Assessment** is the only Mitigation core capability in which states and territories reported increased proficiency ratings since 2015.

Of the Mitigation core capabilities, **Community Resilience** has shown the most improvement since 2012, with the number of states and territories rating themselves proficient increasing by eight percent. Tribal communities and localities have taken **Community Resilience** into their own hands by either initiating their own risk-reduction projects or, in the case of some tribal communities, avoiding risks altogether by physically relocating. In addition, 81 percent of states and territories consider addressing **Community Resilience** capability gaps their own responsibility rather than the Federal Government's. This is the fourth-highest percentage of any core capability.

The Federal Government's efforts to encourage the adoption of more resilient building codes and to improve the efficacy of the NFIP, in addition to the formation of public-private partnerships to supplement funding for wildfire mitigation projects, have all contributed to **Long-term Vulnerability Reduction**. Despite these efforts, **Long-term Vulnerability Reduction** is the only Mitigation core capability with a lower than average proficiency rating (see Figure 9).



Notes: Vertical red lines (|) indicate the average ratings for all core capabilities. The chart and statements do not include contributions from the three cross-cutting core capabilities—Planning, Operational Coordination, and Public Information and Warning

Figure 9. In their 2016 State Preparedness Report responses, states and territories provided information on their high priority core capabilities, as well as ratings on core capability proficiency.

Table 5 lists the most frequently identified "functional area" gap for each Mitigation core capability, as selected by states and territories in their 2016 State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from an analysis of the Goal, the Mitigation Framework, and other national-level preparedness doctrine.

Table 5. In their 2016 State Preparedness Report responses, states and territories identified remaining gaps in their ability to accomplish various functions associated with each Mitigation core capability.

Most Frequently Identified Functional Area Gap in Each Mitigation Capability	
Core Capability*	Gap
Community Resilience	Communication and outreach
Long-term Vulnerability Reduction	Incorporating mitigation measures into construction and development
Operational Coordination**	Command, control, and coordination
	Establishing a common operating picture
Planning	Whole community involvement and cooperation
Public Information and Warning	New communication tools and technologies
Risk and Disaster Resilience Assessment	Obtaining and sharing data
Threats and Hazards Identification	Stakeholder collaboration/coordination

* For core capabilities that cut across two or more mission areas, the 2016 State Preparedness Report did not include separate data requests that were specific to each mission area. Gaps identified for these core capabilities are identical for the different mission areas.
** The top-two functional area gaps for Operational Coordination were tied in terms of how frequently they were selected.

By the Numbers

A new study found that $4.80 in losses was avoided for every $1 spent on certain mitigation activities

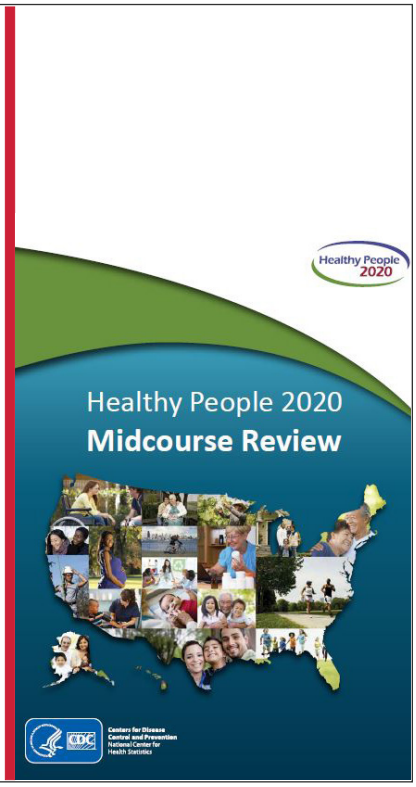
A 2016 study by the University of Pennsylvania Wharton School found that every $1 spent on new construction under the Florida Building Code over 10 years saved the state $4.80 in potential losses.

An ASPR and CDC working group issued 16 new preparedness objectives

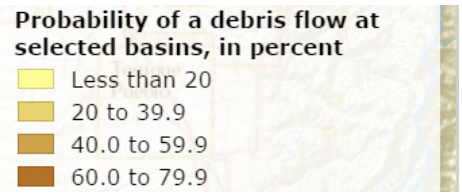
In May 2016, a working group by ASPR and CDC introduced 16 new preparedness objectives for Healthy People 2020. This initiative provides science-based, 10-year national objectives for improving the health of Americans by establishing benchmarks and monitoring progress. The new objectives use data from various sources, including CDC, FEMA, and Save the Children.

Community Development Block Grant Disaster Recovery assistance—totaling $2.3 billion—for 2016 disasters includes mitigation Requirements

In January 2017, the U.S. Department of Housing and Urban Development (HUD) published a Federal Register Notice including additional language requiring long-term recovery and hazard mitigation planning to promote sound and sustainable long-term recovery.



Mitigation Snapshots



San Francisco Sea Level Rise Action Plan

Sea level rise is one of San Francisco's most pressing environmental threats. To address it, a task force comprising local agencies developed a plan for San Francisco to mitigate the impacts. Published in March 2016, the plan outlines goals and objectives, such as conducting a vulnerability and risk assessment. San Francisco intends to build upon the plan and fully develop an adaptation plan for sea level rise by 2018.

USGS Interactive Map

In August 2016, USGS produced an interactive map that allows residents living in and around New Mexico's Jemez Mountains to see where they are located in relation to post-wildfire areas that may present debris-flow hazards (e.g., fast-moving landslides). The map also provides land managers and decision-makers with the ability to pinpoint locations where mitigation activities would minimize both the threat of wildfires and the potential for debris flows.

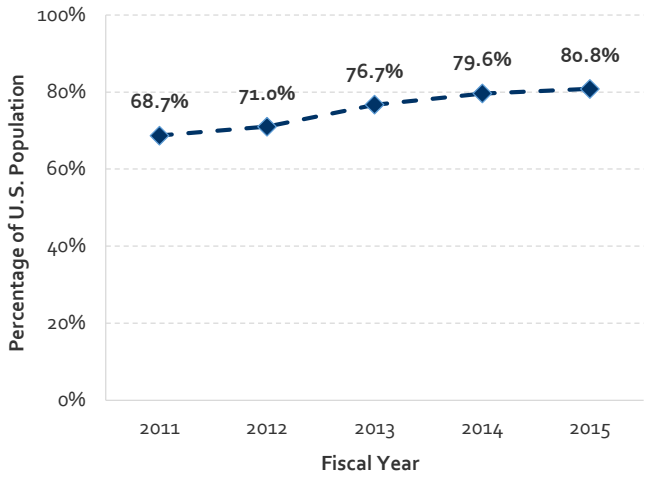
RainReady Midlothian

Midlothian, Illinois, has faced chronic flooding in recent years. In response, Midlothian and its partners developed a flood plan, RainReady Midlothian, that establishes a common understanding of the village's flood risk, describes methods of reducing flood impacts, and explains how to implement them. In addition, the plan emphasizes using green infrastructure not only to mitigate the negative impacts of floods, but also to preserve natural habitats, create jobs, and beautify neighborhoods.

Preparedness Indicators

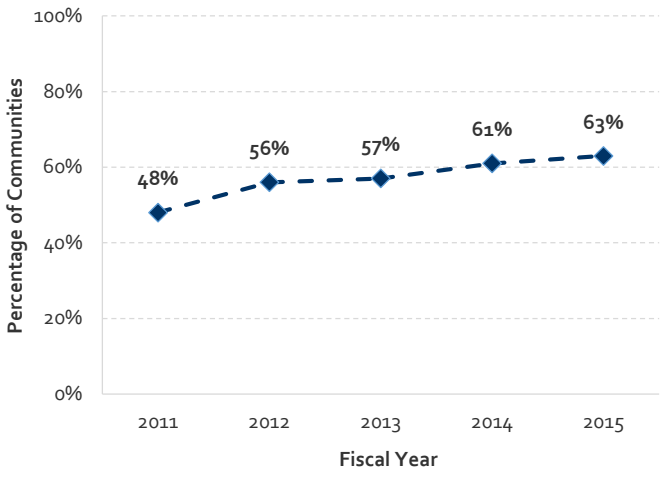
Percentage of U.S. population (excluding territories) covered by formal mitigation strategies

Hazard mitigation strategies guide jurisdictional risk reduction efforts. DHS measures the percentage of the Nation's population covered by formal mitigation strategies. Between fiscal years 2011 and 2015, this percentage has risen from 68.7 percent to 80.8 percent—an increase of more than 12 percentage points.



Percentage of communities adopting disaster-resistant building codes

FEMA encourages the adoption and enforcement of disaster-resistant building codes to help communities increase their structural resilience. Adoption rates have shown an upward trend over the past five years. From fiscal year 2011 to fiscal year 2015, the percentage of communities adopting building codes with provisions that adequately address earthquake, flood, and wind hazards rose from 48 percent to 63 percent.



Mitigation

Key Findings

Key Finding:

Recent innovations in early warning systems have the potential to improve the public- and private-sectors' ability to forecast and communicate threats and hazards.

Federal agencies and academic institutions made advancements in earthquake early warning systems in 2016. In February, USGS announced that its prototype earthquake early warning system, "ShakeAlert," entered the next phase of development, in which beta users can receive USGS ShakeAlert warnings on computers or smart devices. ShakeAlert has already detected thousands of earthquakes, including two that caused significant damage. Depending on the location of the earthquake's epicenter and the density of seismic instrumentation, this early warning system provides anywhere from a few seconds to minutes of advanced warning before shaking begins, allowing public safety and key facilities' personnel to take protective actions. In addition, the National Aeronautics and Space Administration (NASA) and Scripps Institute of Oceanography developed improved global positioning system (GPS) technology to estimate more accurate earthquake data, including location, magnitude, depth, and tsunami potential. By combining GPS data on the earth's permanent displacement with seismic data, researchers can determine the magnitude of an earthquake more accurately and predict the likelihood of an ensuing tsunami. NASA started working with NOAA's Tsunami Warning Centers to evaluate the new technology for potential additional application in NOAA's tsunami early warning system.

Mission Area Connections

Early Warning Systems

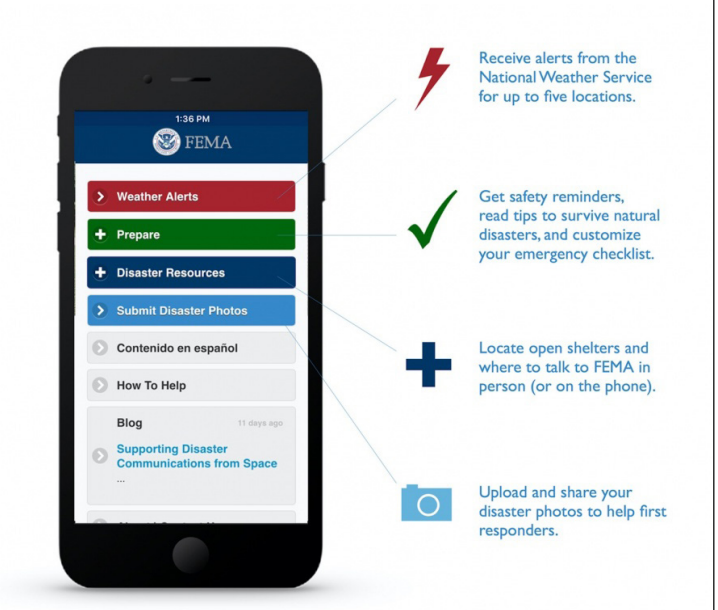
Becoming familiar with public information and warning systems is an essential activity in advancing mitigation. Receiving alerts ahead of an event enables people to take action to reduce the potential damage to themselves and their homes. Early warning systems also help first responders by giving them additional time to prepare and prioritize before an incident occurs.

The Federal Government has also made progress in developing new technologies for monitoring droughts and floods. In February 2016, NOAA's National Integrated Drought Information System launched new drought early warning systems in the Pacific Northwest and the Midwest. NOAA worked with state, local, and tribal partners in each region to develop these systems, which make climate projections and drought forecasting data readily available to local decision-makers. NOAA also released the Nation's first-ever national water forecast tool, which provides more accurate, detailed, and frequent information on water levels and the potential for areas to flood. The new tool models water movement in the Nation's rivers and streams, improving the ability to predict extreme flooding events. Whereas previous capabilities confined NOAA's water forecasting potential to 4,000 locations every few hours, this model extended that number by nearly seven-hundredfold. The tool provides hourly forecasts for the entire river network at 2.7 million locations. This can especially benefit emergency managers in flash-flood areas by giving them advance warning of at-risk areas to notify or evacuate.

Mitigation Case Study: FEMA App

In 2016, FEMA launched a new feature for the FEMA app that enables users to receive automatic notifications to their devices, reminding them to take steps to prepare their homes and families for disasters. The reminder feature allows users to receive pre-scheduled safety and preparedness tips, including updating emergency kits, testing smoking alarms, and practicing a fire escape plan. Additionally, the FEMA app—available in English and Spanish—provides emergency tips for what to do before, during, and after a disaster; interactive checklists for emergency kits; the ability to store emergency meeting locations; maps to nearby open shelters; and National Weather Service alerts for severe weather, flash flooding, and other hazards.

In October 2016 (the month when Hurricane Matthew made landfall in the United States), Apple users downloaded the FEMA App more than 85,000 times, quadrupling the previous record of 20,000 downloads the week after Hurricane Sandy in 2012. Since its creation in 2011, more than 800,000 downloads of the FEMA app on Android and Apple devices have occurred (as of December 2016). Users have credited FEMA app alerts with helping them avoid flash flooding, as well as actively monitor hazards.



Key Finding:

Federal departments, the private sector, and industry groups have launched new efforts to improve understanding of the value of stronger building codes and to increase their adoption.

Throughout 2016, Federal departments and agencies developed new tools and policies to increase the adoption of building codes that lessen the impacts of natural hazard events. The U.S. Army Corps of Engineers (USACE) created a website promoting community resilience through the use of the latest standards, building codes, and climate science. The website is a comprehensive resource for planners and designers to learn how to improve building integrity and resilience. In addition, FEMA issued a new policy in 2016 that requires the use of hazard-resistant building codes as the minimum design standard for building restoration projects under the Public Assistance Program. Requiring recipients of this funding to incorporate hazard-resistant design standards for their building projects will enhance infrastructure resilience in jurisdictions that lack effective building codes. In September 2016, FEMA also issued a new disaster risk reduction policy that requires all FEMA offices and programs to encourage their stakeholders to adopt and enforce hazard-resistant building codes, standards, and provisions.

Building industry stakeholders have also taken steps to encourage the adoption of stronger building codes. For example, as part of its Urban Resilience Program, the Urban Land Institute created Returns on Resilience, an online resource that helps communities build more disaster-resistant homes and buildings. Additionally, the Insurance Institute for Business and Home Safety (IBHS) released a mobile application ("FORTIFIED Home On The Go") to educate homeowners about how to build safer, stronger structures in the face of severe weather events. IBHS also launched incident-specific nationwide programs to help owners implement home improvement projects that increase the resilience of their houses against wind storms and hail storms.

Mitigation Case Study: Tsunami Safe Haven

After a tsunami devastated Japan's northeast coast in 2011, the Ocosta School District Board of Directors in Westport, Washington, decided to improve their community's tsunami preparedness. In May 2016, the Ocosta School District—with support from Washington State's Project Safe Haven initiative, private-sector partners, and community members—completed construction of a new elementary school that includes a vertical-evacuation safe haven above the gymnasium. This is the first tsunami safe haven of its kind in North America, capable of holding approximately 2,000 people. Since its completion, the school has conducted several tsunami evacuation drills with its students. In addition, as part of a state exercise on June 11, the Washington National Guard demonstrated how they could use helicopters to rescue people from the safe haven.

Key Finding:

FEMA is improving the oversight, accountability, and sustainability of the NFIP to better help insurance policyholders reduce future risk.

In the wake of Hurricane Sandy, residents of affected states expressed concerns that the private insurance companies that implement the NFIP underpaid their claims. In response, FEMA requested that the DHS Office of the Inspector General audit the NFIP's Write Your Own (WYO) program—the cooperative arrangement that allows private insurance companies to write and service NFIP policies under their own names. The DHS Office of the Inspector General published a report in March 2016 concluding that FEMA had not sufficiently monitored the reimbursement or appeals process. Therefore, FEMA could not ensure that WYO companies were properly implementing the NFIP. To address these challenges, FEMA announced several improvements to the program in 2016, including:

- *Removing the NFIP's Financial Assistance/Subsidy Arrangement with WYO companies to provide greater flexibility and governance in the future;*
- *Providing customers in the appeals process with a contact at FEMA (previously, customers could only communicate with their private insurance company); and*
- *Establishing a team within the FEMA Office of Chief Counsel to monitor all lawsuits and oversee all legal bill payments.*

FEMA is also taking new steps to strengthen the NFIP's financial framework. Payouts to claims from major flooding events—including those resulting from Hurricanes Katrina, Ike, and Sandy—have left the NFIP $23 billion in debt (as of December 31, 2016), requiring the program to pay nearly $400 million per year in interest payments to the U.S. Department of the Treasury on the borrowed funds. FEMA is attempting to defray the cost of claims from large and unexpected events and expand its ability to cover these claims by purchasing reinsurance—a form of insurance for insurance providers—from a number of private companies.

In addition, maintaining a balance between the solvency of the NFIP and the affordability of its policies has been an ongoing challenge. Although most NFIP insurance policies have insurance rates that reflect the true flood risk, Congress instituted premium discounts for certain classes of policies. Recent reform legislation directed the NFIP to phase out some of these discounts to increase revenue and improve the program's fiscal stability. However, FEMA still hears concerns about the perceived high cost of flood insurance and about the accuracy of flood maps and insurance rates. As directed by Congress in recent legislation, FEMA is studying flood insurance affordability and providing recommendations for an affordability framework to Congress by September 2017.

Despite these challenges, the NFIP successfully executed the flood insurance components of FEMA's mission to support several flooding incidents in 2016. In addition to providing WYO companies further guidance through bulletins, FEMA website updates, and public fact sheets associated with each event, NFIP also issued advanced payments to provide expedited relief to survivors, coordinated with State Insurance Commissioners and WYO companies to ensure policyholder needs were being met, deployed staff to support field operations, and provided analytical support to stakeholders making resource decisions. In addition, the NFIP closed over three-quarters of claims resulting from three significant flood events—Hurricane Matthew, Hurricane Hermine, and the August Louisiana floods—within a few months. This demonstrates the progress that NFIP has made in more efficiently helping policyholders impacted by recent events recover.

Key Finding:

Federal and state actors are taking steps to address human-induced earthquakes, which are contributing to an overall increase in seismic hazards in the central United States and present threats to infrastructure and people.

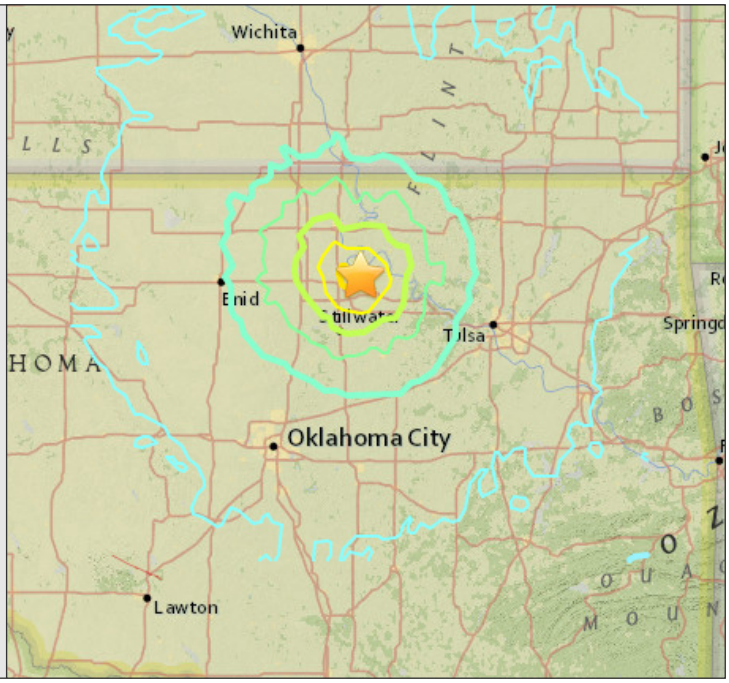
Human-induced earthquakes, such as those caused by reinjecting wastewater into the ground during oil and natural gas extraction, are partially responsible for an increase in earthquakes in the central United States. Between 1973 and 2008, the average number of earthquakes of magnitude 3 or higher each year for this region was 24. In 2015, the number of earthquakes peaked at 1,010. While these induced earthquakes have been of smaller magnitude, they can still create seismic hazards to important structures. Oklahoma, for example, experienced a 5.8 earthquake in 2016, which was the largest earthquake in its history. The structural damage from the 5.8 magnitude earthquake was substantial enough for the state's governor to declare a state of emergency for Pawnee County and for the Oklahoma Corporation Commission, which regulates and supervises activities associated with the production of oil and gas, to shut down all reinjection wells within 725 square miles of the earthquake's epicenter. Earthquakes present a particularly serious threat to oil and natural gas infrastructure in Oklahoma, which contains about five percent of the Nation's pipeline mileage (the third-highest percentage of any individual state).

In 2016, USGS published its first hazard maps to include both natural and human-induced seismic risks. Also for the first time, the maps address earthquake hazards on a one-year timeline—which is unique to induced earthquakes, where changes in policy or industry activity can directly affect their frequency. The new forecasts enable emergency response personnel to better assess risks to people and infrastructure and to issue safety information, if necessary. The maps highlight risks from induced earthquakes for approximately seven million people in areas of the central and eastern United States. Oklahoma and Texas have the largest populations exposed to induced earthquakes.

Kansas has also responded to the threat of human-induced earthquakes. In March 2015, the state commission responsible for regulating oil and gas production issued an order that required oil and gas companies to reduce their saltwater injection rates in counties that had experienced recent increases in seismic activity. During a 180-day period before the commission's order, two counties experienced 107 earthquakes of magnitude 2.5 or greater. This decreased to 65 in the 180 days after the order. Whether the order resulted in the reduced seismic activity remains inconclusive, but in August 2016, the commission issued another order to reduce saltwater injection rates to an expanded geographical area.

Mitigation Case Study: Reducing the Likelihood of Human-Induced Earthquakes in Oklahoma

Oklahoma has taken steps to reduce the consequences of human-induced earthquakes. In January 2016, the Governor allocated $1.4 million in state emergency funds to earthquake research and regulation activities by the Oklahoma Geological Survey and the Oklahoma Corporation Commission. The Oklahoma Geological Survey plans to use this funding to improve its ability to collect and analyze earthquake data, while the Oklahoma Corporation Commission used it to direct wells operating in the northwest portion of the state to reduce wastewater reinjection by approximately 40 percent. However, the commission's authority to mandate compliance is unclear, and the state has explored non-regulatory options to mitigate this hazard.



Key Finding:

Coastal communities, including tribal communities, are exploring relocation options to address the growing risks posed by extreme weather events, including sea level rise and coastal erosion.

Increasing sea levels can cause storm surge to push farther inland, leading to more frequent and widespread flooding of coastal areas. Destructive flooding has increased by as much as 900 percent over the past five decades, and a recent study found that 4.2 million people in the continental United States will be at risk of inundation by the year 2100.

For the first time, in 2016 the Federal Government allocated funds to the State of Louisiana to move the entire Isle de Jean community in response to these threats. Louisiana is relocating the entire Isle de Jean Charles community, which is also home to the Band of Biloxi-Chitimacha-Choctaw Indians, to higher ground using a $48 million grant from the National Disaster Resilience Competition. The island has lost 98 percent of its landmass to coastal erosion and sea level rise in the past 60 years. In 1955, the island was five miles wide; in 2016, it was a quarter-of-a-mile wide. The Quinault Indian Nation in Washington State is also developing a master plan to move their main village to higher ground. Taholah, one of the tribal nation's two main population centers, is particularly vulnerable to flooding, coastal erosion, and increasing storm events, since it is located at the confluence of the Pacific Ocean and the Quinault River. In addition, tribal villages in coastal regions of Alaska have begun exploring the option of relocating their communities. The Alaska Division of Community and Regional Affairs established multi-agency planning groups (i.e., Village Planning Groups) with the tribal villages of Shishmaref and Kivalina. Both tribal villages are suffering from land loss due to erosion and increasingly severe coastal flooding.

In 2016, the Community Resilience Working Group, co-chaired by HUD and the U.S. Department of the Interior (DOI), enhanced Federal collaboration to assist these villages. GAO reports have identified 31 villages at risk from coastal erosion and flooding, including those mentioned above.

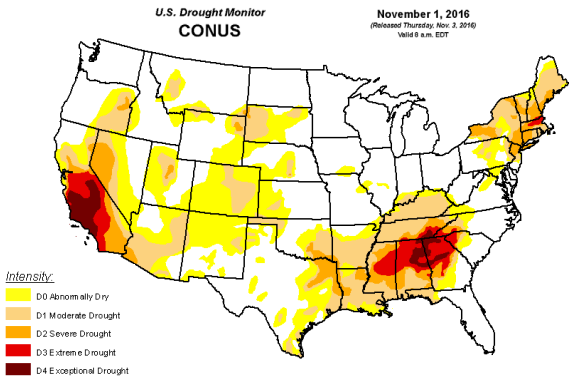
Key Finding:

As studies predict that drought conditions will persist and intensify, new efforts to fully understand and reduce the long-term consequences of drought have emerged.

Recent research predicts that rising average temperatures will amplify and prolong drought conditions in the future. A March

2016 report from the DOI's Bureau of Reclamation (USBR) estimates that by the end of the 21st century, the United States will experience a temperature increase of five to seven degrees Fahrenheit. Increasing temperatures diminish snowpack, reduce stream flows, and limit the availability of water, further intensifying drought conditions. In addition, the report found that the April to July stream flows of several major river basins in the West will decrease between seven and 27 percent.

The Federal Government has taken the lead on addressing the threat that drought poses to the Nation. In March 2016, *Presidential Memorandum: Building National Capabilities for Long-Term Drought Resilience* formally institutionalized the National Drought Resilience Partnership (NDRP), a Federal partnership of seven departments and agencies tasked with helping communities better prepare for future droughts and reduce the impact of drought events. An accompanying Federal Action Plan identifies specific goals and associated actions for the NDRP to improve resilience to drought. In response, the NDRP completed efforts and launched new ones in 2016 to understand the long-term impacts of drought:



- *NDRP partners are working with The Ohio State University and other private and public partners to develop a national soil moisture monitoring network, which will facilitate more comprehensive and accurate drought impact assessments.*
- *A U.S. Department of Agriculture (USDA) Forest Service (USFS) study on the consequences of drought for forests found that more frequent droughts could lead to larger wildfires, a higher probability of large-scale insect outbreaks, and reduced forest growth. The report also includes data that land managers can use for measuring the effectiveness of and building upon their drought resilience and climate adaptation efforts.*
- *To help states understand the economic impacts of drought, DHS is developing three reports that explain drought's effects on infrastructure operations that are critical to state economies. Two of the reports will identify how California's drought affected data center and manufacturing operations. The third report will focus on how drought has affected thermoelectric power plant operations in California and Texas. DHS plans to develop the reports' findings into decision-support guides for stakeholders making decisions on how to accommodate competing water needs during droughts.*
- *USGS, the Nature Conservancy, and the Wildlife Conservation Society formed the Ecological Drought Working Group to assess the ecological impacts of drought and its implications for human well-being, in order to help communities prepare for and adapt to the effects of drought.*

NDRP members also reported recent activities that aim to strengthen drought resilience over the coming years:

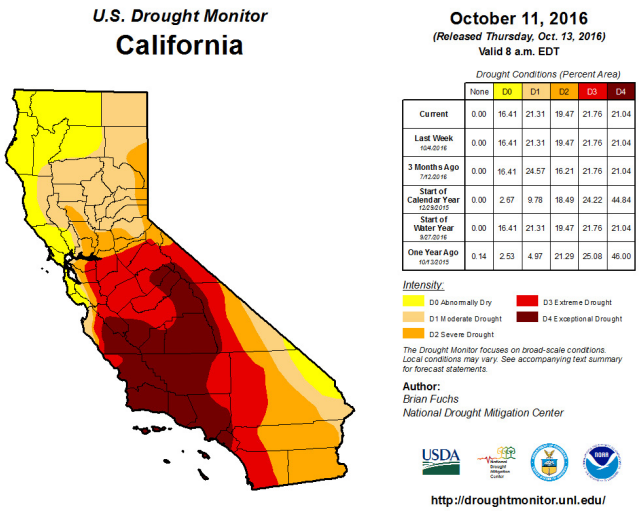
- *The USDA and USBR are investing $47 million to support local water management projects and agricultural water-use efficiency across 11 states in the West.*
- *USDA's Natural Resources Conservation Service (NRCS) allocated $1.1 million towards local drought mitigation projects in the Missouri Headwaters Basin in Montana.*
- *The USBR began five pilot studies exploring how reservoir operations can adapt to the impacts of climate change. The pilots, which will end in December 2017, study water sources in the Great Plains, the Mid-Pacific, the Pacific Northwest, and the Upper and Lower Colorado regions. Based on these pilots, USBR is developing guidance to identify and implement improvements to reservoir operations by considering improved scientific information, enhancing existing operational flexibility, and planning for changes to reservoir operations under drought conditions.*
- *The EPA and Montana's Department of Natural Resources, in partnership with other Federal and state agencies and nongovernmental organizations, launched a three-year demonstration project to enhance long-term drought resiliency in the Missouri headwaters basin by providing tools for drought monitoring, assessing, and forecasting; developing local and regional capacity to plan for drought; and implementing local projects to build regional drought resilience. The results will enhance local drought resilience and demonstrate how communities across the country can also mitigate drought.*

Key Finding:

As the costs of wildfire suppression rise, public and private initiatives to fund wildfire risk reduction projects are emerging.

Mitigation Case Study: The California Drought

Entering its sixth consecutive year of drought, California has been in a state of emergency since January 2014. As of October 11, 2016, 84 percent of the state is experiencing drought, and the remaining 16 percent is abnormally dry. However, California's water conservation efforts, such as refraining from hosing off sidewalks and reducing runoff while watering lawns, have shown promising results. Between June 2015 and March 2016, California communities reduced water use by nearly 24 percent, which could provide 6.5 million Californians with enough water to last a year. In May 2016, Governor Brown issued an executive order directing state agencies and the public to use water more wisely, eliminate water waste, strengthen local drought resilience, increase the efficiency of agricultural water use, and improve drought planning. Through these requirements, the order aims to transition drought mitigation in California from temporary to permanent activities.



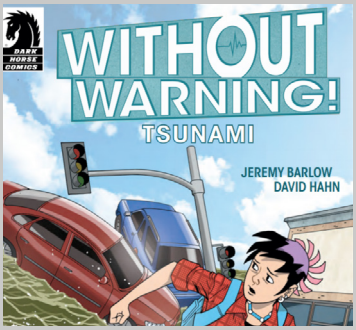
Wildfire suppression costs have risen rapidly over the past few decades, mainly due to longer and more severe fire seasons. According to USFS, fire seasons are now, on average, approximately 78 days longer than in 1970, and USFS expects this trend of longer fire seasons and increasing fire suppression costs to continue over the next decade. Between fiscal years 2014 and 2015, the USFS suppression budget grew by $115 million and the budget for non-fire programs that reduce the risk of future wildfires—such as forest restoration projects—fell by the same amount.

Forest restoration projects can play an important role in helping to minimize the risk of wildfires by thinning forests and reducing vegetation that fuels them. Private and nonprofit organizations have helped bolster Federal initiatives for wildfire risk reduction projects in 2016. For example:

- *In June 2016, USFS and NRCS announced a partnership with the American Forest Foundation to address wildfire risk across 3.5 million acres of land in the western United States and provided a combined initial investment of $5 million to fund forest restoration projects and public engagement. A portion of the funds will enable the American Forest Foundation to conduct outreach and education to 17,500 landowners in important watersheds. The remainder of the funds will provide cost-share dollars directly to landowners in one of the project landscapes. The partnership's goal in the first two years is to restore more than 11,000 acres of land.*
- *As in 2015, DOI committed $10 million in 2016 to 10 Wildland Fire Resilient Landscapes (WFRL) "Collaboratives," to improve the integrity and wildfire resilience of forests and rangelands nationwide. WFRL Collaboratives consist of partnerships among Federal, tribal, state, and local governments, private landowners, and nonprofit organizations. Employing integrated land management techniques and pooling their resources, WFRL Collaboratives restore native vegetation and modify or remove vegetative fuels to support fire resilience and landscape management objectives. During 2015 and 2016, the WFRL Collaboratives accomplished 930,000 acres of landscape-level treatments.*
- *Blue Forest Conservation—a team of financial and engineering professionals—is working with USFS, other USDA agencies, and nonprofit partners to develop and pilot the Forest Resilience Bond in California. This new investment platform will deploy private capital to accelerate forest restoration projects in watersheds. The bond enables the beneficiaries of these projects (e.g., water utilities) to repay investors over a 10-year period to help defray the financial burden.*

2016 Preparedness Campaigns

FEMA estimates that as of 2016, **less than a quarter of Americans have attended preparedness meetings or trainings**. Eighteen percent of respondents to the 2015 National Household Survey reported attending a meeting on how to become better prepared for a disaster within the last year. This is a decrease of five percentage points from 2012. To improve this trend, both public and private stakeholders used **more accessible media to promote individual and household preparedness** in 2016.



The Oregon Office of Emergency Management worked with a graphic novel publishing company to produce **a comic book touting tsunami preparedness** targeted towards younger audiences.

As part of National Preparedness Month, **the popular video recipe website Tastemade** partnered with FEMA to develop preparedness products designed to leverage the popularity of the online recipe video trend.

20th Century Fox and Blue Sky Studios partnered with Save the Children to launch a new emergency preparedness public service announcement (PSA) campaign featuring characters from the feature film **"Ice Age: Collision Course."**

FEMA's Ready Campaign and the Ad Council demonstrated how **"Being Ready Can Be Scary Simple"** in a series of videos that encourage families to prepare for emergencies by discussing emergency contacts and packing go bags.

The USFS, the Ad Council, and the National Association of State Foresters launched **a new Smokey Bear PSA campaign** to promote awareness about how to avoid accidentally starting a wildfire.

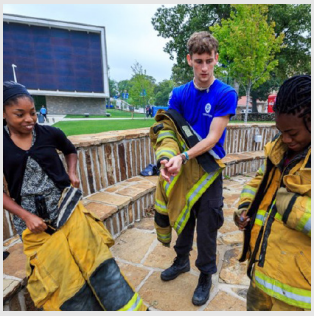
For the first time, the Ready Campaign released their "Don't Wait. Communicate. Make Your Emergency Plan Now" national **PSA in Mandarin Chinese**—the third most-spoken language in the United States.

Mitigation Case Study: Youth Preparedness

Promoting emergency preparedness at an early age contributes to overall individual preparedness. Examples of age-appropriate programs that engage youth to be better prepared for disasters include:

- ***The Pillowcase Project:*** *In 2013, the American Red Cross partnered with the Walt Disney Company to launch the Pillowcase Project, a nationwide program that teaches elementary school students how to prepare for and stay safe during disasters. As of September 2016, this program has reached more than 500,000 students, teaching 3rd–5th graders how to create their own emergency supply kit by packing essential items in a pillowcase for easy transport during an emergency. Since its inception, the program has helped save at least six lives from house fires. By sharing the information with their families and following what they had learned through the Pillowcase Project, students were able to help save their loved ones and themselves.*

- ***FEMA Youth Preparedness Council:*** *As children grow older, they have opportunities to improve the resilience of not just their families, but also their communities. The FEMA Youth Preparedness Council consists of high school students who serve as national advocates of youth preparedness. In 2016, a FEMA Region IX council member organized the 2016 Service Learning, Youth and Community Preparedness Summit as part of her ongoing efforts to strengthen community resilience in Guam. During the summit, local students developed emergency plans for a variety of hazards, including earthquakes, typhoons, and tsunamis.*



- ***ReadyCampus:*** *For college students, experiencing disasters while in school can cause difficulties as they are no longer under the protection of their parents or guardians. To address this vulnerability, FEMA Region VII released an updated version of its* ReadyCampus Development Guide *in 2016 for institutions of higher education. ReadyCampus is a student-focused program that helps these institutions develop and implement their own actionable, adaptable, and scalable preparedness programs. As of fall 2016, 11 institutes of higher education within Region VII are using the development guide and promoting positive interactions between students, campus and local emergency management, and public safety officials. These activities not only enhance understanding of campus emergency procedures and available resources, but also increase awareness about emergency management as a career path for college students.*

Response

Mission Area Overview

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

Core Capabilities in Practice

The Response mission is to save lives, protect property and the environment, and meet basic human needs after an incident. The National Response Framework describes 15 core capabilities, including how they guide the Nation's response to disasters and emergencies.

To effectively respond to an incident, emergency management officials and responders implement tasks, as identified through **Planning** efforts. They use **Operational Coordination** to ensure that tasks are carried out in an organized fashion. Through **Public Information and Warning**, officials deliver clear, actionable, and accessible information about relevant threats and hazards to the community. **Operational Communications** enable emergency managers and responders to exchange critical information promptly and efficiently. Throughout the response, decision-makers use **Situational Assessment** to understand the extent and nature of the hazard, which supports informed decisions.

For those survivors who may be immobilized or trapped, trained personnel conduct **Mass Search and Rescue Operations** to locate and rescue these individuals. For incidents involving fires, **Fire Management and Suppression** efforts may also be necessary to save and protect lives, as well as property and the environment. When a large number of fatalities occur, **Fatality Management Services** recover the deceased and share information to help reunify families.

During the response, **Environmental Response/Health and Safety** operations and **On-scene Security, Protection, and Law Enforcement** protect both response workers and the public. Public, private, and community-based organizations provide **Public Health, Healthcare, and Emergency Medical Services** and **Mass Care Services** to address the needs of survivors, including those with access and functional needs, such as children, individuals with disabilities, older adults, and persons with limited English proficiency. Moreover, officials use **Critical Transportation** and **Logistics and Supply Chain Management** to ensure that affected communities receive essential commodities and services. This aids owners and operators of **Infrastructure Systems** in restoring and revitalizing systems and services for the community.

Core Capabilities in the Response Mission Area

- Critical Transportation
- Environmental Response/Health and Safety
- Fatality Management Services
- Fire Management and Suppression
- Infrastructure Systems
- Logistics and Supply Chain Management
- Mass Care Services
- Mass Search and Rescue Operations
- On-scene Security, Protection, and Law Enforcement
- Operational Communications
- Operational Coordination
- Planning
- Public Health, Healthcare, and Emergency Medical Services
- Public Information and Warning
- Situational Assessment

The following are examples of actions taken in 2016 to improve preparedness that highlight the relationships among a select number of the 15 core capabilities in the National Response Framework:

Operational Communications and Public Information and Warning

The Integrated Public Alert and Warning System (IPAWS) enables public safety officials to issue alerts and quickly provide the public with life-saving information. From a single interface, officials can access various public alerting systems, such as the Emergency Alert System, Wireless Emergency Alerts, and NOAA's All Hazards Weather Radio. As of December 2016, all 50 states have adopted IPAWS; in total, 851 public safety organizations—including two territories, the District of Columbia, two tribes, and two Federal agencies—have received access.

Additionally, FEMA and the Federal Communications Commission (FCC) conducted the second nationwide test of the Emergency Alert System in September 2016. The test demonstrated the readiness of radio and television broadcast stations, cable operators, and other Emergency Alert System participants to receive and broadcast a national-level emergency message to the public. In the 2016 test, 95 percent of all participating broadcasters, cable operators, and other Emergency Alert System particpants received the national test message, representing a significant improvement over the first national test in 2011 (at 82 percent). Moreover, the 2016 test message was the first time that a national test message was presented in multiple languages, including both English and Spanish.

Planning and Public Health, Healthcare, and Emergency Medical Services

On September 8, 2016, HHS's Centers for Medicare & Medicaid Services finalized a rule requiring healthcare providers and suppliers participating in Medicare and Medicaid to meet four emergency preparedness best practice standards. Affecting more than 72,000 healthcare providers and suppliers, the rule requires them to develop emergency plans and coordinate with Federal, regional, state, local, tribal, and territorial stakeholders. These more comprehensive requirements help ensure that facilities are sufficiently prepared to provide and coordinate patient care during disasters and emergency situations. Providers and suppliers affected by this rule must comply by November 16, 2017.

In addition, CDC has released multiple guidance documents, for Zika and for many other infectious threats. For example, CDC recently released a review of biologic threat preparedness for pregnant women. To help deal with the challenge of Zika, CDC developed nine clinical guidance documents for healthcare providers caring for patients with Zika. CDC and the Centers for Medicare & Medicaid Services also collaborated on Zika healthcare funding and performance metrics.

Environmental Response/Health and Safety and Planning

Few, if any, states have established pre-incident waste management plans (PI-WMPs) to address the potential waste generated from wide-area urban incidents involving chemical, biological, or radiological threat agents. Responding to such incidents without a PI-WMP can increase the overall cost and timeline of response and recovery efforts.

- *EPA—in collaboration with states and local agencies and first responders—is developing a PI-WMP tool, an initial version of which is ready for testing. The tool, which incorporates the latest EPA knowledge and research, assists emergency management planners and others in building their own PI-WMP.*
- *EPA collaborated with New York City's Department of Mental Health and Hygiene and New York state agencies to develop guidance that provides tactical solutions and strategies for responding to a wide-area biological incident taking place in New York City.*
- *EPA worked with Virginia's Departments of Emergency Management and Environmental Quality to develop the first-ever PI-WMP for a subway system, which was used to address waste generated during a field test that evaluated the response to a biological incident.*

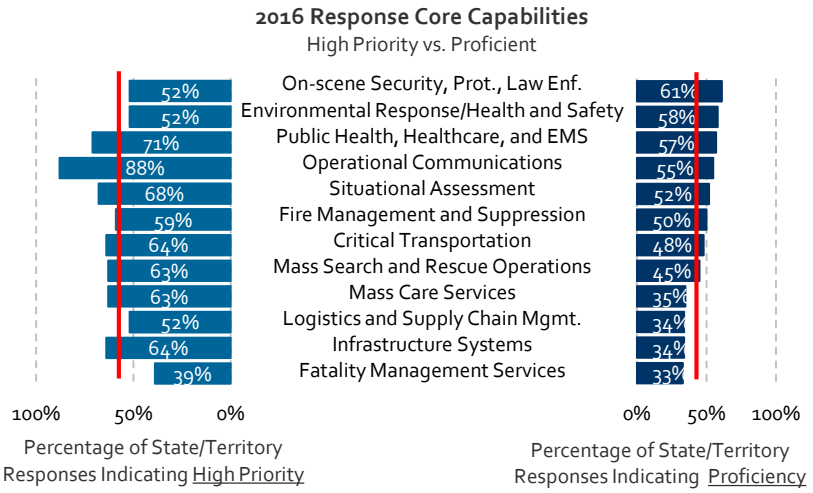
Summary of Progress

The Response mission area continues to be an area of relative strength nationwide. Real-world incidents in 2016 provide validation of capability progress, as captured in several of this section's key findings. In addition, states and territories reported higher-than-average proficiency for eight Response core capabilities, making Response the mission area with the highest levels of proficiency for the fifth consecutive year.[7]

Response efforts during the August Louisiana flooding, the Zika virus outbreak, and Hurricane Matthew highlighted specific strengths in **Mass Search and Rescue**; **Operational Coordination**; and **Public Health, Healthcare, and Emergency Medical Services**, while revealing challenges in delivering **Mass Care Services**. Training and exercises occurring across the

[7] Unless otherwise noted, figures and statements do not include contributions from the three core capabilities common to all mission areas—i.e., Planning, Operational Coordination, and Public Information and Warning.

Nation further demonstrate the extensive preparedness activities underway in this mission area. For example, 84 of the 98 exercises conducted under FEMA's NEP in 2016 addressed one or more Response core capabilities (50 more exercises than the next highest mission area). Five of the 10 capabilities most frequently selected as a high priority were in the Response mission area. Even so, **Fatality Management Services**, **Infrastructure Systems**, **Logistics and Supply Chain Management**, and **Mass Care Services** exhibited below-average levels of proficiency in 2016 State Preparedness Report responses (see Figure 10). Though states and territories reported a five percent increase in **Fatality Management Services** from 2015 (the largest increase of all core capabilities), **Infrastructure Systems**, **Logistics and Supply Chain Management**, and **Mass Care Services** all declined in proficiency from last year.



Notes: Vertical red lines (|) indicate the average ratings for all core capabilities. The chart and statements do not include contributions from the three cross-cutting core capabilities—Planning, Operational Coordination, and Public Information and Warning

Figure 10. In their 2016 State Preparedness Report responses, states and territories provided information on their high priority core capabilities, as well as ratings on core capability proficiency.

Table 6 lists the most frequently identified "functional area" gap for each Response core capability, as selected by states and territories in their 2016 State Preparedness Report submissions. Functional areas break down core capabilities into more granular-level functions, which were identified from an analysis of the Goal, the National Response Framework, and other national-level preparedness doctrine.

Table 6. In their 2016 State Preparedness Report responses, states and territories identified remaining gaps in their ability to accomplish various functions associated with each Response core capability.

Most Frequently Identified Functional Area Gap in Each Response Capability	
Core Capability*	Gap
Critical Transportation	Evacuation
Environmental Response/Health and Safety	Health and safety monitoring and assessment
Fatality Management Services	Mortuary services
Fire Management and Suppression	Specialized firefighting
Infrastructure Systems	Infrastructure site assessments
Logistics and Supply Chain Management**	Donations management
	Resource delivery

Most Frequently Identified Functional Area Gap in Each Response Capability	
Core Capability*	Gap
Mass Care Services	Sheltering
Mass Search and Rescue Operations	Specialized operations
On-scene Security, Protection, and Law Enforcement	Securing disaster areas
Operational Communications	Interoperable communications between first responders
Operational Coordination**	Command, control, and coordination
	Establishing a common operating picture
Planning	Whole community involvement and cooperation
Public Health, Healthcare, and Emergency Medical Services	Medical surge
Public Information and Warning	New communication tools and technologies
Situational Assessment	Analyzing information

*For core capabilities that cut across two or more mission areas, the 2016 State Preparedness Report did not include separate data requests that were specific to each mission area. Gaps identified for these core capabilities are identical for the different mission areas.
**The top-two functional area gaps were tied in terms of how frequently they were selected.

The 2017 *National Preparedness Report* identifies **Infrastructure Systems** as a national area for improvement (see page 12). Additionally, three core capabilities specific to Response—**Environmental Response/Health and Safety**, **Operational Communications**, and **Situational Assessment**—are capabilities to sustain in this year's report (see page 11).

By the Numbers

The FEMA Office of Disability Integration and Coordination trained 650 individuals

In 2016, FEMA's Office of Disability Integration and Coordination delivered its two-day course, "Integrating Access and Functional Needs into Emergency Planning," 25 times to a total of approximately 650 individuals, which included emergency planners and managers, as well as disability support, service, and advocacy personnel. The course informs participants on how to use disability-inclusive practices throughout emergency response and recovery.

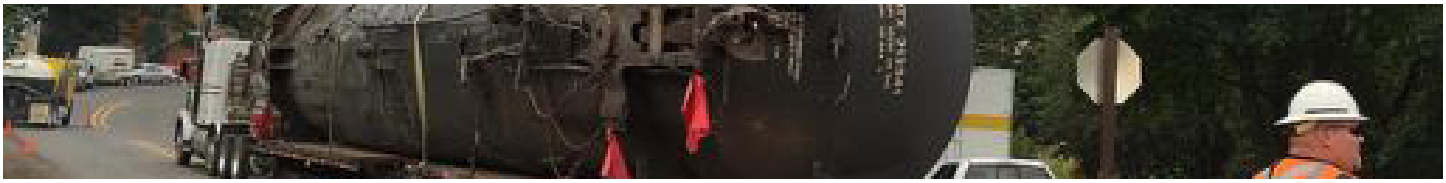
ASPR identified four capabilities and 17 associated objectives for the healthcare delivery system

In November 2016, ASPR released *2017–2022 Health Care Preparedness and Response Capabilities*, which identifies four capabilities and 17 associated high-level objectives that the Nation's healthcare delivery system should undertake to prepare for, respond to, and recover from emergencies. Recipients of Hospital Preparedness Program (HPP) funding will implement these capabilities starting with the July 2017 HPP project period.

The U.S. Fire Administration delivered 3,466 courses

In fiscal year 2016, the U.S. Fire Administration's National Fire Academy delivered 3,466 courses and trained 99,636 students in preparedness subjects, including Incident Management, Hazardous Materials Response, and Mass Casualty Incident Management.

Response Snapshots



Emergency Preparedness in Chicago Child Care Centers

In 2016, the City of Chicago, FEMA, HHS, and the American Red Cross of Greater Chicago held a four-part workshop series on emergency preparedness for child care center directors and employees. More than 40 child care directors from Chicago attended the workshops to review ways of better preparing their facilities for emergencies, plan escape routes, and draft action plans to use community resources during an emergency.

Columbia River Gorge Inland Spill Exercise Series

This exercise series consisted of national, regional, and principal-level, discussion-based exercises that addressed a fictional crude oil spill in the Columbia River. An incident similar to the exercise scenario later occurred on June 3 in Mosier, Oregon, in which 16 railcars carrying crude oil derailed along the Columbia River. Participation in the exercise series resulted in enhanced response coordination among state, local, and tribal organizations, as well as the railroad industry, during the actual spill.

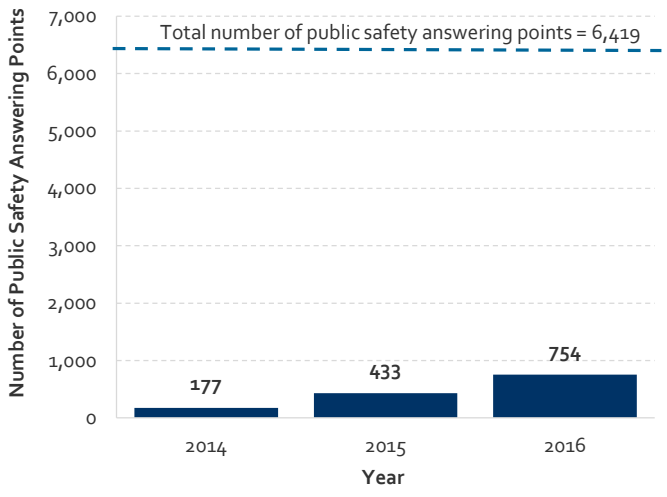
Wireless Network Resiliency Cooperative Framework

In April 2016, five wireless service providers and the Cellular Telecommunications Industry Association announced the Wireless Network Resiliency Cooperative Framework, a voluntary initiative that enhances industry collaboration through various actions (e.g., encouraging mutual aid between service providers, coordinating service restoration). After working with wireless service providers to test the framework during the August Louisiana floods and Hurricane Matthew, where it contributed to rapid restoration of wireless communications, FCC adopted the framework in December 2016.

Preparedness Indicators

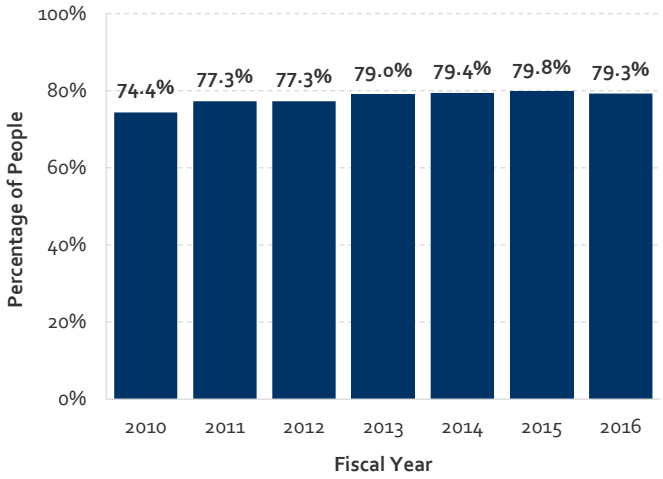
Cumulative number of PSAPs ready to receive text-to-911 messages

With an estimated 70 percent of 911 calls made from cell phones, FCC encourages 911 emergency call centers to accept text messages from mobile phones or devices in addition to voice calls. Before 2014, none of the Nation's PSAPs (i.e., emergency call centers) were capable of receiving text-to-911 requests. This measure analyzes the cumulative number of new public safety answering points ready to receive text-to-911 requests. As of December 28, 2016, 754 of the Nation's 6,419 public safety answering points are ready to receive text-to-911 messages.



Percentage of people in imminent danger saved in the maritime environment

Each year, FEMA, the Air Force Rescue Coordination Center, the National Park Service, and the U.S. Coast Guard (USCG) collectively assign or carry out tens of thousands of rescue missions in urban, inland, and maritime/coastal environments. In particular, USCG serves as the Federal search and rescue coordinator for the maritime environment. This measure assesses the percentage of people in imminent danger saved each year by USCG. Though factors beyond USCG's control can lead to tragic outcomes, the percentage of people saved in fiscal year 2016 was 79.3 percent.



Response

Key Findings

Key Finding:

Public- and private-sector partners are collaborating to advance diagnostics, case monitoring, and case management in response to the Zika virus outbreak.

As of December 28, 2016, CDC reported more than 39,700 cases of Zika virus infections in U.S. states and territories. While infected adults can experience no to mild, flu-like symptoms, Zika virus infection during pregnancy can cause serious birth defects. Federal, state, and local partners have worked to diagnose Zika cases, monitor infections in pregnant women and infants, and expand care for affected infants and families.

Diagnostic Tests: Federal agencies have collaborated with private research companies since the start of the outbreak to advance Zika diagnostic capabilities. Because no commercially available U.S. Food and Drug Administration (FDA)-approved diagnostic tests existed for the Zika virus disease before the current outbreak, FDA issued 14 Emergency Use Authorizations (as of December 12, 2016). These authorizations allow the use of unapproved Zika diagnostic tests during an emergency. To expedite diagnostic development, ASPR and BARDA coordinated the collection and sharing of blood samples from individuals infected with Zika with diagnostic companies to validate test performance. Furthermore, CDC purchased $2.5 million in supplies and equipment for laboratories in every state, the District of Columbia, Puerto Rico, and 16 DoD facilities to expand access to Zika testing. As of September 2016, only two states have not completed the process to be able to use the diagnostic test associated with the purchased materials. Before this purchase, local health departments that could not perform Zika testing had to send samples to CDC.

Safeguarding the U.S. Blood Supply Against Zika Virus

Because most people infected with the Zika virus do not show any symptoms, blood donors may be unaware that they are infected. Although no reported Zika virus transfusion–transmitted cases have occurred in the United States as of January 2017, documented cases of probable Zika virus transfusion–transmitted cases have occurred elsewhere (in Brazil). In addition to supporting diagnostic tests for Zika in individuals, BARDA is working on developing diagnostic tests that enable detection of the Zika virus in the blood supply. Although no FDA-licensed test for the Zika virus exists, FDA Investigational New Drug authorizations are allowing blood centers in all states to use these tests to screen donated blood. In addition, FDA-approved devices that can effectively reduce the amount of Zika virus in blood components (i.e., plasma, platelets) provide an alternative means of ensuring the safety of the U.S. blood supply.

Surveillance: To monitor the number of pregnant women with evidence of Zika virus infection and track infant outcomes, government agencies implemented various surveillance measures. The CDC created the U.S. Zika Pregnancy Registry to collect information from state, local, tribal, and territorial health departments (except for Puerto Rico) on pregnancy and infant outcomes following laboratory evidence of Zika virus infection during pregnancy. As the number of Zika virus cases is significantly higher in Puerto Rico, the Puerto Rico Department of Health worked with CDC to develop a similar Zika

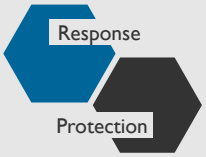
surveillance system, the Zika Active Pregnancy Surveillance System. The CDC uses the information from these surveillance systems to update clinical care recommendations, plan services for pregnant women and families affected by Zika virus, and improve prevention of infection during pregnancy.

Case Management: Public health agencies are working to expand awareness about the Zika virus and the issues associated with caring for infants affected by congenital Zika virus infection. Case management is particularly challenging for infants, since knowledge regarding the potential effects of Zika virus infection during pregnancy is limited. Nevertheless, HHS's Health Resources and Services Administration (HRSA) and ASPR both released planning resource guides, such as "Supporting Children with Special Healthcare Needs Planning Resource," which describe Federal and nonprofit services and programs for infants and children with special healthcare needs. These resources can help support the complex health needs of families affected by the Zika virus. CDC released interim guidance for doctors and healthcare providers on evaluating and providing care for pregnant women or infants with possible Zika virus infection, which will be updated as understanding of the virus evolves. CDC continuously engages with professional medical organizations to share any advancements in Zika virus knowledge.

Public- and private-sector partners are also involved in other efforts to improve care for children and families affected by the Zika virus, including:

- *In May 2016, ASPR developed Promoting Stress Management for Pregnant Women during the Zika Virus Disease Outbreak, which includes strategies that healthcare providers can use to help their pregnant patients manage stress during a Zika virus update. ASPR also partnered with HHS's Office of Minority Health to produce a culturally appropriate, Spanish-language version of the document.*
- *HRSA awarded grants to Puerto Rico, the U.S. Virgin Islands, and American Samoa health departments to fund healthcare and support services for children and families affected by the Zika virus.*
- *HHS and the American Academy of Pediatrics are collaborating to provide technical assistance and education, including tele-mentoring and consultation, to clinicians in the United States, including Puerto Rico.*
- *The Puerto Rico Primary Care Association, in partnership with the Migrant Clinicians Network, is using a telecommunications platform to host monthly meetings with seven clinics across the territory for clinicians to collaborate and discuss how they are addressing problems with Zika diagnosis and treatment in their communities.*
- *Through a cooperative agreement, CDC has worked with the American Congress of Obstetricians and Gynecologists and the American Academy of Pediatrics to develop tools and resources (e.g., toolkits, videos) for healthcare providers and families.*
- *CDC has conducted surveys of providers to assess the understanding and uptake of clinical guidance.*
- *CDC has worked with many organizations during the public health response to Zika, including: the Society for Maternal-Fetal Medicine; the Infectious Diseases Society for Obstetrics and Gynecology; the American Academy of Family Physicians; the American Nurses Association; the Association of Women's Health, Obstetric and Neonatal Nurses; the Association of Maternal and Child Health Programs; the Association of State and Territorial Health Officials; the National Association of County and Health Officials; CityMatCH (the National Organization of Urban Maternal and Child Health Leaders); MotherToBaby; and Family Voices. In addition, CDC is closely working with the Centers for Medicare & Medicaid Services and HRSA.*
- *CDC has instituted a new local health department program that assigns individuals to local health departments to help with surveillance, outreach, and referral to care.*

Mission Area Connections



Information Sharing

The increasing pace and scale of global human movement is enhancing the potential spread and speed of disease transmission. In 2005, DHS signed a Memorandum of Understanding (MOU) to, among other forms of cooperation, share traveler information with HHS to prevent the introduction, transmission, and spread of serious communicable diseases in the United States. However, the MOU did not fully address the sharing of traveler information from HHS to DHS. During the 2014 Ebola virus epidemic, this became problematic when DHS needed quick information from HHS's CDC on potentially infected persons traveling to or arriving in the United States. To improve information sharing between DHS and HHS, the two departments signed a new MOU in 2017 to allow for the rapid provision of traveler information by HHS's CDC to DHS's CBP, when appropriate.

Evaluation of U.S. Capacities for Public Health Emergencies

In 2016, ASPR led 23 Federal agencies in a comprehensive self-assessment of U.S. capacities to detect, prevent, and respond to public health emergencies. An external, independent evaluation of those capacities by a multinational, multi-sectoral team of experts under the Framework of the International Health Regulations followed, which resulted in a report outlining strengths and areas for improvement. The Office of Policy and Planning within ASPR is coordinating the development of a strategic "roadmap" to address the health security gaps identified in the report; and working with Federal agencies to describe as many as 40 specific action plans that address the highest priority gaps. Over the next two to three years, the Office of Policy and Planning will continue to track progress on the action plans and prepare the U.S. Government to conduct another independent evaluation in 2020.

Key Finding:

Complex incidents that do not fall within the Stafford Act continue to challenge Federal response.

A Stafford Act declaration provides the legal authority for the Federal Government to provide specific forms of supplemental Federal assistance to jurisdictions during an emergency or major disaster that overwhelms state, local, tribal, and territorial governments. Most notably, a Stafford Act declaration triggers specific funding mechanisms, like the Disaster Relief Fund, which are otherwise unavailable to Federal agencies. In incidents that do not receive a Stafford Act declaration, there is no identified mechanism to fund the response, leaving agencies to seek funding solutions on an ad hoc basis. Although the lead Federal agency routinely handles incident response in a non-Stafford incident, the incident's scale, complexity, and implications may require coordinated Federal support across agencies. Examples include the 2012–2013 national drought, the 2014 influx of unaccompanied children across the Southwest border, the 2014 Ebola virus epidemic, the Flint Michigan Water Contamination, and the Zika virus outbreak. The 2015 *National Preparedness Report* detailed interagency coordination challenges in responding to non-Stafford Act events due to uncertainty regarding when, how, and under whose authority national-level coordination structures could be used.

HHS Public Health Emergency Declaration for Zika Virus Outbreak

In 2016, the vast majority of Zika virus infections in the United States and its territories occurred in Puerto Rico. Consequently, on August 12, 2016, the Secretary of HHS declared a public health emergency for Puerto Rico. The public health emergency declaration allows HHS to award grants, access emergency funds, and temporarily appoint personnel. In a follow up to this declaration, HHS staffed a group of public health experts in Puerto Rico to coordinate Federal, state, and local response activities. Since HHS does not have a designated disaster fund, however, the effectiveness of the response was contingent on receiving additional appropriations from Congress, according to HHS. On November 4, 2016, the Secretary of HHS renewed the public health emergency declaration.

During the Zika virus outbreak, the Nation's early collaboration and application of National Response Framework coordination structures highlighted progress in managing a non-Stafford incident response. To address coordination challenges reported in previous responses, the President declared HHS as the lead Federal agency for managing both response and recovery activities. HHS's leadership role during the Zika virus outbreak, as well as the Flint water contamination crisis (see page 83), highlights its new and evolving responsibility to coordinate Federal efforts in the face of threats to national health security. Despite some initial confusion in response efforts, HHS (with ASPR acting as its lead representative) coordinated Federal agencies early in the Zika virus outbreak to efficiently support state and local response efforts. Beginning January 5, 2016 ASPR convened the Disaster Leadership Group for Zika response; this group brings together senior leaders from across the operating and staff divisions of HHS to discuss major policy decisions, align efforts, and maximize response resources. Since February 2016, a broader group of Federal agencies have coordinated efforts through the ASPR-led Zika Virus Task Force, which developed the *United States Government Zika Virus Disease Contingency Response Plan* to outline Federal agency roles and responsibilities in combatting the spread of Zika virus. In addition, ASPR extended the concept of a Unified Coordination Group—a National Response Framework coordination structure traditionally used in Stafford Act events—to synchronize, augment, and integrate ongoing Zika prevention and response activities. In Puerto Rico, the most severely affected U.S. jurisdiction, ASPR, FEMA, and other Federal agencies established the first-ever Unified Coordination Group in response to a biological incident. Based on lessons learned from the Zika virus outbreak, Federal agencies are refining the requirements and processes for establishing a Unified Coordination Group in non-Stafford incidents to improve future responses.

Lessons Learned from the 2014–2016 Ebola Virus Disease Epidemic

To strengthen the response to future biological incidents, Federal agencies are working to implement lessons learned from the Ebola virus epidemic. In June 2016, *The Report of the Independent Panel on the HHS Ebola Response* found that the United States was not prepared to respond to emergent crises that require a rapid, integrated domestic and international response; did not produce communications with an appreciation for the public's fear; and applied different policies at the Federal, state, and local level. In response to these findings, HHS published the *Ebola Response Improvement Plan* detailing actions the Department plans to take to improve preparedness and response efforts for future public health crises. HHS will release at least two reports in the next year to delineate progress on each active action item described in the plan.

Key Finding:

Some state and local jurisdictions are taking advantage of private-sector and nonprofit delivery mechanisms to address persistent challenges in dispensing medical countermeasures.

During a public health emergency, the Nation's largest supply of potentially life-saving pharmaceuticals and medical

supplies for use in a public health emergency, the SNS, can quickly distribute large quantities of medical countermeasures to state, local, tribal, and territorial jurisdictions, which in turn dispense the countermeasures to affected populations. However, state and local authorities have identified challenges in delivering supplies to affected individuals during a public health emergency. These challenges include the public's unwillingness to place themselves at increased risk of exposure by going to a central site to receive countermeasures; potentially large crowds (and increased potential for exposure); and the inability of authorities to staff a more distributed approach to delivery.

To identify tools, plans, and resources that jurisdictions have implemented to address these challenges, ASPR led—in collaboration with CDC, DoD, and FEMA—six Medical Countermeasure Dispensing Planning Regional Summits in 2016. One best practice jurisdictions shared was using public-private partnerships. For example, Washington State developed and signed MOUs with over 400 pharmacies to use their existing infrastructure to dispense medical countermeasures during a public health emergency. In 2016, 83 percent of Washington residents lived within five miles of a participating pharmacy. More broadly, Federal agencies used best practices identified during the summits to inform a national virtual tabletop exercise, as well as to develop "Emerging Best Practices in Medical Countermeasures Dispensing," which is a training course available through the Emergency Management Institute.

Federal, state, and local governments have also begun coordinating with Meals on Wheels America to better assist individuals unable to travel to a pharmacy or dispensing site during future public health emergencies. In 2016, CDC collaborated with Meals on Wheels and state and local jurisdictions to develop standardized protocols and processes that jurisdictions can use to have Meals on Wheels deliver medical countermeasures to its existing clients. Several jurisdictions have already partnered with Meals on Wheels to support medical countermeasures dispensing, including counties in Maryland and North Carolina, and the states of Kansas, Oregon, and Massachusetts.

Key Finding:

Federal agencies demonstrated their agility by anticipating and reacting to evolving response needs during Hurricane Matthew.

After Hurricane Matthew made landfall on October 4, 2016, in Haiti, the National Hurricane Center projected that Hurricane Matthew would hit the United States in Florida as a Category 4 storm and cause mass evacuations across the Southeast United States from Florida to South Carolina.

In light of the possible consequences of such an approaching storm, FEMA took numerous steps to ensure rapid support to affected communities. Although FEMA has prepositioned resources ahead of other storms, the agency took a faster approach toward deploying personnel in Hurricane Matthew than in response to previous storms. For example, on the day of the first Matthew-related major disaster declaration, FEMA had deployed 1,390 personnel to Florida, Georgia, North Carolina, and South Carolina, compared to slightly more than 600 staff deployed to potentially impacted states for Hurricane Sandy over a similar time period. In addition, FEMA prepositioned 2.8 million meals, 3 million liters of water, and 48,000 blankets.

Other Federal agencies and organizations mobilized or prepared resources prior to Hurricane Matthew's arrival:

- *USACE worked with FEMA to coordinate mission assignments four days prior to the storm's landfall. A mission assignment for temporary emergency power set ahead of the storm expedited the installation of 26 generators at damaged facilities after the storm.*
- *HHS deployed multiple teams and liaison officers to potentially impacted states. HHS also securely disclosed Federal health data from its emPOWER Initiative to support life-saving outreach efforts to more than 40,000 at-risk individuals with access and functional needs in Florida and North Carolina.*
- *DoD transported more than 120,000 gallons of gasoline and diesel fuel, 236,000 meals, and other commodities to military bases in Georgia and North Carolina, and set prepare-to-deploy orders for 21 search and rescue aircrafts and*

three teams in preparation for response and recovery activities.

- *With assistance from FEMA, the American Red Cross and other voluntary partners deployed 1,400 staff to support anticipated sheltering and feeding operations.*
- *In addition to having more than 100 AmeriCorps Disaster Response Team members on standby, AmeriCorps deployed 45 staff members to Emergency Operations Centers in Florida and 20 staff members to a special-needs shelter ahead of the storm.*

Federal departments and agencies adjusted their response posture and assigned deployment locations as Hurricane Matthew's forecasted track evolved. On October 8, Hurricane Matthew made landfall in South Carolina rather than in Florida, causing severe flooding and coastal damage to South Carolina, Georgia, and North Carolina. One day after Hurricane Matthew's landfall, FEMA and other Federal agencies significantly readjusted staff deployments so that the number of staff deployed to Florida and Georgia decreased to allow a robust deployment of staff to the affected areas of North and South Carolina. During this same period, though deliveries of essential commodities continued to Florida, Georgia, and South Carolina, FEMA increased its deliveries to North Carolina by 93 percent (compared to 68 percent in Florida) to adjust for the location of actual landfall.

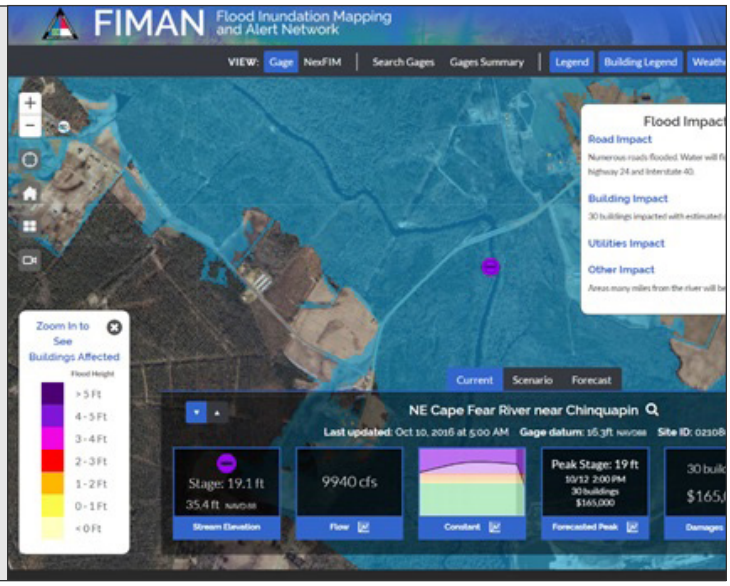
NOAA Surveying Efforts Following Hurricane Matthew

In the aftermath of Hurricane Matthew, NOAA mobilized various surveying capabilities to assist in response efforts. NOAA's ship, the *Ferdinand R. Hassler*, and Navigation Response Teams provided rapid response surveys of the ports of Charleston, South Carolina, and Savannah, Georgia, that allowed ships to transit safely in and out of the ports. NOAA Office of Coast Survey staff also assisted USACE in completing surveys between pilot areas and USACE docks.

Additionally, NOAA's National Geodetic Survey (NGS) collected aerial oblique imagery along the East Coast from Key Largo, Florida, to Cape Henry, Virginia, and imagery over inland portions of South Carolina. Compared with traditional imagery, oblique imagery captures a wider area and provides visuals of the sides of buildings (as opposed to only the tops of buildings). In total, NGS collected 5,177 images (covering 1,230 square miles), which were used to assess damage to infrastructure and buildings, coastal hazards to navigation, and flood damage.

Response Case Study: North Carolina's Real-Time Flood Warning System

North Carolina's Flood Inundation Mapping and Alert Network System integrates USGS and state-collected data to analyze, map, and communicate flood risks in real-time to emergency responders and the public. During Hurricane Matthew, the system developed detailed flood maps and projections of peak flood levels, based on National Weather Service flood forecast information, that helped local emergency responders plan transportation routes, state troopers identify the hardest-hit areas to support, and two prisons decide whether to evacuate. In total, the system received 3.7 million hits by potential users during this period.



Key Finding:

The whole community supported the response to the August flooding in Louisiana through both traditional and innovative practices, although mass care challenges remain.

In 2016, the United States experienced several severe flooding incidents. According to NOAA, four incidents each resulted in more than $1 billion in damages. In particular, the August flooding in Louisiana was the most damaging U.S. flood since Hurricane Sandy in 2012. Record rainfall amounts hit some areas over a period of less than 48 hours.

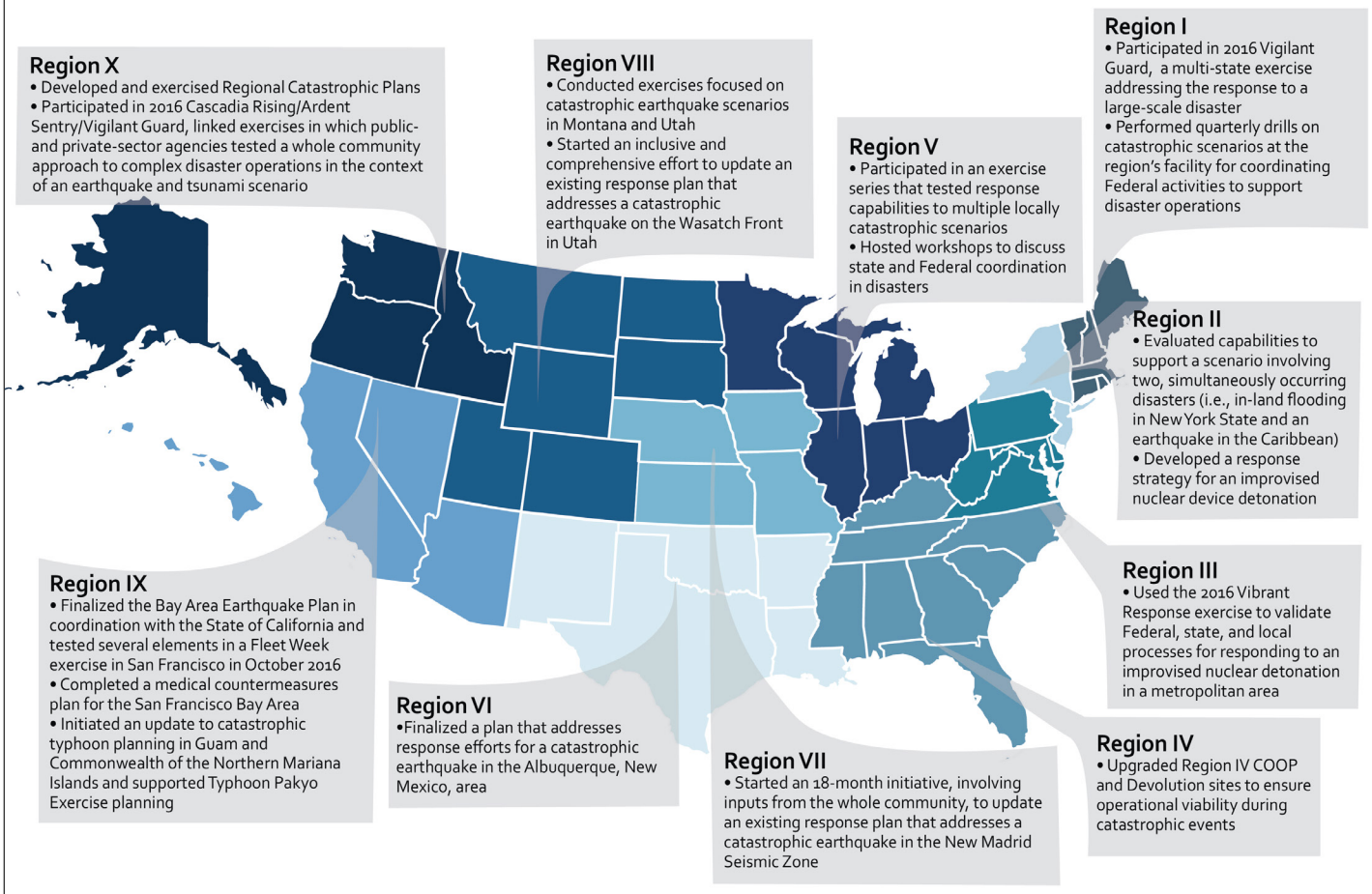
The sudden, swift-moving floodwaters trapped Louisiana residents in homes and cars, resulting in thousands needing rescue. In response, government agencies and volunteers conducted search and rescue operations that rescued 30,000 individuals, as well as thousands of pets. For example, the Louisiana National Guard deployed more than 3,800 Guardsmen and rescued more than 19,000 individuals and 2,660 pets. FEMA Urban Search & Rescue deployed 120 personnel and the Texas Urban Search & Rescue Task Force assessed 5,320 buildings and secured 17 caskets. Moreover, groups of local volunteers known as the "Cajun Navy" used their boats to rescue thousands of additional individuals trapped by floodwaters. FEMA Urban Search & Rescue delivered "Just-In-Time" training to volunteers, who had no prior knowledge of search and rescue protocols, and provided essential mapping and GPS equipment from their task force cache to support search squads. Since cache resources were insufficient to support all search squads, volunteers also used smart phones and other alternatives to track and document searches.

In their annual State Preparedness Report submissions, states and territories most frequently indicated Mass Care Services capability gaps in "sheltering" (63 percent of all responses). During the flooding in Louisiana, public- and private-sector partners sought to address the extensive demand for mass care services. However, the Louisiana flooding revealed several challenges in mass care response efforts. For example, Federal and community partners reported difficulty in finding hotel rooms, including accessible hotel rooms, to participate in sheltering; tracking hotel use by survivors; and providing survivor transportation assistance, particularly accessible transportation assistance. In addition, community service organizations described lower volunteer turnout and deficiencies in volunteer housing compared to previous response efforts.

Response Case Study: Multi-Agency Shelter Transition Task Force

During the August flooding in Louisiana, FEMA created a Multi-Agency Shelter Transition Task Force to transition survivors from shelters into temporary housing. Task force teams comprised representatives from Federal and nongovernmental organizations, including FEMA, the American Red Cross, and Catholic Charities. Teams reviewed survivor cases as a group, which increased coordination of resources across agencies and organizations to best support the needs of disaster survivors, including maintaining the health, independence, and self-determination of individuals with disabilities.

Catastrophic Preparedness



Each year, FEMA conducts various activities nationwide to better prepare for catastrophic incidents. For example, in June 2016, more than 20,000 individuals representing Federal, state, and local governments; tribal nations; private sector businesses; and nongovernmental organizations participated in a four-day exercise addressing a 9.0-magnitude earthquake along the Cascadia Subduction Zone—a 700-mile fault line off the coast of the Pacific Northwest. The exercise helped test and validate existing catastrophic plans, uncovering strengths and areas for improvement in coordinating delivery of Response core capabilities, particularly Critical Transportation; Mass Care Services; Operational Communications; Operational Coordination; Public Health, Healthcare, and Emergency Medical Services; and Situational Assessment (see also page 96). For example, while some jurisdictions effectively communicated the status of their transportation infrastructure and ongoing damage assessment efforts, there was an overall failure to quickly prioritize which key transportation routes to restore into and out of the affected region. Updates to existing plans are occurring based on lessons learned and senior leadership guidance from this exercise. As shown in the map above, this exercise was one of several efforts in 2016 to improve catastrophic preparedness.

Response Case Study: District of Columbia Mass Fatality Exercise

To address areas for improvement highlighted by the Navy Yard shooting in 2013, the District of Columbia Office of the Chief Medical Examiner hosted the District's first-ever Mass Fatality Symposium and full-scale exercise in September 2016. This event brought together stakeholders from across the National Capital Region (including the fire and emergency medical services, police departments, and health departments), as well as international fatality management experts, to share information and to discuss lessons learned from mass fatality incidents. Through the exercise, the District evaluated Homeland Security Grant Program investments it had made to address gaps identified in the Navy Yard shooting after-action report. The investments—which included the *District Wide Fatality Management Plan* and the purchase of a mobile command vehicle, mobile digital x-ray system, and field disaster morgue—significantly improved the District's mass fatality services. The exercise enabled the District to validate its strength in multi-agency leadership and collaboration, as well as the ability to adapt to lead agency protocols and procedures.

Key Finding:

Though Federal, state, and local agencies have worked to address challenges in interoperability for first responder emergency communications, progress has been incremental.

Although the ability of Federal, state, and local responders to communicate by voice, data, and video in real-time is critical to an effective response, emergency communication systems often lack interoperability. In their 2016 State Preparedness Report submissions, states and territories most frequently identified Operational Communications capability shortfalls in "interoperable communication between responders" (63 percent of all responses). To address this problem, the Federal Government, in conjunction with public safety organizations and entities, has been working since 2012 to establish a single, nationwide, interoperable network—the Nationwide Public Safety Broadband Network (NPSBN)—for public safety and first responder communications. The FirstNet, the independent government authority established by law to create this network, has continued to make progress toward this goal:

- *In fiscal year 2016, FirstNet held over 400 meetings with states, territories, and tribes to ensure the NPSBN is designed to meet the needs of public safety agencies throughout the Nation.*
- *In November 2016, FirstNet opened a laboratory in Boulder, Colorado, to provide a test environment for validating and verifying future features, devices, and applications before their deployment to the NPSBN.*
- *As of December 2016, FirstNet is evaluating proposals to select a private-sector partner to build and deploy the NPSBN.*[8]

Interoperability challenges often stem from issues of governance, procedures, training, and education, rather than technology. To help address these issues, Federal, state, and local partners continue to use state- and regional-level governance bodies to provide a forum for public safety officials to set standards, share best practices, and conduct joint exercises and training. In addition, the DHS Office of Emergency Communications (OEC) Interoperable Communications Technical Assistance Program provides direct support to state, local, and tribal emergency responders and has helped promulgate best practices and

[8] Since the writing of this report, FirstNet has selected a network partner and on March 30, 2017, announced the award of the NPSBN contract.

standards nationwide. In fiscal year 2016, OEC conducted 21 statewide communication interoperability plan workshops and completed 180 requests for technical assistance, including 27 requests for training on broadband technologies. As of December 2016, while all 56 states and territories have a foundational strategic plan that addresses interoperability issues, 54 have revised statewide communication interoperability plans.

Also in fiscal year 2016, OEC developed and implemented the Interoperable Communications Capabilities Analysis Program through a series of six pilot observations during planned events in California, the District of Columbia, Hawaii, Indiana, Los Angeles, and San Antonio. The purpose of these pilots was to observe multi-jurisdictional and multi-disciplined planned events to identify best practices and gaps between the stated communication needs of public safety agencies and their current assets. The program builds on groundwork laid in 2010, when OEC worked with public safety agencies to measure progress made toward interoperability. Additionally, OEC and the National Governors Association hosted workshops in five states to review and identify best practices and strategies to implement in their statewide interoperability plans. Through these workshops, states recognized the need to identify a single entity to oversee all aspects of emergency communications; to secure sustainable funding for that entity to ensure seamless interoperability; and to increase education and outreach to public safety agencies to avoid misconceptions about interoperable communications. OEC is incorporating these lessons learned and best practices into future technical assistance offerings and workshops.

Response Case Study: Datacasting Pilot in Houston, Texas

In 2016, the City of Houston piloted DHS's datacasting capabilities during the Republican Primary Debate in February and the NCAA Final Four Basketball Tournament in April. Supported by the DHS Science and Technology Directorate, datacasting technology uses available bandwidth in digital television signals to deliver encrypted data to targeted recipients. During the events, the city was able to securely share emergency operations center displays, surveillance camera footage, and live-stream mobile videos to public safety officials from multiple agencies, increasing situational awareness. By taking advantage of existing television infrastructure (with its pre-existing redundant systems), datacasting provides a relatively inexpensive, highly reliable solution to current interoperability challenges. Datacasting is meant to be complementary to, not competitive with, the NPSBN by providing a supplemental broadband capability to offload bandwidth-intensive content (e.g., video footage). In October 2016, DHS and America's Public Television Stations—a nonprofit organization of 350 public television stations in all 50 states—signed an agreement to make datacasting technology available nationwide.

In 2016, FCC also took steps to improve interoperable communications between U.S. and Canadian responders. First responders on both sides of the U.S.–Canadian border frequently provide cross-border assistance to nearby jurisdictions, but, until recently, faced challenges communicating with one another. For example, in 2007, a Canadian fire truck was delayed at the border while attempting to respond to a fire in New York because it was unable to communicate with the border crossing station or on-scene incident commander. A 2014 letter of intent updated the 1952 treaty between the United States and Canada, which allowed public safety agencies to operate mobile radios across the border, to allow public safety agencies to use portable radios, and to use local or cross-border frequencies to communicate with responding agencies. As a result, in June 2016, FCC released guidance to U.S. public safety agencies seeking to cross into Canada, to communicate

with the United States from Canada, to host Canadian responders on U.S. frequencies, and to use Canadian frequencies to communicate with Canadian first responders. The guidance, developed in collaboration with Canada, helps improve communications for first responders on both sides of the border.

Response Case Study: Canada-United States Enhanced (CAUSE) Resiliency Experiment Series

In April 2016, the DHS Science and Technology Directorate's First Responders Group, in collaboration with Public Safety Canada and Defense Research and Development Canada's Centre for Security Science, carried out the fourth installment of the CAUSE Resiliency experiment series (i.e., CAUSE IV). The goals for this series are to build and strengthen binational communications interoperability, and to connect, test, and demonstrate emerging operational technologies. CAUSE IV took place at the Blue Water Bridge (on the Michigan-Ontario border), the second-busiest transit point between the United States and Canada, and consisted of two distinct, but connected scenarios. The first tested voice and data communications during cross-border patient transfers, and the second tested alerts and warning during a tornado. Participants found that the interoperable technologies tested facilitated the exchange of cross-border voice, video, and data communications; and supported decision-making processes for local and cross-border response operations. However, the experiment also identified the need to establish formal policies and procedures to guide the appropriate use of these technologies and optimize their benefits.

Key Finding:

New Federal guidance establishes a mechanism to coordinate Federal response to large-scale malicious cyber activity, while cyber threats such as attacks on industrial control systems continue to rise.

Reacting to persistent concerns over cybersecurity, the Federal Government has sought to better coordinate the U.S. response to malicious cyber activity. One such example is Presidential Policy Directive (PPD) 41, which provides a framework for responding to large-scale cyber incidents with national security implications. For significant cyber incidents,[9] PPD 41 directs that a Cyber Unified Coordination Group will be stood up. This approach addresses cyber incidents with the same coordination structure already used to coordinate Federal interagency responses to other types of incidents. In particular, this Cyber Unified Coordination Group identifies three sets of actions to take in response to a cyber incident: threat response, asset response, and intelligence support (see Figure 11). An interagency working group also released a document advising the whole community on how and when to report major cyber incidents to the Federal Government. Additionally, a finalized *National Cyber Incident Response Plan* further clarifies the roles and responsibilities of Federal agencies and state, local, and private-sector partners in the event of a cyber incident, including significant cyber incidents.

[9] PPD 41 defines a significant cyber incident as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Cyber Unified Coordination Group			
Lead Agency	**Threat Response - FBI**	**Asset Response - DHS**	**Intelligence Support - ODNI**
Role	Addressing law enforcement functions such as gathering evidence, conducting investigations, attributing the attack, identifying patterns or related attacks, and identifying means to pursue and mitigate the immediate threat	Providing technical assistance to affected entities, identifying other sectors that may be vulnerable after an incident, and mitigating broader risks to regions or sectors	Contributing to the building of situational awareness during an incident, promoting information sharing, analyzing threat trends, identifying knowledge gaps, and weakening the capabilities of adversaries

Figure 11. A Cyber Unified Coordination Group, as defined by PPD-41, addresses three sets of activities, each led by a specific Federal entity.

The Federal Government is taking steps to enhance information sharing and responses to cyber incidents. FBI notifications to critical infrastructure sector victims of cyber attacks continued to rise in 2016 (i.e., up more than 450 notifications from 2015, an 11.5 percent increase in notifications recorded in Cyber Guardian). Cyber attacks on industrial control systems are of particular concern, in part because of the potential for costly physical consequences. Industrial control systems include a variety of computerized or automated functions that help operate large facilities such as utilities. Disruptions to these control systems could disable such facilities or create conditions that could result in physical harm or loss of life. In fiscal year 2016, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) closed 290 incidents involving critical infrastructure, principally affecting the Critical Manufacturing (63 incidents), Communications (62 incidents), and Energy (59 incidents) sectors. In 2016, DOJ indicted a group of alleged state-sponsored Iranian-based hackers in connection with several cyber incidents, including remote hackers that accessed the control systems of a dam in New York.

MISSION AREA CONNECTIONS

Response

Protection

VULNERABILITY ASSESSMENTS

ICS-CERT has also expanded its facilitation of domestic assessments to help operators of privately and municipally owned infrastructure identify and address vulnerabilities to secure their control systems. The team conducted 130 assessments across 12 sectors in fiscal year 2016, up from 112 assessments across eight sectors in fiscal year 2015. The assessments included:

- *Fifty-five Design Architecture Reviews, which provide critical infrastructure operators with a comprehensive technical review and cyber evaluation of their industrial control systems;*
- *Forty-three Network Architecture Verification and Validation assessments, which help owners and operators visualize traffic on their control-system networks; and*
- *Thirty-two Cyber Security Evaluation Tool assessments, which provide organizations with a broader understanding of their cybersecurity posture.*

Key Finding:

First responders have adopted new approaches to combat active shooters; however, recent events illustrated the need for expanded responder medical training.

To maximize lives saved, active shooter response tactics have shifted away from containment efforts to subduing the shooter, accessing the injured quickly, and rapidly providing appropriate medical care to address life-threatening injuries. In 2013, FBI adopted Advanced Law Enforcement Rapid Response Training, which emphasizes immediately engaging and neutralizing the threat, as the national training standard for active shooter response. Since 2002, more than 105,000 law enforcement

officers received this training. Moreover, the International Association of Chiefs of Police recommended in 2013 that all law enforcement personnel receive tactical emergency medical training, including life-threatening hemorrhaging control. Since then, additional opportunities for law enforcement officers to receive such trainings have emerged. For example, as part of DHS's "Stop the Bleed" campaign, which seeks to raise awareness of basic techniques to stop life-threatening bleeding, trauma surgeons trained more than 80 Tulane University police officers in 2016 on how to use tourniquets. In addition, FEMA supported the Tactical Emergency Casualty Care training—which covers how to stop bleeding, maintain airways, prevent hypothermia, and efficiently move patients—to more than 10,000 first responders.

Recent active shooter incidents have reaffirmed the value in the shift to using such tactics. In the 2015 San Bernardino shooting, responding officers formed a four-man team to immediately engage the shooter based on their active shooter training. Additionally, a fire medic assigned to a SWAT team triaged victims inside the Inland Regional Center where the shooting occurred, which an after-action review found enhanced victim extrication and survival. Similarly, during the 2016 Orlando nightclub shooting, officers began evacuating victims from the dance floor while a potential threat from the shooter still existed.

An after-action review of the San Bernardino shooting, however, found that law enforcement officers were not adequately trained to provide on-scene emergency medical care to shooting victims. In 2016, the Federal Government expanded funding opportunities available to state and local police departments to better support active shooter training, including medical training. Congress passed the *Protecting Our Lives by Initiative COPS Expansion (POLICE) Act of 2016* to allow law enforcement and medical personnel to use Office of Community Oriented Policing Services (COPS) grants—which more than 13,000 of the Nation's 16,000 law enforcement agencies have received since 1994—for active shooter training. Additionally, in December 2016, DHS announced the new Program to Prepare Communities for Complex Coordinated Terrorist Attacks, which will provide nearly $36 million in funding to state, local, tribal, and territorial jurisdictions to improve their ability to prepare for, prevent, and respond to complex coordinated terrorist attacks, such as active shootings.

Response Case Study: Active Shooter/Hostile Event Summit II

In January 2016, the InterAgency Board, a voluntary panel of emergency preparedness and response practitioners, and its Federal partners brought together over 80 participants from 14 agencies and organizations to the second Active Shooter/Hostile Event summit. The goal of the summit was to develop and publish a set of guidelines for municipalities to use in building their own Active Shooter/Hostile Event plans or modifying existing plans. The resulting *Active Shooter/Hostile Event Guide*, released in July 2016, includes specific procedures for incident command, emergency communications, medical operations, training and exercises, community outreach and engagement, and equipment.

Recovery

Mission Area Overview

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

Core Capabilities in Practice

The *National Disaster Recovery Framework* (NDRF) provides a flexible structure and process for jurisdictions affected by disasters to recover quickly and effectively. The NDRF identifies eight core capabilities needed to support the physical, emotional, and financial needs of disaster-affected community members.

Three core capabilities facilitate the effective implementation of disaster recovery activities. Communities use **Operational Coordination** to ensure that multiple levels of government and other recovery partners build successful coalitions. Key stakeholders provide regular input into pre- and post-disaster **Planning** processes to identify recovery objectives and how to best achieve those objectives. Community leaders convey the actions being taken to support recovery efforts and explain what assistance is available to residents and businesses through the **Public Information and Warning** core capability.

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

The remaining five core capabilities address specific aspects of recovery. Re-establishing the functions and facilities necessary to provide **Health and Social Services**—such as hospital care or healthcare, child care, counseling, and other services—helps address the physical and mental health of disaster survivors. Communities set strategies for **Economic Recovery** to return economic and business activities to a healthy state. The recovery process also involves experts coordinating with the community to preserve, protect, and restore **Natural and Cultural Resources**, including publicly and privately owned cultural assets and historical properties. Public- and private-sector owners and operators of **Infrastructure Systems** must also restore and sustain essential community services. Meanwhile, residents displaced by disasters seek temporary and permanent **Housing** solutions, including affordable and accessible housing.

The following are examples of actions taken in 2016 to improve preparedness that highlight the relationship among a select number of Recovery core capabilities:

Housing and Public Information and Warning

Following Louisiana's historic floods in August, state, local, and nongovernmental stakeholders—in coordination with the Federal agencies responsible for supporting disaster housing activities—hosted the first-ever Housing Resource Fairs in different state parishes. The events provided hundreds of Louisiana homeowners and renters with housing resources and information to aid in short- and long-term housing recovery. The fairs covered topics such as temporary and permanent housing solutions, insurance, and home elevation. To address the shortage of available rental units for displaced residents, the fair in East Baton Rouge also provided resources to help transition financially ready families from renting to purchasing a home, with the goal of freeing up rental units for others.

Planning and Operational Coordination

The Maryland Emergency Management Agency released the "Local Recovery Planning Toolkit," an online collection of materials and guidance to help local jurisdictions with their recovery planning. To assist jurisdictions in developing their own pre-disaster recovery plans, the toolkit provides materials from regional recovery initiatives underway in the state. Ellicott City played a role in developing some of these materials (as part of the Baltimore Urban Area's recovery planning efforts), which better prepared the city for recovering from flash flooding in 2016. The toolkit also includes guidance and case studies on transitioning the management of recovery efforts to a long-term recovery committee. Jurisdictions in Maryland have begun using the toolkit to help develop customized recovery plans.

Health and Social Services

In 2016, ASPR developed behavioral health materials and tools to ensure these considerations are integrated into response and recovery efforts. For example, ASPR updated its "HHS Disaster Behavioral Health: Current Assets and Capabilities" fact sheet, which helps emergency planners understand potential behavioral health resources to take advantage of during emergency response and recovery efforts. ASPR also developed a new fact sheet to assist HHS responders with effectively directing people to appropriate resources during times of extreme stress. In November 2016, ASPR released an update of the *HHS Disaster Behavioral Health Concept of Operations*, adding language to address incidents of mass violence and terrorism, and to further describe behavioral health assets and capabilities. ASPR also convened three interagency meetings with HHS, DOJ, the U.S. Department of Education, and the American Red Cross to enhance collaboration and information sharing in relation to providing behavioral health support after mass violence events, such as school shootings. As a result, ASPR developed internal tools and protocols to ensure a shared understanding of roles, responsibilities, and resources available in the aftermath of these types of incidents.

Natural and Cultural Resources and Economic Recovery

In February, the Deepwater Horizon Natural Resource Damage Assessment Trustee Council—including all five Gulf of Mexico states, NOAA, EPA, DOI, and USDA—released an all-inclusive restoration plan for the Gulf of Mexico as part of a legal settlement with BP stemming from the 2010 *Deepwater Horizon* oil spill. The plan builds on earlier activities and sets the approach for comprehensive restoration in the Gulf, including water quality, wildlife, and recreational activities. The plan also identifies possible effects of proposed actions on communities and their economies, such as employment opportunities or impacts to fishing industries. In addition to payments to address damages to natural resources, BP will provide up to $5.9 billion to the Gulf States and local governments to address economic damage claims resulting from the spill. BP will also pay $5.5 billion in civil penalties under the Clean Water Act, most of which will help restore natural resources, boost economic recovery, and strengthen tourism and seafood industries.

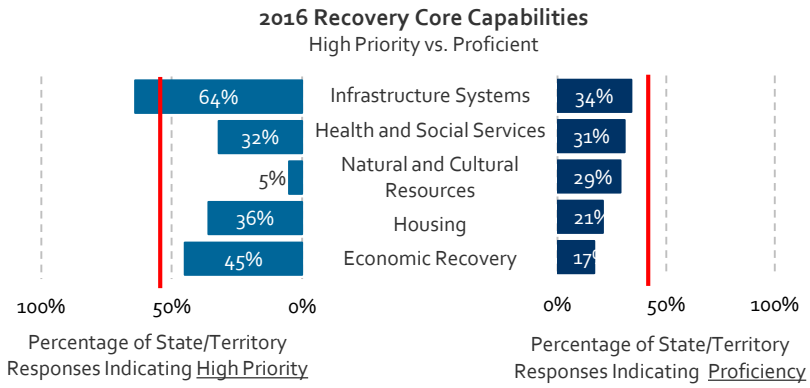
Summary of Progress

The Recovery mission area continues to face challenges. For the fifth consecutive year, states and territories reported some of their lowest levels of proficiency in Recovery core capabilities. Recovery-specific core capabilities also remain a lower priority for states and territories relative to most other core capabilities. Data does indicate that the Nation is focusing more attention on this mission area than before. Despite progress, five Recovery core capabilities—**Economic Recovery**, **Health and Social Services**, **Housing**, **Infrastructure Systems**, and **Natural and Cultural Resources**—continue to show proficiency levels that are well below average. In particular, the 2017 *National Preparedness Report* identifies four of these core capabilities—**Economic Recovery**, **Housing**, **Infrastructure Systems**, and **Natural and Cultural Resources**—as national areas for improvement (see page 12).

As captured in this section's key findings, recovery efforts for the Louisiana floods, Hurricane Matthew, and the Flint water crisis have called attention to specific challenges in **Housing**, **Health and Social Services**, and **Economic Recovery**, while highlighting improvements in **Operational Coordination**. Moreover, the current NEP cycle of exercises has also emphasized addressing the Recovery mission area. Specifically, 41 percent of NEP exercises addressed one or more core capabilities in the Recovery mission area, compared to 27 percent in the prior cycle. Based on FEMA preparedness grants in fiscal year 2015 (the latest year for which grant data by core capability are available), a smaller portion of funding goes to the Recovery mission area than to any other mission area. Excluding the core capabilities common to all mission areas (i.e., Planning, Operational Coordination, and Public Information and Warning), grant expenditures on Recovery core capabilities represented less than 1.3 percent of all FEMA preparedness grants in fiscal year 2015, with **Health and Social Services**, **Economic Recovery**,

Housing, and Natural and Cultural Resources each receiving less than $2 million.

States and territories reported the lowest proficiency ratings in the Recovery mission area for the sixth consecutive year (see Figure 12).[10] Moreover, excluding **Natural and Cultural Resources**, the proficiency ratings of all remaining Recovery core capabilities declined in 2016. In their State Preparedness Report submissions, states and territories reported a two percent decrease in proficiency ratings in the Recovery core capabilities between 2015 and 2016. This included a six percent proficiency decrease in **Housing** in 2016—the third-largest decrease of all core capabilities. Moreover, states and territories reported that Recovery core capabilities remain among those in the greatest danger of decline. Twenty-nine percent selected **Economic Recovery** as among those in most danger of decline, as well as 20 percent for **Natural and Cultural Resources**, **Infrastructure Systems**, and **Housing**.



Notes: Vertical red lines (|) indicate the average ratings for all core capabilities. The chart and statements do not include contributions from the three cross-cutting core capabilities—Planning, Operational Coordination, and Public Information and Warning

Figure 12. In their 2016 State Preparedness Report responses, states and territories provided information on their high priority core capabilities, as well as ratings on core capability proficiency.

Natural and Cultural Resources, **Health and Social Services**, and **Housing** were among the core capabilities that states and territories most frequently reported as low priorities. In particular, 52 percent reported **Natural and Cultural Resources** as a low priority, the most of any core capability. Conversely, **Infrastructure Systems** has consistently been the Recovery core capability with the highest priority rating—80 percent of states and territories selected it as a high priority in 2015 and 64 percent selected it as a high priority in 2016. Despite the high priority rating, however, states and territories reported a four percent decrease in proficiency in 2016.

Table 7 lists the most frequently identified "functional area" gap for each Recovery core capability, as selected by states and territories in their 2016 State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from an analysis of the Goal, NDRF, and other national-level preparedness doctrine.

[10] Unless otherwise noted, figures and statements do not include contributions from the three core capabilities common to all mission areas—i.e., Planning, Operational Coordination, and Public Information and Warning.

Table 7. In their 2016 State Preparedness Report responses, states and territories identified remaining gaps in their ability to accomplish various functions associated with each Recovery core capability.

Most Frequently Identified Functional Area Gap in Each Recovery Capability	
Core Capability*	Gap
Economic Recovery	Economic impact assessments
Health and Social Services	Determining health and social needs
Housing	Addressing housing shortages
Infrastructure Systems	Infrastructure site assessments
Natural and Cultural Resources	Environmental preservation and restoration
Operational Coordination**	Command, control, and coordination
	Establishing a common operating picture
Planning	Whole community involvement and cooperation
Public Information and Warning	New communication tools and technologies

* For core capabilities that cut across two or more mission areas, the 2016 State Preparedness Report did not include separate data requests that were specific to each mission area. Gaps identified for these core capabilities are identical for the different mission areas.
** The top-two functional area gaps for Operational Coordination were tied in terms of how frequently they were selected.

By the Numbers

SBA approved 25,235 Disaster Assistance Loans

In fiscal year 2016, SBA approved 25,235 Disaster Assistance Loans totaling more than $1.4 billion. Approximately 50 percent of this total stemmed from the August floods in Louisiana. Disaster assistance loans help businesses, nonprofits, homeowners, and renters repair and replace physical losses, and assist nonprofits and small businesses with post-disaster operating expenses.

30 states provided training on disaster recovery

In 2016, approximately 30 states used the "Recovery from Disaster: The Local Community Role" course to provide instruction to local communities, allowing greater access to the course (beyond solely Federal offerings). The course focuses on the roles and responsibilities of local disaster recovery teams, and provides guidance on developing and implementing pre- and post-disaster recovery plans.

FEMA consolidated 15 recovery policies

In September 2016, FEMA published *Individuals and Households Program Unified Guidance*, which provides recovery stakeholders with increased transparency about how the Individuals and Households Program works. The unified guidance consolidates 15 previously disjointed policies (many not publicly available) into a single reference.

Recovery Snapshots

Iowa Legal Aid App

In August, Iowa Legal Aid, a nonprofit organization that provides legal services and support to the state's vulnerable and low-income populations, launched a disaster relief mobile app that helps users prepare for, respond to, and recover from disasters. Among its many features, the app allows users to securely store insurance information, learn about post-incident assistance and legal rights, and communicate with Iowa Legal Aid staff following disasters. As of January 2017, more than 200 downloads of the app have occurred.

"Homes for White Sulphur Springs" Program

This program—a collaboration between Mennonite Disaster Service (MDS) and private sector partners—assists in the recovery of White Sulphur Springs, West Virginia, which experienced flooding in June 2016. The program buys out properties located in the floodplain and allows their owners to use proceeds from the sale toward purchasing homes in a new housing development (outside the floodplain). As of December 2016, the program had raised over $1.7 million, providing MDS with funds to purchase materials for 20 homes—many of which are already complete and occupied by disaster survivors.

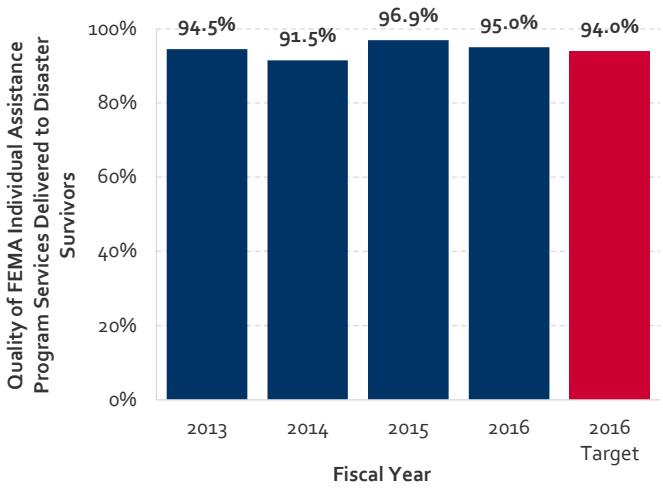
Spatial Analysis of Behavioral Health

In 2016, CDC published a study using geographic information system (GIS) and spatial analysis to locate at-risk areas and populations following Hurricane Katrina. The analysis indicated that hospitalizations increased from 2004 to 2008 and geographically shifted from flood-exposed areas to more insulated areas over time, with poverty as a central factor. The study demonstrates the potential for GIS tools to locate at-risk populations, which emergency managers can use to improve pre-disaster recovery plans and better allocate resources post-disaster.

Preparedness Indicators

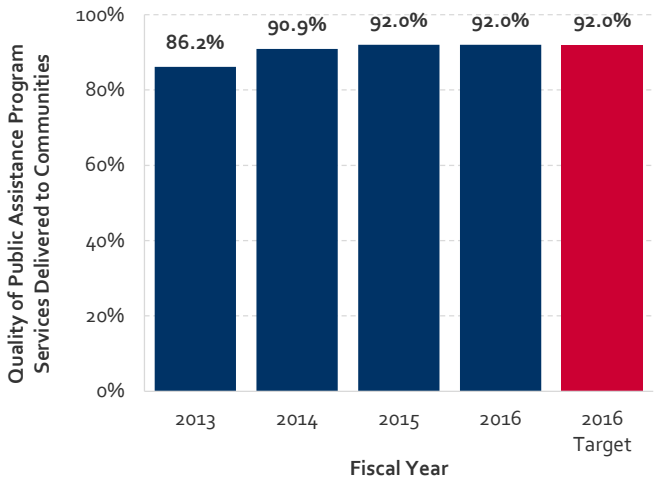
Quality of FEMA Individual Assistance Program services delivered to disaster survivors

FEMA's Individual Assistance Program helps individuals and households affected by disasters to recover as quickly and efficiently as possible. This performance measure demonstrates how well the program delivered services to affected individuals by combining metrics such as how long it took to award assistance funds, how quickly assistance call centers answered survivor calls, and how satisfied survivors were with the program. At 95 percent, fiscal year 2016 results surpassed the target set for the fiscal year (94 percent).



Quality of Public Assistance Program services delivered to communities

FEMA's Public Assistance Program provides grants—averaging $4.7 billion annually over the last 10 years—for infrastructure recovery and debris removal to state, local, and tribal governments so that communities can quickly recover from disasters. This performance measure combines inputs such as how quickly FEMA began addressing requests for assistance and how well tools and processes worked in delivering program services. At 92 percent, results from fiscal year 2016 were unchanged from the previous year. FEMA is implementing a new delivery model for Public Assistance that aims to improve the program's effectiveness and better meet the needs of applicants.



Recovery

Key Findings

Key Finding:

Recovery activities following the Flint, Michigan, water crisis demonstrate the adaptability of the private and public sectors in coordinating resources during a non-traditional disaster, despite challenges in addressing the crisis's ongoing effects.

In April 2014, the City of Flint, Michigan, changed its water source from Lake Huron to the Flint River. The river's water corroded municipal pipes, causing lead and other pollutants to leach into the city's drinking water and creating a public health crisis. In January 2016, President Obama signed an emergency declaration under the Stafford Act, authorizing FEMA to provide commodities such as water filters and test kits for the state to distribute. More broadly, he designated HHS as the lead Federal agency to coordinate Federal efforts in support of response and recovery. Public- and private-sector organizations also mobilized, using their own resources to contribute to Flint's recovery.

Private-sector organizations supported Flint's recovery needs in numerous ways:

- *In May 2016, 10 private foundations—including the Ford Foundation and the Robert Wood Johnson Foundation—committed nearly $125 million to the city.*
- *Grants to local businesses from programs such as the Moving Flint Forward Fund are assisting with economic recovery. By June 2016, the fund provided grants to 30 Flint businesses to help them retain jobs, make repairs, and purchase new equipment, among other needs.*
- *Philanthropic dollars helped Flint open a new early childhood learning center with a particular focus on children exposed to lead.*
- *United Way and the American Red Cross supported the establishment of community resilience groups, facilitated information sharing, and provided funding to community organizations that support vulnerable populations.*
- *The Food Bank of Eastern Michigan, with support from Pepsi Co. and the C.S. Mott Foundation, opened two mobile distribution centers that provide bottled water, food, supplies, and physical and mental health support to Flint residents.*
- *AARP also partnered with the City of Flint to send volunteers to inform seniors about FAST Start, a program to replace residential pipelines. The organization conducted a survey of senior residents, developed an action plan, and is planning to launch public service announcements on TV to increase its reach to seniors.*

State and local governments augmented these private-sector activities. In coordination with local partners and residents, state agencies developed a list of short-, intermediate-, and long-term goals to facilitate Flint's recovery. These goals addressed topics such as health and human services, education, water infrastructure, and economic development. The state also created the Flint Water Interagency Coordinating Committee, a group of city and state partners working toward solutions to address recovery issues. As of February 2016, total state funding for the water crisis topped $230 million.

At the Federal level, HHS introduced recovery considerations early in the Federal response and coordinated Federal recovery efforts through non-Stafford Act authorities. Numerous Federal agencies engaged in initial recovery efforts, and continue to work with state and local governments and community organizations to provide health and economic recovery services:

- *HHS coordinated efforts such as health screenings, behavioral health and nutrition programs, as well as long-term health studies to ensure the best health support and outcomes for residents exposed to contaminants. HHS also collaborated with the American Red Cross and the Genesee County Health Department to train behavioral health providers on providing psychological first aid.*

- *Through a National Dislocated Worker Grant, the U.S. Department of Labor is providing up to $15 million toward employment-related projects that include assistance with humanitarian and recovery efforts. The state received an initial $7.5 million award, which it is using to provide Flint residents with temporary employment performing recovery-related activities, as well as additional training and career assistance to help these individuals secure permanent employment.*
- *The USDA is working to ensure that children have increased access to foods rich in nutrients that may help reduce lead absorption. Under the Summer Electronic Benefits Transfer Pilot program, USDA expanded funds toward nutritious food purchases during the summer months for over 15,000 lead-impacted children in affected areas. The USDA also gave funding to several county schools for fresh fruit and vegetables for their students.*

Despite the progress public- and private-sector partners made during the recovery, a number of challenges emerged. For example, the Flint water treatment plant lacked the technical and managerial capacity to ensure that the water purchased from the Great Lakes Water Authority had adequate concentrations of the appropriate chemicals, including a chemical used to optimize treatment within the city's oversized and damaged distribution system. In October 2015, EPA formed the Flint Safe Drinking Water Task Force to provide the city with technical assistance to optimize treatment. Residents low usage of water, however, resulted in reduced flow through the distribution system, hindering the re-coating of pipes with a protective scale.

EPA Intervention in the Flint Michigan Water Contamination

Regarding EPA intervention in Flint, the EPA's Office of Inspector General (OIG) found that EPA had the authority and sufficient information to issue an emergency order months sooner than it did, to require the City of Flint, Michigan, and the Michigan Department of Environmental Quality to take necessary action to protect public health. The EPA OIG concluded that the delay was due to a lack of understanding of how and when EPA can use its emergency authorities to immediately address urgent public drinking water issues. The EPA OIG issued a management alert recommending that EPA update its guidance and provide staff training on issuing emergency orders under Section 1431 of the Safe Drinking Water Act.

Additionally, initial progress was slow in replacing the pipes that led to the contamination. As of late September 2016, Flint only replaced 177 of the several thousand lines with the $27 million in initial funds provided by the state. Moreover, while HHS and EPA announced that filtered water was safe for consumption on June 25, 2016, unfiltered water in Flint remained unsafe to drink throughout 2016. By the end of 2016, the city replaced approximately 800 lines, as well as refined its operational plan to replace 6,000 lines per year over the next three to four years. In January 2017, the Michigan Department of Environmental Quality reported that the most recent compliance period showed that lead in Flint's drinking water is now below the Federal action level established in the Lead and Copper Rule, which is 15 parts per billion. As of February 2017, the lead values in Flint's water remained below the Federal action level. Nevertheless, out of caution, EPA and state officials are advising that Flint residents continue to use filters while lead service lines are being replaced. The State of Michigan plans to continue its program to offer free water sampling for Flint's residents.

Key Finding:

Nongovernmental and private organizations provide critical support during disaster recovery, but their ability to sustain recovery efforts faces challenges.

Nongovernmental and private organizations are providing valuable recovery assistance in the wake of disasters. A 2016 RAND study called attention to the significance of corporate and nonprofit funding in disaster recovery. It noted that the private sector introduces flexible funding methods and strategies, as well as helps develop new technologies and brings them into play. Recent real-world events also demonstrate the opportunities for private organizations to supplement Federal efforts in disaster recovery. Since 2015, the Center for Disaster Philanthropy has awarded grants to approximately 20 organizations through its Midwest Early Recovery Fund to aid low-attention disaster recovery efforts, especially those supporting individuals disproportionately impacted by disasters. During the program's first two years, the Center

for Disaster Philanthropy made 31 grants totaling $1.6 million. The fund aided the 2016 establishment of the "Bridge to Recovery Coalition," which uses public and private resources to help repair homes owned by vulnerable and at-risk residents and damaged by the December 2015 flooding in Missouri.

In addition, state chapters of Voluntary Organizations Active in Disaster (VOAD) played a significant role in 2016 events, collaborating with the public sector and communities to address long-term recovery needs. In West Virginia, the state's VOAD chapter worked with both public- and private-sector partners on the Bridge Project, which helps families regain access to critical services by rebuilding bridges that were located on private property and destroyed by flooding in 2015. As of June 2016, the project rebuilt 16 bridges.

While the involvement of private organizations is crucial to disaster recovery, their ability to sustain recovery operations remains challenging. Although private organizations receive financial assistance and support from volunteers immediately following a disaster, both forms of support may not be stable over time. In 2016, organizations across the country found it increasingly difficult to attract and sustain volunteers and donors over the long-term recovery process. The number of volunteers assisting West Virginia flood recovery efforts fell rapidly after an initially large turnout. After two major flooding events in Louisiana, volunteers and resources to assist with home cleanup were also in short supply. Moreover, depleted resources and low volunteer turnout adversely impacted state VOAD capability. These challenges are exacerbated when an event receives low media attention, as was the case in Louisiana. Fundraising totals from the public also decreased in 2016, and donations shifted toward smaller organizations—including crowdsourcing websites—as opposed to larger, well-known organizations. These fluctuations and shifting trends can destabilize recovery activity on the part of private organizations.

Recovery Case Study: Louisiana Disaster Recovery Alliance

After observing limited levels of individual and philanthropic giving following the March 2016 flooding in Louisiana, the Federal Disaster Recovery Coordinator and Philanthropic Liaison team began working to engage the philanthropic community in Louisiana. After the August 2016 floods, this effort gained momentum and led to the establishment of the Louisiana Disaster Recovery Alliance. The purpose of the alliance was to garner support for ongoing recovery efforts by raising awareness about flooding disasters and strengthening cross-sector engagement. This first-of-its-kind consortium also brings together private, nonprofit, and corporate partners together with government stakeholders to improve recovery by fostering dialogue and information sharing. This includes more effectively using public and private resources for recovery efforts by avoiding duplications of effort. The Louisiana Disaster Recovery Alliance will also help philanthropic partners collect recovery funds during non-disaster periods to finance and support lower-scale disasters that do not receive a major disaster declaration.

Key Finding:

Re-establishing child care services is an important element in helping families to recover, but most child care centers face severe challenges after a disaster.

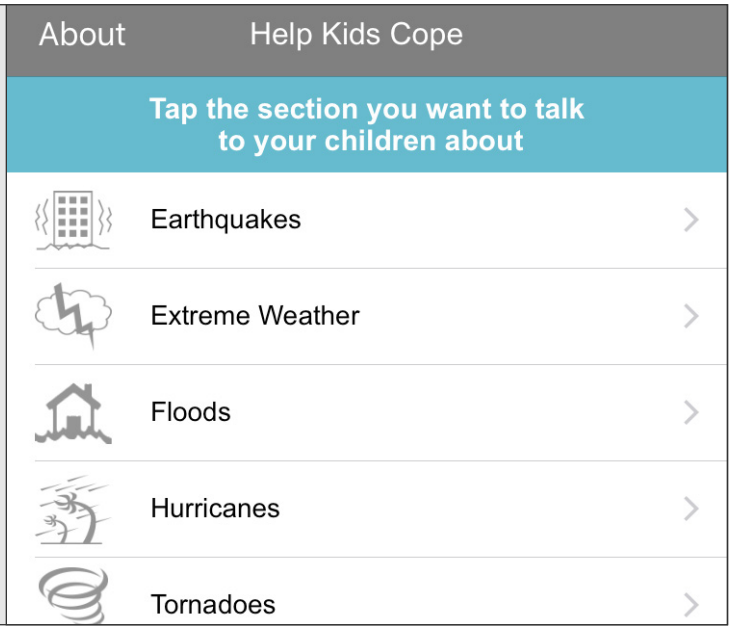
Child care services play an important role in recovery by ensuring that children are safe while their parents take part in rebuilding efforts. For example, without adequate child care services, parents may be unable to easily and quickly return to work. Child care providers, however, may face their own challenges following a disaster, preventing them from repairing damages or reopening quickly. After Hurricane Sandy in 2012, both center- and home-based child care providers reported challenges with rebuilding, including lengthy application processes for disaster assistance, and initially paying (or being unable to pay) for repairs out of pocket. More than four years later, the challenges facing child care providers remain. One month after the August 2016 Louisiana floods, 70 child care centers were still closed (10 percent of the state's licensed care capacity), affecting up to 5,000 children and their families.

One major challenge states and localities identify for child care centers in post-disaster recovery is funding. The vast majority of child care facilities are not eligible for financial assistance from FEMA's Public Assistance Program because they are businesses and for-profit entities. Centers may be underinsured, insurance claims processing may take many months, and they may lack funds to pay for repairs out of pocket, leaving the businesses financially vulnerable. Although private nonprofit child care centers are eligible for Public Assistance, many do not apply for undetermined reasons. Of the 70 Louisiana child care centers closed one month after the August floods, at least eight have closed their doors permanently.

Federal and state governments have made efforts to support recovery planning for child care centers in 2016. HHS's Administration for Children and Families published its *Post-Disaster Child Care Needs and Resources*, which outlines Federal and non-Federal resources that address various child care challenges following a disaster. Additionally, FEMA introduced its "Children and Disasters" webpage in April, consolidating information and links to approximately 50 resources related to children's needs in disasters. By the end of 2016, the webpage had received over 14,000 views. Some efforts have faced challenges and made limited progress. The Child Care and Development Block Grant Act of 2014, as amended, required each state to develop and fully implement a comprehensive statewide child care disaster plan—including guidelines for reopening child care facilities following a disaster—by September 30, 2016. However, as of March 2016, only 10 states had met this requirement.

Recovery Case Study: "Help Kids Cope" App

Following a disaster, children can experience—to a more extreme degree than adults—short- and long-term trauma and behavioral health problems, including post-traumatic stress disorder, depression, anxiety, and social withdrawal. In 2016, the National Child Traumatic Stress Network released its Help Kids Cope app, which is designed to assist parents in talking to their children about different disasters. The app includes sections on explaining disasters to children, as well as preparedness, response, and healing tips. By providing information on disasters before they occur, the app can help parents anticipate and prevent extreme reactions and prepare children for potentially traumatic experiences. Since its release, users have downloaded the app more than 1,500 times.



Key Finding:

Recent flooding events highlight ongoing gaps in delivering housing solutions efficiently and effectively after disasters.

In their 2016 State Preparedness Report submissions, only 21 percent of states and territories reported proficiency in their Housing capability ratings, the third lowest among all core capabilities. Moreover, 59 percent of states and territories reported that they perceive it to be primarily the responsibility of the Federal Government to address gaps in the Housing core capability. In August 2016, torrential rains in Louisiana caused the flooding of more than 100,000 homes, resulting in significant demand for Federal housing assistance. As of December 2016:

- *FEMA provided more than $745 million to survivors through its Individuals and Households Program, which provides grants that eligible individuals can use to support repair or replacement of their homes, temporary rentals, and other disaster-related expenses.*
- *SBA approved over 15,000 home loans—totaling approximately $1 billion—that disaster survivors can use to replace or rebuild their primary residence.*
- *The USDA Multi-Family Housing program identified 700 available apartments in rural regions across the state to address the housing needs of disaster survivors in rural areas.*

Mission Area Connections

Recovery

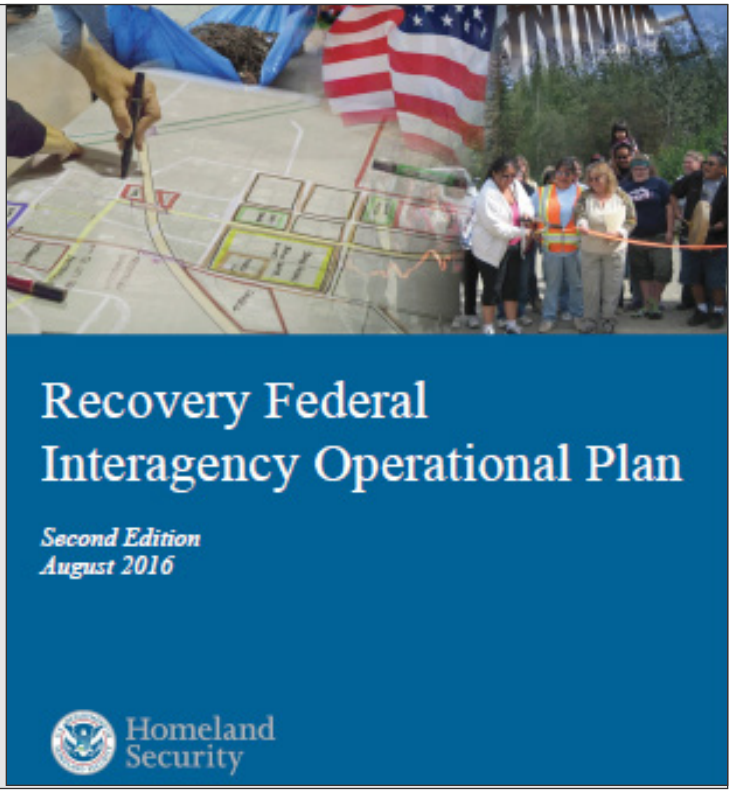
Mitigation

Floodplain Management and Housing

Following a disaster, relocating or rebuilding outside of floodplains can enhance a community's flood resilience. However, balancing long-term vulnerability reduction while meeting the permanent housing needs of disaster survivors continues to be a challenge. As 2016 flooding disasters demonstrated, individuals and families may prefer to rebuild in their current locations due to the difficulties in relocating or rebuilding elsewhere.

Recovery Case Study: Sustainability Advisor

The Federal Government officially introduced the position of "Sustainability Advisor" in the 2016 update to the *Recovery Federal Interagency Operational Plan*. The Sustainability Advisor advocates for and guides Federal, state, and local partners in adopting sustainable, green, and resilient principles and practices in recovery operations. Following 2016 flooding in Louisiana, EPA deployed a Sustainability Advisor for the first time. In Louisiana, the Sustainability Advisor is working with FEMA to integrate opportunities to advance sustainable development, mitigation planning, and long-term disaster recovery by leveraging financial and technical resources to support regional and local needs, such as green infrastructure, ecosystem assessment, and grant writing. Additionally, the Sustainability Advisor is partnering with other Federal, state, and local partners to increase education and outreach efforts that promote the incorporation of sustainability practices into land use decisions, housing alternatives, and capacity building efforts.



In addition, the flooding led to one of the largest mobilizations in history of FEMA manufactured housing units (second only to Hurricane Katrina), with over 3,000 manufactured housing units in Louisiana as of December 2016. Some are upgraded units that adhere to strict HUD safety standards and feature an innovative sprinkler system to address the risk of fire. In addition, upgraded units are available for eligible disaster survivors with disabilities or other access and functional needs that include improved accessibility features, in accordance with the Uniform Federal Accessibility Standards. Survivors unable to identify other means of housing may depend on manufactured housing units as an alternative temporary housing option.

However, the experiences of displaced residents following the August flooding in Louisiana, as well as other flooding events in 2016, highlighted several challenges in identifying housing solutions:

- ***Assistance for Renters:*** *Although FEMA provides eligible survivors with temporary rental assistance, this benefit can be difficult for survivors to use in rental markets with low availability. Renters within flood-impacted areas faced limited short-term or long-term housing options—with waitlists for apartments as long as five years—due to a rental market still stretched from March flooding. Survivors often preferred to remain in their neighborhoods and school districts, narrowing the pool of practical rental options. To assist with this challenge, the Federal Government increased the amount of rental assistance available to survivors in designated parishes by 25 percent. This increase widened the pool of options that were affordable to survivors who required temporary housing.*

- ***Manufactured Housing Units:*** *Following 2016 floods in Louisiana, FEMA made over 3,000 manufactured housing units available, and individuals and families had occupied approximately 2,500 of these by December 2016. However, FEMA projected that more than 4,000 units were necessary to address needs in Louisiana. Additionally, delivery and installation of these units can be logistically challenging. Understanding these issues, FEMA worked in 2016 to prioritize and improve production efficiency for manufactured housing units.*

- ***Homeowner Verification:*** *Following a disaster, homeowners' absence of paperwork providing proof of ownership (e.g., deed or title) can complicate the receipt of disaster assistance. While much improved since 2005 (i.e., Hurricane Katrina), in the aftermath of the Louisiana flooding, some families whose homes had been passed down from generation to generation were unable to produce the required paperwork to verify home ownership. While FEMA is typically able to work with eligible individuals to identify acceptable alternatives to verify their ownership, these additional steps can complicate a disaster survivor's ability to navigate the FEMA assistance process.*

- ***Rebuilding in Floodplains:*** *Immediately following disasters, homeowners without flood insurance may not have the resources to move or hire contractors, and often complete repairs on their own. Even if owners receive funding assistance, they may have already taken on debt with repairs, motivating them to remain in their homes. Additionally, survivors may often prefer to stay in their current communities and school districts.*

- ***Accessible Housing Options:*** *Prolonged shelter operations following the Louisiana floods highlighted the lack of housing options available and appropriate for individuals with disabilities. Additionally, destroyed or damaged vehicles belonging to these individuals now meant that most would have to rely on public transportation in the interim or permanently, precluding them from housing options in remote geographic areas. Moreover, survivors with disabilities often need to stay in close proximity to their established support system, which further limited the pool of available accessible housing options.*

Recovery Case Study: Sevier County and mountaintough.org

In late 2016, a series of wildfires devastated Sevier County, Tennessee. To assist with recovery efforts, Sevier County and its cities created mountaintough.org, a website that links survivors to resources such as food and supplies, job opportunities, and information on applying for disaster assistance. To address housing needs, mountaintough.org includes a form to help survivors identify housing opportunities. The form asks for details such as preferred monthly rent and number of residents to strategically match applicants with appropriate options. Property owners can also fill out a separate form to list any units available for rent.

Key Finding:

Federal departments and agencies are implementing corrective actions to address persistent challenges to core capabilities in the Recovery mission area.

Each year, the *National Preparedness Report* identifies core capabilities that are in need of improvement, requiring sustained attention from leadership and the Nation to address persistent challenges. In the Recovery mission area, previous *National Preparedness Reports* have repeatedly identified five core capabilities as areas for improvement: Economic Recovery, Health and Social Services, Housing, Infrastructure Systems, and Natural and Cultural Resources (see Table 8).

Table 8. Each edition of the *National Preparedness Report* has identified Recovery core capabilities as national areas for improvement.

Core Capability	2012	2013	2014	2015	2016	2017
Economic Recovery	•	•		•	•	•
Health and Social Services	•	•	•			
Housing	•	•	•	•	•	•
Infrastructure Systems	•	•	•	•	•	•
Natural and Cultural Resources	•	•			•	•

In 2016, Federal departments and agencies with responsibilities under these core capabilities took a number of actions to address identified challenges:

- ***Economic Recovery:*** *Previous* National Preparedness Reports *have identified that economic development professionals and emergency managers often struggle to communicate effectively and share information, which can impede efforts toward economic recovery. To address these challenges, FEMA launched a compendium of resources on* DisasterAssistance.gov *to make post-disaster recovery information easily accessible to both disaster survivors and community leaders, including economic development and emergency management professionals. In addition, each U.S. Economic Development Administration (EDA) regional office is conducting outreach to regional partners involved in economic recovery, with the goal of establishing Economic Recovery Support Function Regional Working Groups. The objective of these groups is to build regional capability by helping states identify resources, as well as promoting collaboration and information sharing among stakeholders.*
- ***Health and Social Services:*** *Recent studies and real-world events suggest that stakeholders can better integrate health considerations into plans and collaborate more effectively to meet the needs of survivors following disasters. To meet*

increasing demands for Federal engagement on Health and Social Services post-disaster, ASPR plans to cross-train staff to support field recovery operations. ASPR continues to update recovery planning resources on its website and through its Technical Resources, Assistance Center, and Information Exchange, a healthcare emergency preparedness information gateway, consisting of three complementary domains (i.e., Technical Resources, Assistance Center, and Information Exchange), that ensures the whole community has access to information and resources to improve preparedness efforts. In addition, the National Institutes of Health (NIH) Disaster Research Response (DR2) Program, led by the National Institute of Environmental Health Sciences, is an available resource for all state, local, and municipal health departments, as well as all academia and others interested in performing timely health data collection and vital research in response to disasters. The open access protocols and tools are available on the National Library of Medicine NIH DR2 website. CDC is currently using the DR2 resources to help with disaster preparedness and training for local and state health departments through organizations such as the Council for State and Territorial Epidemiologists.

- ***Housing:*** *Persistent challenges remain in identifying successful strategies to restore permanent or long-term housing for communities after disasters, including affordable and accessible housing. To address these issues—as well the lack of comprehensive, updated housing doctrine—HUD and FEMA developed and plan to release the* Housing Recovery Support Function Concept of Operations*. The update comprehensively addresses housing issues ranging from emergency sheltering through permanent housing. With a focus on populations who may be disproportionately impacted by a disaster, HUD also released a toolkit in 2016 that helps recovery stakeholders better consider homeless individuals in pre-disaster planning, response, and long-term recovery. The toolkit includes a "Recovery Action Plan," with strategies for finding transitional or permanent housing solutions for individuals experiencing homelessness after a disaster.*
- ***Infrastructure Systems:*** *Public- and private-sector partners continue to focus on improving infrastructure systems to address vulnerabilities posed by deteriorating critical infrastructure. To facilitate information access and sharing, the National Institute of Standards and Technology's Community Resilience Standards Panel—with cooperation from other Federal partners—created a new section on the "U.S. Climate Resilience Toolkit" website. The new section includes resource compendiums for topics ranging from wastewater and energy systems to disaster planning and social equity. The portal allows easy access to resources that can help communities strengthen their infrastructure resilience. Additionally, DHS is conducting a phased rollout of the Infrastructure Development and Recovery program, an initiative to support the critical infrastructure community with planning expertise, resources, technical assistance, and subject-matter expertise on critical infrastructure protection and recovery. The Infrastructure Development and Recovery program applies a holistic approach to strengthening security and resilience that incorporates resilient strategies, policies, and best practices and informs planning, design, construction, and day-to-day operations of critical infrastructure. DHS piloted the program with local jurisdictions in Alabama, California, and Colorado in December 2016. FEMA is also piloting a new model for reviewing and validating Public Assistance grant applications (see page 92 for additional details).*
- ***Natural and Cultural Resources:*** *While the Natural and Cultural Resources core capability has potentially significant ramifications for disaster recovery—particularly for communities whose economies depend on natural resources—many states and territories do not consider it a priority (see page 14). To bring greater attention to this capability, the National Endowment for the Humanities provided grant funding to organizations such as the Foundation of the American Institute for Conservation of Historic and Artistic Works (FAIC), the Museum of Fine Arts, Houston, and the Bureau of Indian Affairs to launch new forums and webinars in 2016 to provide training and guidance to emergency managers and cultural resources partners. In the FAIC webinar series, for example, cultural-heritage experts shared best practices for topics such as organizing disaster assistance networks, integrating volunteers into recovery efforts, and developing tabletop exercises for training.*

2016 Federal Interagency Recovery Readiness Assessment

The Recovery Support Function Leadership Group (RSFLG) is the senior-level entity that coordinates responsibilities and resolves operational, resource, and preparedness issues relating to interagency recovery activities at the national level. In 2015, the RSFLG created and implemented the Federal Interagency Recovery Readiness Assessment to assess the Federal Government's readiness to support state, local, tribal, and territorial communities in their recovery from disasters and improve resiliency for future incidents. In 2016, the RSFLG refined and reapplied the methodology for this assessment to determine how departments and agencies could perform during multiple, simultaneous, and very large events. Within this scenario, over 25 departments and agencies evaluated their capacity to support recovery efforts, as measured by over 600 Recovery support statements detailing Federal programs or actions implemented during recovery efforts.

During 2016, RSFLG member departments and agencies reflected on experiences since the original publication of the NDRF in 2011 and self-assessed their ability to provide the services, resources, or other support outlined in each support statement. Early analysis of the resulting data indicates that support statements were rated "Perform without challenges" 11 percent of the time (designated "P" in Figure 13) and "Perform with some challenges" 55 percent of the time (designated "S"). Further analysis is underway to identify the causes for ratings of "Perform with major challenges" or "Unable to perform" (designated "M" and "U," respectively). This additional analysis should also reveal how significant the reductions in performance are, including in the "Perform with some challenges" category.

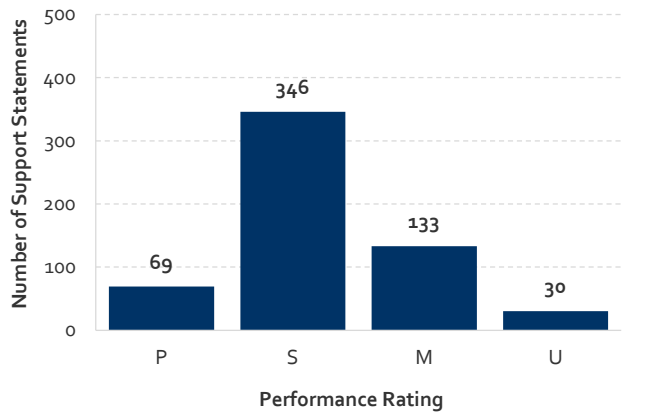


Figure 13. Departments and agencies provided self-assessed performance ratings for Recovery support statements.

In the self-assessment, Federal departments and agencies most frequently identified "personnel" and "financial" causes behind the challenges inhibiting performance (see Figure 14). For example, personnel constraints may lead some Federal departments and agencies to assign disaster recovery responsibilities as an "additional duty," which can conflict with staff members' primary duties and lead to less support for recovery activities both pre- and post-incident. For other Federal departments and agencies, however, establishing a dedicated recovery cadre may present a financial challenge, as costs associated with developing and maintaining such a cadre are prohibitively large and untenable. Ongoing analysis efforts of the 2016 readiness assessment data, as well as future assessments, will seek to better understand the relationship between these challenges and the appropriateness of possible solutions for individual Federal departments and agencies.

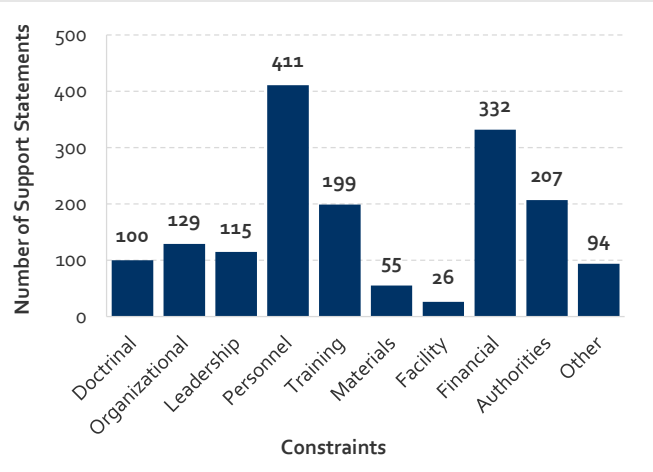


Figure 14. Federal departments and agencies identified one or more constraints inhibiting their performance in Recovery support statements.

Key Finding:

FEMA is applying new methods to provide public assistance for the reimbursement of debris removal, emergency protective measures, and infrastructure projects.

FEMA's Public Assistance Program provides grants to states, tribes, and territories for debris removal, emergency protective measures, and the repair and replacement of public facilities such as roads and bridges following a presidential disaster declaration. Public Assistance Program distributions account for slightly more than half of all FEMA grants and have provided an average of $4.7 billion in disaster assistance annually over the past 10 years. While the program has played an important role in helping communities recover from disasters, a number of challenges in the grant process have hampered the program's timeliness and efficacy.

Jurisdictions seeking support from the Public Assistance Program to support a recovery project must submit an application to FEMA. Historically, FEMA has reviewed and validated the applications without regard to a project's size and complexity, or the changing needs of affected communities. This has resulted in inconsistent and long processing times from application to initial obligation of funds. Moreover, issues arose related to thoroughly reviewing projects, as well as clearly communicating to applicants their eligibility status. This has resulted in instances where applicants funded projects they believed were eligible, only to face a de-obligation of funds or a lack of reimbursement.

To address these challenges, FEMA is piloting a new model for reviewing and validating Public Assistance grant applications. FEMA designed the new model to help affected communities receive funding more quickly by categorizing projects and processing applications according to cost and complexity. This can help prevent large, complex projects from delaying the processing of grants for smaller or already completed projects, which FEMA could otherwise quickly process to speed community recovery. FEMA also developed new positions staffed with subject-matter experts to perform more specialized roles in order to increase consistency during all phases of the application process. Finally, to improve accountability, information sharing, and communication with applicants, the model includes a new web-based tracking system that applicants can use to view and upload required project documentation and track the status of their project applications.

FEMA tested the new delivery model following a late 2015 flooding disaster in Iowa, as well as in 2016 flooding events in Oregon and Georgia. These tests revealed a number of strengths and challenges related to the new delivery model. For example, FEMA found that the new process promoted consistency throughout the grant process. However, both FEMA staff members and applicants reported having insufficient understanding of the new process, as well as many of the tools developed to document damage, work, and costs. Additionally, in Oregon, FEMA had difficulty determining the staffing levels required to implement the new model. FEMA is using the lessons learned from these pilot tests to further update the processes and project-tracking system tools, and FEMA will continuously assess and modify both as needed during future pilots. FEMA is also working to train Public Assistance staff, FEMA Regions, states, and applicants on the new model and its requirements before implementing it nationally.

Ongoing Challenges

Conclusion

While *National Preparedness Reports* (of which this is the sixth) describe numerous actions taken to increase national preparedness, they also identify persistent or emerging issues that hinder progress. This section highlights examples of such issues in each of the five mission areas. No easy solutions exist for addressing these complex, national challenges. Instead, each requires innovative ideas and sustained efforts from all preparedness stakeholders to achieve meaningful improvements.

Prevention

Challenge:

Collecting information in an environment of increasingly encrypted communications

The expansion of platforms for encrypted communications, through which terrorists can avoid legal efforts to access and monitor their communications, complicates the IC's ability to prevent and investigate terrorist actions. While encryption services have been available for some time, the seamless integration and default enabling of them on popular devices (e.g., mobile phones) have simplified and facilitated the use of encrypted communications. This change has had the unintended effect of limiting access to a potentially valuable source of intelligence to uncover and interdict terrorist plots. However, weakening encryption so that communications can be readily intercepted increases the cyber risks presented by hackers, criminals, and espionage. More broadly, encrypted communications touch on the conflicting demands for security, privacy, economic competitiveness, and government access to information. Increased engagement between the IC and private-sector companies may provide alternatives to help resolve these conflicting demands.

Challenge:

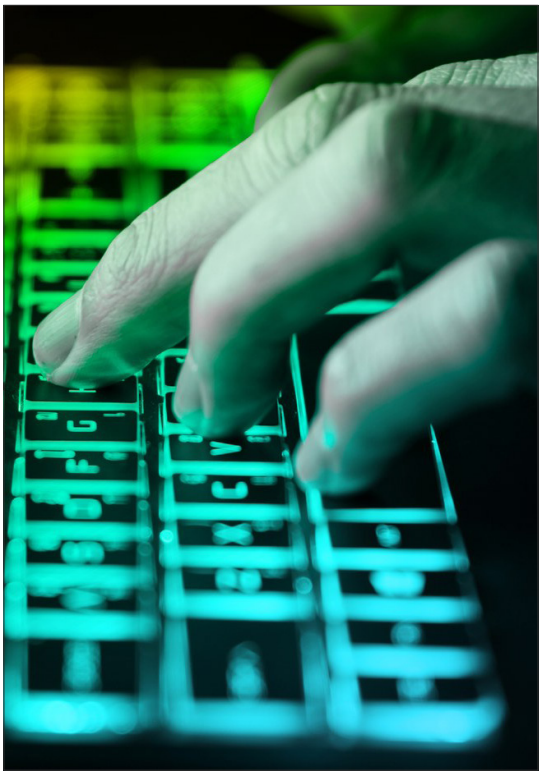
Detecting and preventing attacks by homegrown violent extremists

Detecting and interdicting plots by homegrown violent extremists (i.e., individuals inspired by foreign terrorist organizations based and primarily radicalized to violence in the United States whose actions are not directed by a foreign terrorist organization) is one of the most difficult challenges law enforcement and intelligence agencies face. Although attacks by this type of individual are historically rare (fewer than 100 such attacks have occurred in the United States since the 1940s), these attacks are becoming increasingly common and deadly. The current decade has already surpassed each prior decade since the 1940s in both the numbers of attacks perpetrated and associated fatalities. Moreover, the June 2016 Orlando Pulse nightclub shooting, which was committed by a homegrown violent extremist, was the deadliest shooting in U.S. history. Homegrown violent extremists are less likely to draw the attention of authorities because their radicalization to violence and planning may be observable only by family or associates who may be hesitant to inform law enforcement, which decreases the likelihood that their terrorist plot will be discovered by law enforcement. Additionally, the growing prevalence of terrorist messaging online increases the number of avenues through which individuals could become radicalized to violence and decide to launch independent attacks. To help prevent radicalization to violence, the Federal Government and private-sector partners have engaged in efforts such as educational outreach, counter-narrative messaging, and suspension of terrorist-linked social media accounts (see page 39 for additional details).

Protection

Challenge:

Securing increasingly interconnected systems from cyber attack



An increasingly connected set of systems and devices, often called the "Internet of Things," controls or monitors everything, from Wi-Fi–enabled home thermostats to industrial control systems in critical infrastructure facilities. Greater connectivity increases efficiency and convenience, but it also increases potential vectors of attack for malicious cyber actors. This expansion in the number of avenues for malicious cyber activity has the potential to degrade the Nation's capacity to protect (and, if need be, restore) electronic communication, information, and service systems. For example, the 2013 hack into Target's payment systems may have originated with a heating, ventilation, and air conditioning vendor who had remote access to Internet-connected devices to monitor temperatures inside stores. More recently, a DDoS attack in October 2016 widely affected Internet access across multiple areas of the United States (see page 9). As more devices are connected every day (one technology research firm estimated a 30-percent growth in Internet-connected devices from 2015 to 2016, up to 6.4 billion devices worldwide), securing individual systems and entire networks will only grow in complexity. In November 2016, DHS released *Strategic Principles for Securing the Internet of Things (IoT)*, which explains the risks presented by the growth in interconnected devices and systems, as well as provides principles and best practices to help ensure their security.

Challenge:

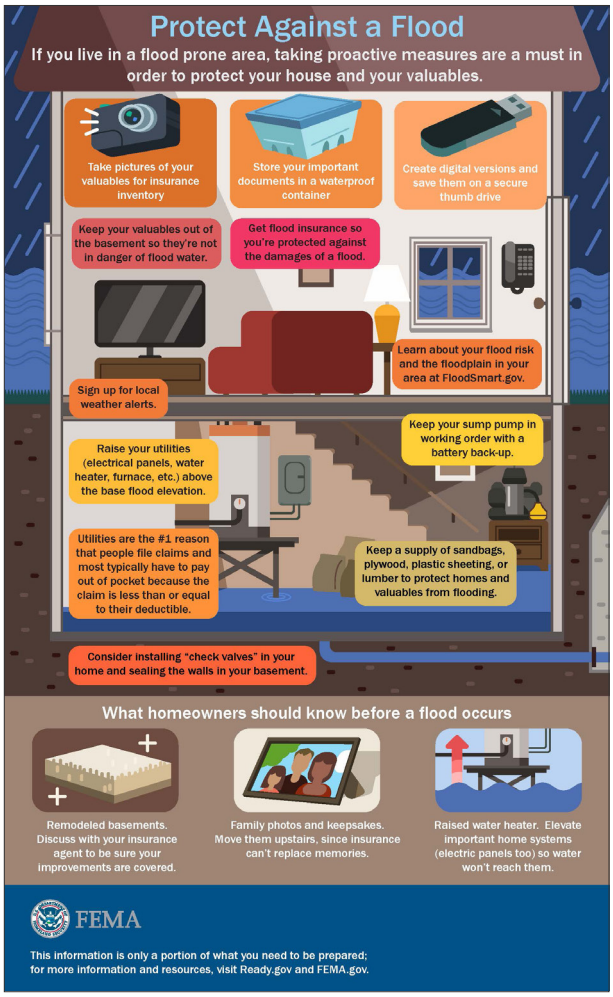
Balancing competing demands between increasing security and minimizing disruptions to travel and commerce

The global movement of people and goods continues to place burdens on balancing steady-state protective operations such as screening, search, and detection operations against minimizing disruptions to travelers and businesses. Over the previous decade, international air travel (measured by distance flown) has grown at an average annual rate of 5.5 percent. As of 2016, TSA screens approximately two million passengers, 4.9 million carry-on items, and 1.3 million checked bags every day. Keeping pace with demand while screening travelers remains a persistent challenge, as exemplified by a springtime surge in airport security wait times in large airports like New York's JFK and concerns over summer delays, and the subsequent expedited hiring of more than 700 TSA officers in May 2016. U.S. seaports handled more than 12.2 million cargo containers in fiscal year 2016 and have experienced a nearly 14 percent increase in units of cargo over the last five years. CBP has taken steps to improve screening efficiency (see page 43). With international travel and commerce increasing, Federal agencies will likely engage in a continual search for ways to help relieve the resulting pressure on screening efforts while maintaining security.

Mitigation

Challenge:

Inspiring individuals to prepare for emergencies



Motivating and empowering individuals to take action prior to an incident is a fundamental pillar for mitigating potential consequences. Through public campaigns such as Ready and America's PrepareAthon!, DHS endeavors to educate individuals on how to prepare for disasters. This includes providing services and auxiliary aids for persons with disabilities and others with access and functional needs, including persons with limited English proficiency. However, increasing the overall level of individual preparedness nationwide proves challenging, as such cultural and behavioral changes require sustained, long-term efforts from the whole community. Although annual National Household Surveys show rising trends in many areas (e.g., having and discussing emergency plans or having supplies), the surveys also identify specific challenges (e.g., variation in awareness by hazard or specific populations) and indicate that the overall level of national preparedness remains low. The varying level of community preparedness education and/or awareness serves as a contributing factor to low levels of national preparedness. For example, in the *2015 National Household Survey*, FEMA reported that only 34 percent of individuals living in areas with a history of flooding reported having read, seen, or heard information on how to better prepare for a flood. Despite such challenges, results from the same survey reaffirm the positive connection between awareness and taking action. To increase awareness and promote action, Federal agencies and community partners target accessible preparedness messages to whole communities, to include underserved populations, and tie these messages to notable events and popular cultural icons. In addition, stakeholders engage in outreach through websites and social media and support and/or participate in programs that promote awareness and action.

Challenge:

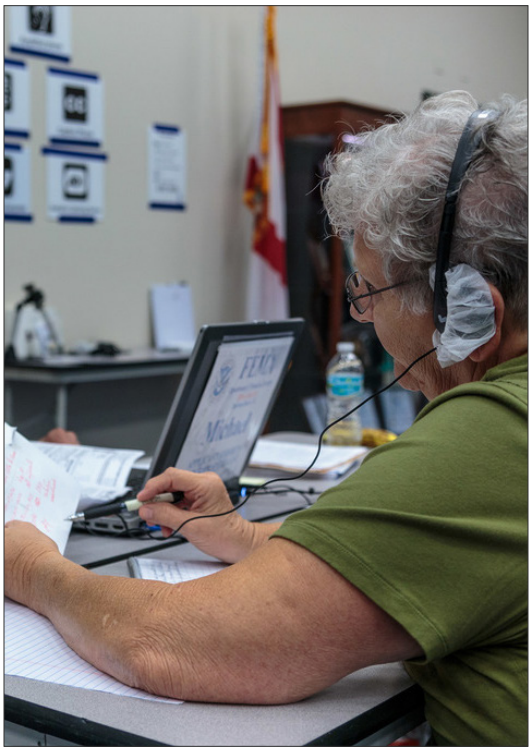
Advancing and communicating cost-benefit analyses to support mitigation decisions

After a disaster, a key component of effective mitigation is the strengthening of resilience against future hazards during rebuilding efforts. Traditionally, FEMA and local governments have examined data on past disasters to project the risk of future disasters and determine whether rebuilding stronger is a worthwhile investment. However, as mitigation stakeholders continue to note, historical meteorological data have not been a good indicator of the growing risk from more frequently occurring natural disasters. In addition, the available data to support cost-benefit analyses are often inconclusive or missing altogether. According to GAO, the lack of comprehensive and reliable data for these analyses may inhibit local governments from investing in mitigation activities. Federal and state stakeholders may be able to improve their cost-benefit analyses and implement better risk management strategies by partnering with private insurance companies, which specialize in identifying, analyzing, and modeling risks.

Response

Challenge:

Ensuring that disaster survivors with disabilities and others with access and functional needs receive equal access to response services



During Hurricane Katrina, many survivors with disabilities and others with access and functional needs experienced difficulties in accessing emergency services, or were stranded while waiting for evacuation assistance or refused shelter by unprepared organizations. Persons with disabilities and others with access and functional needs subsequently experienced a disproportionately high number of fatalities after that hurricane. Since then, emergency managers at all levels of government have placed a greater focus on integrating individuals with disabilities and others with access and functional needs in response efforts. For example, FEMA established the Office of Disability Integration and Coordination in 2010 and added a Disability Integration Advisor position to its deployable disaster workforce in 2012. Challenges remain, however, in providing services for all affected populations during and after a disaster. In 2016, FEMA's National Advisory Council noted that jurisdictions still had limited operational guidance and training on how to incorporate considerations from the *Americans with Disabilities Act* into their emergency management activities. Federal agencies also described difficulty reaching individuals with disabilities and others with access and functional needs with actionable messaging delivered in an accessible format during a disaster. In August 2016, DOJ, HHS, HUD, DHS, and DOT issued joint guidance to ensure that recipients of Federal financial assistance comply with Title VI of the Civil Rights Act of 1964 and not discriminate against individuals on the basis of race, color, or national origin—including those with limited English proficiency—when providing emergency preparedness, response, and recovery services.

Challenge:

Improving responder capacity and coordination in catastrophic events

Despite progress in preparing for an unprecedented catastrophic event, the Nation remains underprepared to respond to an incident on the scale of a catastrophic earthquake in the Cascadia Subduction Zone or the New Madrid Seismic Zone. Unlike other incidents, these scenarios will likely break existing mechanisms and networks that emergency management employs, with projected consequences (e.g., tens of thousands of survivors requiring immediate medical attention, millions requiring emergency shelter) overwhelming official response and recovery measures for an extended period of time. An after-action report on Cascadia Rising 2016/Ardent Sentry 2016 (see page 71) found that the Nation lacked the capacity to fully respond to an incident of this magnitude, which would present complexities and challenges such as simultaneous requests for limited resources (e.g., access to water) and novel communications and transportation challenges, as well as require adaptive solutions to address life-saving needs. One area that emergency planners at all levels of government have struggled with is incorporating survivors, grassroots organizations, and the general public into response efforts. Historically, these groups have been decisive stabilizing factors in the aftermath of every disaster—even catastrophes—by augmenting response capability (e.g., search and rescue, first aid, radio communications) and serving as important sources for creative and unconventional solutions that catastrophic incidents require. By continuing to promote a culture that empowers these groups, emergency managers can develop additional, much-needed capacity to better address catastrophic events.

Recovery

Challenge:

Comprehensively addressing the housing needs of disaster survivors

Previous *National Preparedness Reports* have cited longstanding issues that impede progress concerning the housing needs of disaster survivors, including accessible and affordable housing. For example, many states and territories expect the Federal Government to take on the responsibility of addressing housing gaps, as states often face gaps in capabilities for housing operations following a large-scale disaster. Resource and logistics challenges in large-scale events may stress Federal capacity as well. Federal agencies also face challenges coordinating their efforts across different phases of housing support (from short-term to long-term housing). Because housing options are constrained by legal, administrative, and logistical requirements, the availability of possible housing solutions is sensitive to decisions made early on in a disaster. HUD is implementing a portal for information access and sharing of FEMA Individual Assistance information to expedite delivery of recovery assistance. It also plans to release the *Housing Recovery Support Function Concept of Operations*, which will address Federal coordination of a variety of housing issues from emergency sheltering to permanent housing.

Challenge:

Developing comprehensive pre-disaster plans to support post-disaster recovery efforts

Under the NDRF, pre-disaster recovery planning provides an opportunity for communities to develop partnerships at all levels of government, establish goals, identify essential resources, and accelerate recovery after a disaster. However, as highlighted in prior *National Preparedness Reports*, strengthened participation from key stakeholders in pre-disaster recovery planning is necessary. For example, a 2015 report from the Institute of Medicine, funded by ASPR, HUD, and the Robert Wood Johnson Foundation, affirms the importance of pre-disaster planning that proactively links emergency management and health leadership at the community level. Moreover, insufficient inclusion of economic development experts in pre-disaster planning continues to hinder post-disaster economic recovery efforts and suggests a similar disconnect between the emergency preparedness community and local economic-development experts. To improve coordination and capabilities for economic recovery efforts, EDA and FEMA are developing training opportunities that bring together officials, emergency managers, and economic development specialists, including the private sector. The EDA is also creating regional working groups with the goal of strengthening planning and information sharing among economic recovery partners across the public and private sectors.

Acronym List

Appendix A

ACF	Administration for Children and Families, U.S. Department of Health and Human Services
AOC	Airport Operations Center
ASPR	Office of the Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services
BARDA	Biomedical Advanced Research and Development Authority
BSIR	Biannual Strategy Implementation Report
C2M2	Cybersecurity Capability Maturity Model, U.S. Department of Energy
CAUSE	Canada-United States Enhanced (Resiliency experiment)
CBP	U.S. Customs and Border Protection, U.S. Department of Homeland Security
CDC	Centers for Disease Control and Prevention, U.S. Department of Health and Human Services
COPS	Community Oriented Policing Services
CSI	Container Security Initiative
CVE	Countering violent extremism
DARPA	Defense Advanced Research Projects Agency, U.S. Department of Defense
DDoS	Distributed denial of service
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office, U.S. Department of Homeland Security
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
DR2	Disaster Research Response (Program), National Institutes of Health
E.O.	Executive Order
EDA	U.S. Economic Development Administration
EPA	U.S. Environmental Protection Agency
FAIC	Foundation of the American Institute for Conservation of Historic and Artistic Works
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	U.S. Food and Drug Administration
FEMA	Federal Emergency Management Agency
FESAP	Federal Experts Security Advisory Panel
FIOP	Federal Interagency Operational Plan
FirstNet	First Responder Network Authority
GAO	U.S. Government Accountability Office

GIS	Geographic information system
GPS	Global positioning system
HHS	U.S. Department of Health and Human Services
HPP	Hospital Preparedness Program
HRSA	Health Resources and Services Administration, U.S. Department of Health and Human Services
HSIN	Homeland Security Information Network
HUD	U.S. Department of Housing and Urban Development
I&A	Office of Intelligence and Analysis, U.S. Department of Homeland Security
IBHS	Insurance Institute for Business and Home Safety
IC	Intelligence Community
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IED	Improvised explosive device
IIR	Intelligence Information Report
IP	Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security
IPAWS	Integrated Public Alert Warning System
IT	Information technology
JTTF	Joint Terrorism Task Force
MDS	Mennonite Disaster Service
MOU	Memorandum of understanding
NASA	National Aeronautics and Space Administration
NBIB	National Background Investigations Bureau
NCTC	National Counterterorrism Center
NDRF	National Disaster Recovery Framework
NDRP	National Drought Resilience Partnership
NEP	National Exercise Program
NFIP	National Flood Insurance Program
NGS	National Geodetic Survey, National Oceanic and Atmospheric Administration
NIH	National Institutes of Health, U.S. Department of Health and Human Services
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPSBN	Nationwide Public Safety Broadband Network
NRC	Nuclear Regulatory Commission
NRCS	Natural Resources Conservation Service, U.S. Department of Agriculture
NSA	National Security Agency
OBP	Office for Bombing Prevention, U.S. Department of Homeland Security
ODNI	Office of the Director of National Intelligence
OEC	Office of Emergency Communications, U.S. Department of Homeland Security
OIG	Office of Inspector General
OPM	U.S. Office of Personnel Management
PI-WMP	Pre-Incident Waste Management Plan

PII	Personally identifiable information
POETE	Planning, organization, equipment, training, exercises
PPD	Presidential Policy Directive
PSA	Public service announcement
PSAP	Public safety answering point
RSFLG	Recovery Support Function Leadership Group
SBA	U.S. Small Business Administration
SNS	Strategic National Stockpile
SWAT	Special Weapons and Tactics
TSA	Transportation Security Administration, U.S. Department of Homeland Security
TSC	Terrorist Screening Center
USACE	U.S. Army Corps of Engineers, U.S. Department of Defense
USBR	Bureau of Reclamation, U.S. Department of the Interior
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
USFS	U.S. Forest Service, U.S. Department of Agriculture
USGS	U.S. Geological Survey, U.S. Department of the Interior
VOAD	Voluntary Organizations Active in Disaster
WFRL	Wildland Fire Resilient Landscapes
WMD	Weapon of mass destruction
WYO	Write Your Own program, National Flood Insurance Program
Z-CART	Zika Community Action Response Toolkit

Research Approach

Appendix B

The Federal Emergency Management Agency (FEMA) coordinates the development of the *National Preparedness Report*. To ensure a comprehensive report that reflects progress and challenges occurring nationwide, FEMA takes several actions to collect, analyze, and present information from numerous sources, including:

- *Applying a criteria-based approach in analyzing preparedness assessments, exercises, funding, and long-term trends influencing preparedness to identify national areas for improvement and capabilities to sustain among the 32 core capabilities;*
- *Analyzing 2016 Threat and Hazard Identification and Risk Assessments from 113 states, territories, tribes, and urban areas, as well as 2016 State Preparedness Report submissions from all 56 states and territories, in order to identify national shifts in the threats and hazards that jurisdictions are using to drive their capability requirements, to compare relative performance among all capabilities, and to identify performance trends over time;*
- *Conducting a data call with Federal departments and agencies to solicit their input and identify national preparedness accomplishments and related challenges;*
- *Completing a literature review of open-source material from all levels of government, academia, professional organizations, and the private sector for information on notable progress and challenges related to the 32 core capabilities identified in the Goal;*
- *Coordinating outreach with professional organizations and other non-Federal partners to obtain information, solicit perspectives on preparedness, and identify example case studies;*
- *Examining exercises and real-world events occurring or reported in 2016 to identify preparedness outcomes and lessons learned; and*
- *Engaging Federal departments, agencies, and senior interagency coordination groups to review and supplement report content.*

What is the 2016 Threat and Hazard Identification and Risk Assessment and State Preparedness Report?

The 2017 *National Preparedness Report* includes results from the integrated 2016 Threat and Hazard Identification and Risk Assessment and State Preparedness Report. These programs support the National Preparedness System by helping states, territories, tribes, and urban areas annually assess their preparedness capabilities and identify capability gaps. Jurisdictions use the Threat and Hazard Identification and Risk Assessment process to determine threats and hazards of primary concern, establish capability targets, and analyze the resources required to address anticipated risks. Next, states and territories assess their current capability levels against their assessment targets in the State Preparedness Report. States, territories, and the Federal Government use this information to support decisions to build, validate, deliver, and sustain core capabilities. The Federal Government also uses the results to guide strategic direction for programs that help close preparedness capability gaps.

These activities provided a wide range of sources and insights, as well as a broader perspective on preparedness. In total, the 2017 *National Preparedness Report* reflects input from more than 600 data sources. Since preparedness is the shared responsibility of the entire Nation, FEMA solicited input not only from 124 Federal agencies, but also 29 non-Federal partners. In particular, non-Federal partners contributed to the report in numerous ways, playing prominent roles in a number of preparedness initiatives; issuing the results of various topically relevant assessments, reports, and surveys; and sponsoring conferences and workshops that address preparedness issues.

Sources

FEMA compiled the 2017 *National Preparedness Report* using a combination of qualitative and quantitative preparedness data and contributions from multiple sources.

By the Numbers

167	124	600+	113	29
Inputs Recieved from Formal Data Call	Federal Offices Engaged	Data Sources Referenced	Threat and Hazard Identification and Risk Assessment and State Preparedness Report Submissions	Non-Federal Stakeholders Engaged

Non-Federal Community Engagement Included:

- American Society for the Prevention of Cruelty to Animals
- Blue Forest Conservation
- Center for Internet Security
- Iowa Legal Aid
- National Academy of Sciences
- Washington State Military Department
- Other Private-sector Partners

The majority of the 2017 *National Preparedness Report* consists of key findings that assess specific areas of national preparedness. Key findings draw on both quantitative and qualitative sources to document relevant advancements and challenges. Five criteria helped identify key findings from the data sources and inputs:

- ***Advancements in or challenges to preparedness programs:*** *Whether major initiatives saw progress or difficulties that affected preparedness or resilience nationwide*
- ***Consequential increases or decreases in resources:*** *The extent to which increases or decreases in resources—such as funding and personnel—meaningfully affected building, sustaining, or delivering a core capability*
- ***Broad impact across the public and private sector:*** *Whether preparedness activities or assessments addressed multiple levels of government and non-Federal partners, including performance in real-world incidents*
- ***Significant increases or decreases in capability:*** *The extent to which quantitative data demonstrated increases or decreases in a preparedness capability over time, as well as the underlying drivers for these changes*
- ***Relevance to national priorities:*** *Whether an activity demonstrated progress in establishing or implementing national-level strategies and policies that set priorities for improving capability performance*

For inclusion in the 2017 *National Preparedness Report*, key findings had to satisfy at least two of these five criteria.

9/11 Retrospective

Appendix C

With 2016 marking the 15-year anniversary of the 9/11 tragedy, the 2017 *National Preparedness Report* presents this case study as a means of reflecting on ways the Nation has restructured and retooled its preparedness efforts following 9/11. In the wake of 9/11, Congress and the President established a bipartisan commission to investigate the facts and circumstances surrounding the attacks. In *The 9/11 Commission Report*, published in 2004, commission members identified 41 recommendations to guard against future attacks. This case study highlights some of the Commission's recommendations, noting where the Nation has made substantial progress, as well as where some recommendations remain unfulfilled.

Achieving Greater Unity of Effort

Several of the Commission's recommendations called out the fragmented nature of homeland security efforts at the time of the attacks. For example, commission members determined that structural barriers and concerns about security led to excessive over-classification and compartmentalization of information among agencies, making it impossible for the Intelligence Community to piece together relevant information to uncover and prevent the attacks. They recommended encouraging information sharing to address the observed imbalance between security and shared knowledge.

Since 9/11, various nationwide efforts have enhanced information sharing among Federal, state, and local law enforcement, and the private sector:

- *The Federal Bureau of Investigation (FBI) increased the number of Joint Terrorism Task Forces (JTTFs), which conduct counterterrorism investigations, from 35 in 2001 to more than 100 today. While FBI-led, these task forces integrate other Federal, state, local, tribal, and territorial law enforcement partners and inform intelligence products shared with law enforcement and homeland security agencies.*
- *The Terrorist Screening Center (TSC), created in 2003, consolidated and manages the Terrorist Screening Database (commonly known as the "watchlist") to enable screening for immigration and travel, law enforcement, counterterrorism investigations, and intelligence purposes. The TSC ensures the timely dissemination of terrorist identity information to screening agencies for the appropriate and lawful use of terrorism-related information.*
- *Seventy-eight state and major urban area fusion centers play a complementary role in gathering, analyzing, and sharing information, connecting law enforcement and state and local leadership with the rest of the homeland security enterprise.*
- *Information-sharing platforms (e.g., the Homeland Security Information Network, the Technical Resource for Incident Prevention) facilitate the sharing of sensitive information.*

Information-sharing efforts also now include a more well-defined role for local law enforcement and the public, particularly as it relates to detection. The Nationwide Suspicious Activity Reporting Initiative helps train state and local law enforcement to recognize behaviors and indicators related to terrorism, and standardizes how these observations are documented and shared. Meanwhile, the "If You See Something, Say Something™" campaign has raised public awareness of indicators of terrorism and crime and emphasizes the importance of reporting suspicious activity to the proper authorities.

Several of the aforementioned capabilities were involved in apprehending Faisal Shahzad, a terrorist who attempted to detonate a car bomb in Times Square. On May 1, 2010, two New York City sidewalk vendors—both of whom later referred to the "See something, Say something" mantra—alerted a nearby police officer about a suspicious vehicle. The resulting discovery of a failed car bomb initiated investigations by JTTFs in New York, Connecticut, and Massachusetts, with members from the FBI and New York Police Department playing key roles. The investigations led FBI to nominate Faisal Shahzad to the watchlist. As events unfolded, fusion centers also mobilized to identify and share potential leads with the JTTFs. Two

days later, Faisal Shahzad was attempting to leave the country through JFK airport, but was denied boarding due to his inclusion in the watchlist. U.S. Customs and Border Protection (CBP) officers then took Faisal Shahzad into custody.

A second area in which fragmented preparedness efforts proved costly on 9/11 was in coordinating response activities at the World Trade Center. Commission members identified problems with command and control that hampered responders' abilities to work together, and the commission recommended that emergency response agencies adopt the incident command system and unified command. As a result, in 2003, President Bush directed the establishment of a single, comprehensive National Incident Management System (NIMS)—which incorporates the incident command system and unified command as best practices—to enable responders at all jurisdictional levels and across disciplines to work together. This directive required all Federal departments and agencies to adopt NIMS and made NIMS a requirement for receiving Federal preparedness assistance. Since then, millions of individuals nationwide have received training in NIMS. As of 2016, 91 percent of states and territories have incorporated NIMS concepts and principles into all appropriate training. In recent self-assessments, states and territories have consistently rated themselves the most proficient in carrying out Operational Coordination (compared to other core capabilities). The Nation's performances during Hurricane Sandy, and most recently, Hurricane Matthew, while continuing to reveal room for improvement, indicate progress in coordinating large-scale response efforts.

Commission members also identified issues with interoperability. While evacuating civilians from the World Trade Center, first responders struggled with situational awareness of what other responders were doing. Since its inception in 2003, the U.S. Department of Homeland Security (DHS) has awarded billions of dollars in grants to state and local agencies to enhance their communications capabilities. In addition, under the direction of Congress, DHS worked with stakeholders from all levels of government to develop the first National Emergency Communications Plan, which provided a more strategic approach to strengthening emergency communications capabilities nationwide and included three national performance goals to evaluate emergency communications. To measure progress toward these goals, DHS analyzed performance reports from more than 2,800 counties (covering 30,000 public safety agencies). While nearly 75 percent of counties reported consistently being able to provide communications during routine incidents involving multiple jurisdictions, disciplines, and agencies, only 34 percent reported they could do so during a significant event. Despite wide variation in the level of proficiency, the assessments provided evidence of nationwide progress.

Challenges in Implementing National Initiatives

Despite improvements in emergency communications, progress has been slow to address the 9/11 commission's recommendation to free up and assign additional communication frequencies (i.e., frequency spectrum) for public safety use and to support interoperable communications. While Congress included provisions in the *Middle Class Tax Relief and Job Creation Act of 2012* for a new nationwide broadband network for public safety communications, the establishment of this network remains in progress.

Indeed, a few of the commission's unfulfilled recommendations underscore the sweeping nature of the changes called for in the report, as well as the challenges of implementing change on a national scale. For example, while Congress provided seven billion dollars for initial seed funding for the network, experts expect that the cost of deploying the nationwide public

safety broadband network will likely exceed this initial funding. FirstNet had to consider this fact in its request for proposal and is why its new partner, AT&T, has committed to about $40 billion in additional funding throughout the life of the 25-year contract. Additionally, five jurisdictions in close coordination with FirstNet have moved forward on five Early Builder broadband projects, which will be reconciled and/or integrated with the FirstNet network, when it is deployed in their jurisdictions.

T*he 9/11 Commission Report* outlines two other commission recommendations that have encountered significant implementation challenges:

- ***Establishing a biometric entry-exit screening system:*** *While CBP has collected biometric entry data on foreign nationals since 2004, it still lacks a comprehensive, nationwide system for collecting biometric exit data. Combined entry-exit data—especially biometric data, which provides greater assurance of a traveler's identity —is essential to identifying foreign nationals who are overstaying their visits and who may pose homeland security risks. Five of the 19 hijackers on 9/11 exceeded their authorized stay periods. Collecting biometric data at points of departure, however, will likely disrupt existing processes and delay travel and commerce. For example, U.S. airports lack the infrastructure and processes to ensure exit control (i.e., that screened passengers actually depart) and accomplish this in a time-sensitive fashion.*
- ***Secure Identification:*** *In 2005, Congress passed the REAL ID Act, which sought to enhance national security by preventing the fraudulent issuing and use of state driver's licenses and identification cards. Six of the 9/11 hijackers used state-issued identifications to check in for their flights, of which three were obtained fraudulently. In alignment with the 9/11 Commission's recommendation, the Act establishes minimum security standards for state-issued identification (e.g., driver's licenses) and prohibits Federal agencies from accepting identification that fails to meet these standards, including boarding commercial aircraft and entering Federal buildings. Implementation has encountered resistance and delays, with numerous states enacting laws expressly prohibiting state agencies from complying with the Act, and DHS has provided multiple extensions on its deadlines for compliance. As of January 2016, less than half of states and territories were fully compliant.*

For each of these initiatives, the Nation has encountered multiple barriers to successful implementation, requiring new policies, processes, and legislation; increased awareness and buy-in; supporting infrastructure; and innovative technological solutions. While progress has occurred, it has been incremental in nature, with significant uncertainty regarding timelines for completion.

Conclusion

The effects of the attacks on 9/11 reverberated throughout the homeland and triggered numerous efforts to restructure and retool existing capabilities nationwide to better prepare for all threats and hazards, including the creation of DHS. As highlighted by this case study, the attacks prompted a deep examination of the Nation's state of preparedness and led to sweeping changes, some of which have been challenging to implement. More than 15 years later, however, the Nation is more prepared and resilient as a result.

Capabilities to Sustain

Selection Methodology - Appendix D

The Federal Emergency Management Agency (FEMA) used a two-part analysis to identify capability to sustain candidates. The first part of the analysis assesses proficiency, and the second part assesses a potential gap between demand and performance. Higher scores indicate that a core capability is a better candidate for being a capability to sustain.

In the first part of the analysis, FEMA scored each core capability against nine preparedness indicators to identify core capabilities that the Nation is proficient in executing (see Table 9). A maximum of 5.5 points was possible.

Table 9. Part one of the capabilities to sustain analysis includes nine preparedness indicators that help identify core capabilities the Nation is proficient in executing.

Criteria	No. of Indicators	Max. Point Contribution
Do the key findings in the 2017 *National Preparedness Report* indicate that this capability is an area of strength?	1	1 point
Do the 2016 State Preparedness Report results indicate proficiency in this core capability nationwide?	1	1 point
Is this core capability exercised frequently?	3	1 point
Do data indicate strong participation in relevant training courses for this core capability?	1	0.5 points
Do various assessments indicate that the core capability is relatively mature?	3	2 points

In the second part of the analysis, FEMA scored each core capability against six additional indicators to identify core capabilities in which a growing gap may be likely between demand for the core capability and its performance (see Table 10). A maximum of 3.5 points was possible.

Table 10. Part two of the capabilities to sustain analysis includes six preparedness indicators that help identify core capabilities in which a growing gap in capability may be likely in the future.

Criteria	No. of Indicators	Max. Point Contribution
Do trends in State Preparedness Report results indicate a decreasing ability to meet performance targets for this core capability nationwide?	3	1.5 points
Has this core capability experienced a significant drop in grant funding that may result in a future decline in capability levels?	1	0.5 points
Do Federal strategic plans indicate that increasing demand for this core capability may exist in the future?	1	1 point
Do various drivers influencing change in emergency management indicate that increasing gaps in this core capability may exist in the future?	1	0.5 points

Areas for Improvement

Selection Methodology - Appendix E

The Federal Emergency Management Agency (FEMA) scored each core capability against nine preparedness indicators to identify area for improvement candidates (see Table 11). Higher scores indicated a likely area for improvement. FEMA scored each core capability against nine preparedness indicators. A maximum of 5.0 points was possible.

Table 11. The areas for improvement analysis consists of nine preparedness indicators that help identify core capabilities in which the Nation is less proficient.

Criteria	No. of Indicators	Max. Point Contribution
Do the key findings in the 2017 *National Preparedness Report* indicate that this capability exhibits major deficiencies in its performance nationally?	1	1 point
Do the 2016 State Preparedness Report results indicate low proficiency in this core capability nationwide?	1	1 point
Is this core capability infrequently exercised?	3	1 point
Do data indicate low numbers of relevant training courses for this core capability?	1	0.5 point
Is there evidence of progress in assessing and validating core capability performance?	1	0.5 points
Has this core capability experienced a significant drop in grant funding that may result in a future decline in capability levels?	1	0.5 points
Do various drivers influencing change in emergency management indicate that increasing gaps in this core capability may exist in the future?	1	0.5 points

FEMA reviewed all scores as part of its final selection process. This review set the threshold for consideration as an area for improvement. If a core capability's score was above the required threshold of 1.5 points with no discrepancies identified, FEMA selected that core capability as an area for improvement.