2018 National Preparedness Report

Homeland Security

Executive Summary

The 2018 *National Preparedness Report* provides an overview of key developments in national preparedness—incorporating findings and lessons learned from incidents in 2017 in combination with data and inputs from federal interagency and whole community partners. The report evaluates and measures progress in building, sustaining, and delivering five selected core capabilities that have faced emerging and persistent challenges. Refining the scope of the 2018 edition of the report to focus on these challenging elements concentrates the discussion on what the whole community—including individuals, businesses, nonprofit organizations, and all levels of government— needs to address to increase the Nation's preparedness. The in-depth assessment of the targeted areas provided in this report will be particularly important in the years to come, as the Nation looks to address long-term trends that will influence national preparedness—including rising disaster costs, new technology, an older and more diverse population, and evolving threats such as cybersecurity.

The 2018 *National Preparedness Report* begins with an **Introduction** before providing a **2017 Year in Review**, which highlights notable real-world incidents and ongoing recovery efforts across the Nation in 2017. Next, the **Learning from Incidents and Improving National Preparedness** section summarizes major milestones in national preparedness, including lessons learned from historical incidents—from the 9/11 attacks to the 2017 Hurricane Season. The main body of the report offers 13 key findings that highlight successes and challenges across five core capabilities that have faced **Persistent Preparedness Challenges**—Operational Coordination, Infrastructure Systems, Housing, Economic Recovery, and Cybersecurity. These lessons learned and findings enable the Nation to better understand its capabilities, identify shortfalls, and build capacity to ready the Nation for future large-scale and catastrophic incidents. The report concludes with **The Path Forward**, which discusses future efforts to assess the Nation's capabilities to prepare for the threats and hazards that pose the greatest risk.

What is the National Preparedness Report?

The *National Preparedness Report* is a requirement of the *Post-Katrina Emergency Management Reform Act* and a key element of the National Preparedness System. This annual report evaluates progress and challenges that individuals and communities, private and nonprofit sectors, faith-based organizations, and all levels of government have faced in preparedness. 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.

The 2018 Report offers 13 key findings that highlight successes and challenges across five core capabilities that have faced persistent preparedness challenges—Operational Coordination, Infrastructure Systems, Housing, Economic Recovery, and Cybersecurity

Key Findings

Operational Coordination

The Nation is advancing the implementation of a National Incident Management System (NIMS), but significant challenges remain in implementing the system during large-scale events in incident command, resource management, staffing, and communications.

Infrastructure Systems

Interdependencies between energy and other infrastructure systems present challenges in response and recovery; efforts to mitigate disruptions and to help communities learn from and plan for these challenges are growing.

The whole community has taken steps to increase the resilience of infrastructure, but challenges remain.

Housing

The Nation continues to face challenges with delivering disaster housing and is exploring innovative programs to address capability gaps.

Challenges remain with efforts to coordinate timely and efficient housing damage assessments for survivors after large-scale disasters.

While research shows that incorporating mitigation strategies in rebuilding can yield positive benefits, limited incentives exist to encourage resilient home reconstruction after a disaster.

Economic Recovery

Partners across the whole community have engaged in recent efforts to build business planning capabilities, though many small businesses lack business continuity plans.

While federal agencies have made efforts to streamline disaster recovery assistance, businesses continue to face challenges navigating post-disaster economic recovery programs.

Post-disaster, communities often struggle to effectively communicate and coordinate with the private sector, and efforts to address these challenges are ongoing.

Financial disruptions from disasters can disproportionately affect less-resourced communities, prolonging their return to economic viability.

Cybersecurity

Evolving cyber threats continue to outpace the development of protective practices; at the same time, technology users often fail to implement precautionary measures to safeguard their cyber systems.

Insufficient information sharing between the public and private sectors has hindered the Nation's effectiveness in defending against cyber threats.

The Federal Government faces persistent challenges in the recruitment and retention of cybersecurity personnel, though it has taken steps to improve cybersecurity training for the Nation.

Table of Contents

Introduction

National preparedness is the shared responsibility of individuals, communities, private and nonprofit sectors, faith-based organizations, and all levels of government. As an annual requirement of the *Post-Katrina Emergency Management Reform Act* (PKEMRA), the *National Preparedness Report* has provided an assessment of the Nation's progress toward achieving the *National Preparedness Goal* of a secure and resilient Nation since 2012. The 2018 *National Preparedness Report* presents a revised approach that includes an overview of key developments in national preparedness, including lessons learned across the whole community from incidents in 2017, and an in-depth analysis of five core capabilities that have faced persistent challenges—one capability that has reemerged as a capability to sustain and four capabilities consistently identified as national areas for improvement in past reports. Refining the scope of the 2018 *National Preparedness Report* to focus on these challenges concentrates the discussion on what the whole community—including individuals, businesses, nonprofit organizations, and all levels of government—needs to accomplish to have the most impact on increasing the Nation's preparedness. This in-depth assessment of these persistent challenges will be particularly important in the years to come, as the Nation looks to address long-term trends that will influence national preparedness—including rising disaster costs, new technology, an older and more diverse population, and evolving threats such as cybersecurity. While the scope of this assessment is domestic, national preparedness is strengthened through engagement and cooperation with international partners and organizations, and the sharing of expertise, experiences, and best practices.

The 2018 *National Preparedness Report*: Persistent Preparedness Challenges

The 2018 *National Preparedness Report* focuses on one core capability that has been identified as a capability to sustain and four core capabilities that have been identified as areas for improvement in past reports:

Capability to Sustain

- Operational Coordination

Areas for Improvement

- Infrastructure Systems
- Housing
- Economic Recovery
- Cybersecurity

The report examines the Nation's progress and challenges in each of these capabilities from the first *National Preparedness Report* in 2012 through 2017.

Overview of the National Preparedness Goal and System

The *National Preparedness Goal* (the Goal) describes what it means for the United States to be prepared for all threats and hazards, including natural, technological, and human-caused incidents. The Goal itself defines a vision for national preparedness, 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.*

The Goal identifies 32 core capabilities that preparedness stakeholders need to build, sustain, and deliver. Core capabilities are distinct, critical components needed to achieve the goal of a secure and resilient Nation. These core capabilities provide a common vocabulary for understanding preparedness efforts and discussing tasks across the whole community, enhancing coordination between preparedness stakeholders. The capabilities-based approach for building the Nation's preparedness is applicable to any type of disaster. In addition, continuity planning and operations are inherent components of each core capability and increase the likelihood that organizations can deliver core capabilities of each mission area, especially during catastrophic incidents that impact resource availability. While the 2017 disaster season was primarily characterized by major hurricanes and wildfires, future years could introduce different types of incidents. Focusing on capabilities rather than specific hazards enables communities to build a culture of preparedness and ready the Nation for catastrophic disasters. The Goal organizes these core capabilities into five mission areas that provide a higher-level structure for organizing preparedness activities:

- **Prevention**: Preventing an imminent, threatened, or actual act of terrorism or extremist violence;
- **Protection**: Protecting citizens, residents, visitors, and assets 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 immediate aftermath of an incident; and
- **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.

Appendix B: Mission Area Overview provides a more detailed description of each mission area and its respective core capabilities.

Preparedness is best delivered through a system that is locally executed, state managed, and federally supported. The National Preparedness System provides an organized, flexible, and scalable process to guide preparedness activities for the whole community to build, sustain, deliver, and assess the core capabilities across all hazards. The National Preparedness System has six components, which build on each other to achieve a prepared and resilient Nation (**Figure 1**):

- **Identify and Assess Risk**: Collecting information on existing, potential, and perceived threats and hazards to assess risks;
- **Estimate Capability Requirements**: Identifying the specific capabilities and activities needed to best address risks for disaster planning;
- **Build and Sustain Capabilities**: Determining the best ways—including training, education, and assistance—to use limited resources to build and maintain capabilities;
- **Plan to Deliver Capabilities**: Engaging with all relevant preparedness stakeholders and all levels of government to build awareness and coordinate preparedness efforts;
- **Validate Capabilities**: Using exercises and assessments to test abilities and identify lessons learned to continuously improve capabilities to address threats and hazards; and
- **Review and Update Capabilities**: Performing regular reviews to keep preparedness efforts up-to-date with evolving risks and resources.

The *National Preparedness Report* reflects each part of the National Preparedness System. For the Validate Capabilities component, it serves as the principal analysis and reporting product to monitor the Nation's progress in building, sustaining, delivering, and assessing the 32 core capabilities that support the Goal.

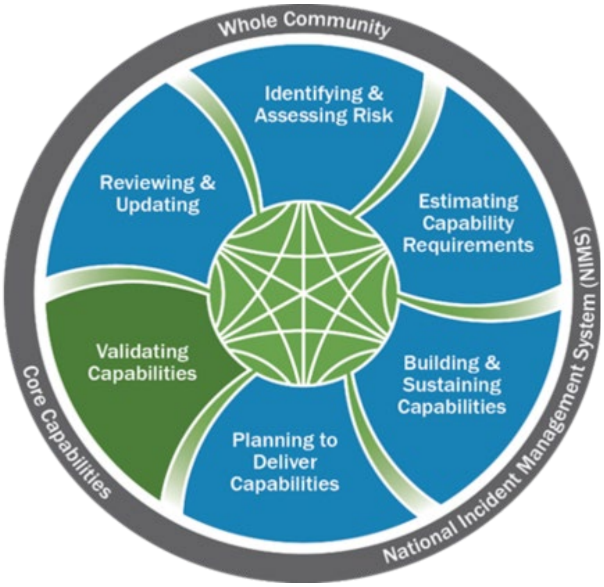

Whole Community
Identifying & Assessing Risk
Estimating Capability Requirements
Building & Sustaining Capabilities
Planning to Deliver Capabilities
Validating Capabilities
Reviewing & Updating
Core Capabilities
National Incident Management System (NIMS)

Figure 1. The National Preparedness System includes six interconnected components that outline an organized process for the whole community to build, sustain, deliver, and assess the core capabilities defined in the Goal.

Report Organization

Following the **Introduction**, the 2018 *National Preparedness Report* continues with the **2017 Year in Review**, which highlights notable real-world incidents that attracted national headlines and ongoing recovery efforts across the Nation in 2017. The section also provides an analysis of preparedness data for 2017.

Next, the **Learning from Incidents and Improving National Preparedness** section summarizes major milestones in national preparedness, including lessons learned from the 2017 Hurricane Season, and provides an overview of efforts to ready the Nation and build capability for catastrophic and large-scale incidents.

The main body of the report—**Persistent Preparedness Challenges**—provides an in-depth analysis of five core capabilities that past *National Preparedness Reports* identified as capabilities to sustain or as recurring areas for improvement: Operational Coordination, Infrastructure Systems, Housing, Economic Recovery, and Cybersecurity (**Figure 2**). The 2018 *National Preparedness Report* reviews challenges across these five core capabilities as well as lessons learned and progress made from 2012 through 2017.

The report concludes with **The Path Forward**, which discusses future efforts to assess the Nation's capabilities to prepare for the threats and hazards that pose the greatest risk. In addition, the 2018 *National Preparedness Report* includes three appendices:

- **Appendix A: Acronym List**: Defines the acronyms appearing in the report;
- **Appendix B: Mission Area Overview**: Describes the five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and the core capabilities in each mission area; and
- **Appendix C: Research Approach**: Describes the steps taken to ensure a comprehensive report as well as the criteria and process used in past reports to identify capabilities to sustain and areas for improvement.

Selected Core Capabilities in the 2018 National Preparedness Report

Core Capability	National Preparedness Reports					
	2012	2013	2014	2015	2016	2017
Operational Coordination	--	--		●		●
Infrastructure Systems	□	□	□	□	□	□
Housing	□	□	□	□	□	□
Economic Recovery	□	□		□	□	□
Cybersecurity	□	□	□	□	□	□

● Capability to Sustain
□ Area for Improvement

Figure 2. The 2018 *National Preparedness Report* provides an in-depth analysis of five core capabilities that have repeatedly been identified in past reports as a capability to sustain or area for improvement.

2017 Year in Review

Each year, the Nation faces a range of threats and hazards that reveal where strengths and shortfalls exist in building, delivering, and sustaining the 32 core capabilities identified in the Goal. The following section provides a snapshot of notable real-world incidents that tested the Nation's capabilities and ongoing disaster recovery efforts in 2017 (**Figure 3**). A review of preparedness trends provides additional context on the Nation's capabilities for preventing, protecting against, mitigating, responding to, and recovering from all threats and hazards.

Year in Review Snapshot

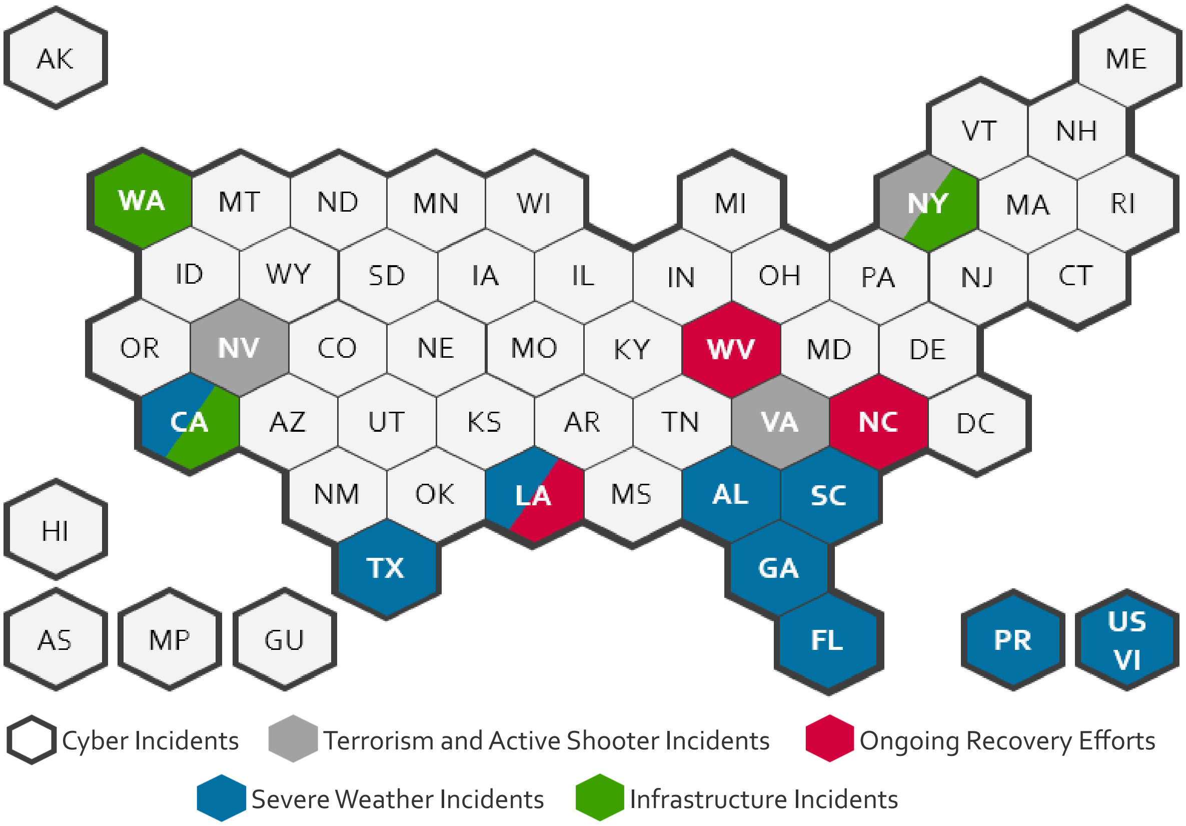


Figure 3. In 2017, the Nation faced a range of threats and hazards while conducting ongoing recovery efforts, including cyber incidents, severe weather incidents, terrorism and active shooter incidents, and infrastructure incidents.

Cyber Incidents

- **May 12–15:** A widespread ransomware campaign affected over one million unique systems in 150 countries, including the United States. Known as "WannaCry," the software locked users out of their systems until users paid a ransom. Unlike typical ransomware attacks, WannaCry used a form of malware that enabled the attack to spread more quickly with each new infection.

- **September 7:** Equifax—one of the Nation's three major credit reporting agencies—informed the public that unknown actors had infiltrated its networks. Hackers potentially stole the sensitive personal information of over 143 million American customers, including names, Social Security numbers, birth dates, addresses, and driver's license numbers. A Federal Bureau of Investigation (FBI) investigation to assess the scope and impact of the breach is ongoing.

Terrorism and Active Shooter Incidents

- **June 14:** An assailant opened fire on members of Congress during a baseball practice in Alexandria, Virginia. Five individuals were injured, including House Majority Whip Steve Scalise. U.S. Capitol Police shot and killed the attacker.

- **October 1:** A gunman opened fire on a music festival in Las Vegas, Nevada. In one of the deadliest U.S. mass shootings, the assailant killed 58 individuals and injured an additional 515. Local police later found the attacker dead from a self-inflicted gunshot.

- **October 31:** A man drove a vehicle along a crowded bike path in Manhattan, New York, killing eight and injuring dozens of pedestrians. Later apprehended by police, the suspect allegedly reported that he conducted the attack on behalf of the Islamic State of Iraq and al-Sham (ISIS).

Active Shooter Trends

An active shooter incident is a situation in which an individual is actively engaged in killing or attempting to kill people using a firearm in a confined and populated area. The number of active shooter incidents has increased significantly from one in 2000 to 30 in 2017. The number of people killed or injured in active shooter incidents totaled 2,145 between 2000 and 2017.

- **December 11**: A man claiming to act on behalf of ISIS set off an intended suicide bomb in the crowded Port Authority Bus Terminal in Manhattan, New York, injuring five people. This type of device, if properly assembled and initiated, could cause property damage, personal injury, or death.

Severe Weather Incidents

- **August 25–September 20:** Three Category 4 hurricanes made landfall across the southern United States and Caribbean territories within four weeks of each other. **Hurricane Harvey** inundated parts of Texas and Louisiana with record-breaking flooding from 60 inches of rain that fell in less than two days. High winds from **Hurricane Irma** resulted in a peak of over eight million customers across Florida, the Seminole Tribe of Florida, Georgia, Alabama, Puerto Rico, and the U.S. Virgin Islands without power. **Hurricane Maria** was the first Category 4 storm to make landfall in Puerto Rico in 85 years. The hurricane forced every airport and port in Puerto Rico to close, resulted in widespread power and communication outages, impacted the delivery of critical medical supplies, and disrupted key supply routes from Puerto Rico to the U.S. Virgin Islands. Recovery from the hurricane may take decades.

- **October 8–October 31:** Wildfires spread through Northern California, burning cities and communities across 245,000 acres and destroying over 8,900 structures. The wildfires forced the evacuation of over 100,000 residents and resulted in the deaths of 43 people.

- **December 4–January 12:** A second series of wildfires devastated large areas of Southern California. The Thomas Fire—the state's largest fire on record—burned a total of 281,893 acres, destroyed 1,063 structures, and led to the death of one person.

Infrastructure Incidents

- **February 7–14:** Heavy rainfall across California resulted in substantial damage to the Oroville Dam's emergency spillway. As a result, state officials ordered 188,000 residents near Lake Oroville to evacuate.

- **March 24–April 3:** Railroad track defects caused two train derailments within a week of each other, interrupting travel for hundreds of thousands of passengers and commuters at Pennsylvania Station in New York City and demonstrating a need for infrastructure improvements. In response, Amtrak launched an emergency repair program to strengthen railroad infrastructure, operations, and preparedness. Recent derailments highlight ongoing challenges with aging and deteriorated infrastructure. Much of the rail infrastructure in Amtrak's Northeast Corridor is beyond its serviceable lifespan, and inadequate funding has led to a backlog of infrastructure maintenance projects.

Ongoing Recovery Efforts

- The Federal Government, along with seven states and territories, implemented coordination mechanisms outlined in the *National Disaster Recovery Framework* (NDRF) eight times in 2017, triggering coordinated federal recovery assistance for affected communities. In 2017, recovery efforts continued for several incidents that occurred in 2016—including severe storms in West Virginia, flooding in Louisiana, and Hurricane Matthew in North Carolina. In Fiscal Year (FY) 2017, the Federal Emergency Management Agency (FEMA) provided nearly $1.4 billion through its Individuals and Households Program (IHP) and Public Assistance grant programs to support recovery from these three 2016 incidents. Recovery efforts for the 2017 Hurricane Season are also still in progress.

2017 Preparedness Snapshots

Most disasters in the Nation do not receive federal disaster declarations and are wholly led and managed by local and state emergency managers. In FY 2017, states and local jurisdictions relied on their own resources to respond to over 35,000 incidents that did not reach the level of a major disaster declaration. Efforts to plan, train, and exercise—funded from local, state, and federal sources—help to build, sustain, and test capabilities required to address disasters and emergencies. In the event that a disaster overwhelms the capabilities of affected states, tribes, or territories, the Federal Government provides additional support for response and recovery operations. For instance, in FY 2017, the Federal Government provided emergency management support to 137 disasters that received a major disaster or emergency declaration. The following sections detail the variety of federal support to state, tribal, and territorial partners to enhance their preparedness and emergency management efforts.

Federal Disaster Assistance

In 2017, federal agencies supported incident response and recovery across the Nation for major disasters and emergencies, fire management, and droughts. The *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act) provides statutory authority for the President to issue major disaster or emergency declarations upon a Governor or Tribal Chief Executive's request in response to incidents that overwhelm state, local, or tribal governments. The Stafford Act defines an emergency as any instance for which, in the determination of the President, federal assistance is needed to supplement state and local or tribal efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. The Stafford Act defines a major disaster as any natural catastrophe or, regardless of cause, any fire, flood, or explosion, which the President determines causes damage of sufficient severity and magnitude to warrant major disaster assistance (**Figure 4**). A major disaster declaration enables the Federal Government to provide a range of disaster assistance programs—including FEMA's Individual Assistance Program, Public Assistance Program, and Hazard Mitigation Assistance Grant Program—to affected communities. Comparatively, an emergency declaration provides a more limited breadth of federal assistance.

A state or territory may also submit a request to FEMA for a Fire Management Assistance declaration, which allows FEMA's Fire Management Assistance Grant Program to provide funding to support wildfire mitigation or control costs (**Figure 5**). Eligible costs include equipment, materials, and staff mobilization activities. Similarly, a state, territory, or tribe can request the Secretary of Agriculture to issue a disaster declaration for agriculture-related disasters, including drought (**Figure 6**). In 2012, the U.S. Department of Agriculture (USDA) streamlined this declaration process to fast-track designations for severe drought. A drought designation triggers a variety of emergency assistance programs, such as the Farm Service Agency Livestock Forage Disaster Program and Emergency Loan Program.

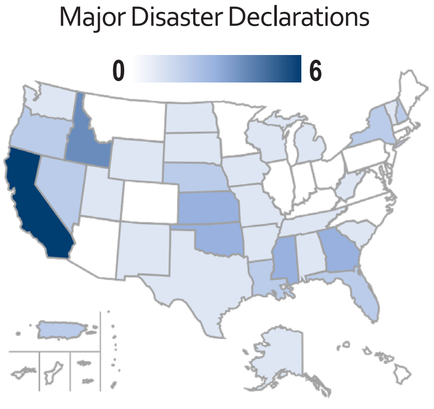


Figure 4. In 2017, federal agencies assisted in 59 major disaster declarations across 33 states and territories.

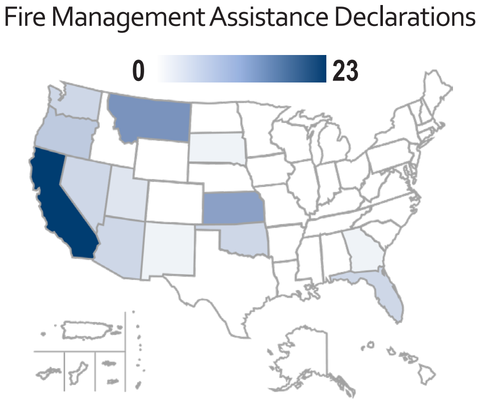


Figure 5. In 2017, federal agencies assisted with 62 instances of fire management across 13 states.

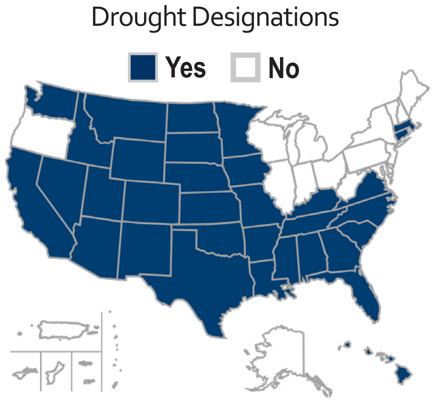


Figure 6. In 2017, federal agencies assisted with USDA-designated drought disasters for 1,681 counties across 33 states.

Federal agencies also provide recovery assistance after major disasters, including disasters that do not receive a Stafford Act declaration. For example, in FY 2017, the U.S. Small Business Administration (SBA) Office of Disaster Assistance approved 27,263 loans for a total of $1.7 billion—comprised of $1.4 billion to over 24,100 homeowners and renters as well as $300 million to over 3,100 businesses. This includes 1,188 approved loans for a total of nearly $59 million to survivors of disasters that did not qualify for assistance under the Stafford Act. In addition, the U.S. Department of Housing and Urban Development (HUD) allocated nearly $7.4 billion in Community Development Block Grant Disaster Recovery (CDBG-DR) funding to assist in long-term recovery from the 2017 incidents.

Investments to Build and Sustain Capabilities

Preparedness begins with investments in activities to build and sustain capabilities at the state, tribal, territorial, and local levels. The Federal Government plays a supporting role by providing grants, exercises, and training to stakeholders from nonprofit organizations, the private sector, and state, tribal, territorial, and local governments to build emergency management capabilities through proactive risk assessments, preparedness activities, and mitigation investments. For example, FEMA provides preparedness (non-disaster) program funding to local and state governments to enhance the capacity of emergency responders to prepare for and respond to a variety of threats. In addition, FEMA's National Exercise Program (NEP) serves as the principal mechanism to examine and validate capabilities across the Nation. Through its National Training and Education Division, FEMA also provides training and education to all communities to strengthen national preparedness. In addition to FEMA's efforts, SBA, HUD, USDA, and the U.S. Department of Health and Human Services (HHS) administer grants, low-interest loans, and training programs that support disaster resilience and recovery. For example, HHS Centers for Disease Control and Prevention (CDC) plays a pivotal role in ensuring that state and local public health systems are prepared for public health emergencies through technical assistance, training and exercises. The Department of Defense (DoD) also supports training efforts that help communities build response capabilities. FEMA, along with other federal agencies, also provides funding to support mitigation activities to enhance the resilience and self-sufficiency of communities before disasters occur and to lower the cost of recovery after a disaster. This section provides a snapshot of these efforts during 2017.

In 2017, FEMA's NEP conducted **101 exercises** across the country, which in total tested **31 out of the 32 core capabilities** (**Figure 7**). The Response mission area remained the most frequently exercised mission area, followed by the Recovery mission area.

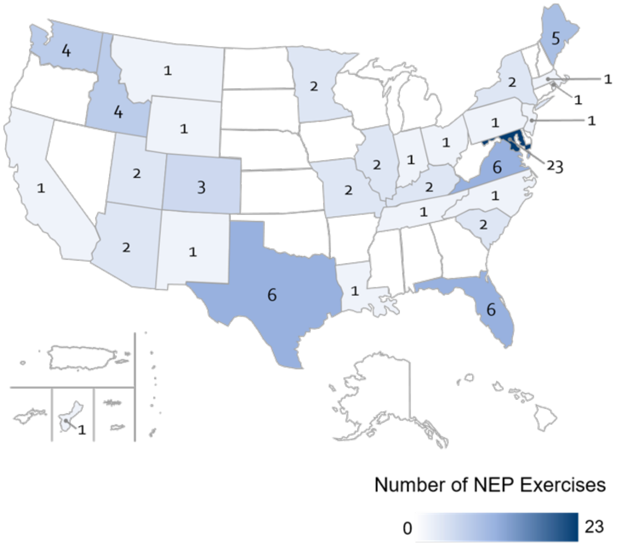


Figure 7. In 2017, NEP exercises across the country tested 31 core capabilities and addressed a variety of threats and hazards, including cybersecurity, hazardous material, and earthquakes.

FEMA supported over **120 continuity training and exercise events** across the Nation. In addition, FEMA published the Continuity Guidance Circular to guide whole community efforts in developing and maintaining the ability to deliver core capabilities during incidents.

In 2017, the DHS Office of Infrastructure Protection Office for Bombing Prevention (OBP) supported **573 counter-Improvised Explosive Device (IED) risk mitigation trainings** for more than **10,000 security stakeholders**, **12 counter-IED preparedness workshops** in high-risk jurisdictions with more than **475 participants**, and **381 capability assessments** of public safety bomb squads and other operational units. In addition, OBP and FBI partners collaborated to provide dedicated assistance to the faith-based communities affected by a surge in bomb threats.

In FY 2017, FEMA provided over **$2.3 billion** in preparedness (non-disaster grants) (**Figure 8**). Additionally, in FY 2017, HHS provided more than **$900 million** in public health and healthcare grants to states and localities.

Distribution of FEMA Preparedness (Non-Disaster) Grants by Core Capability, FY 2017

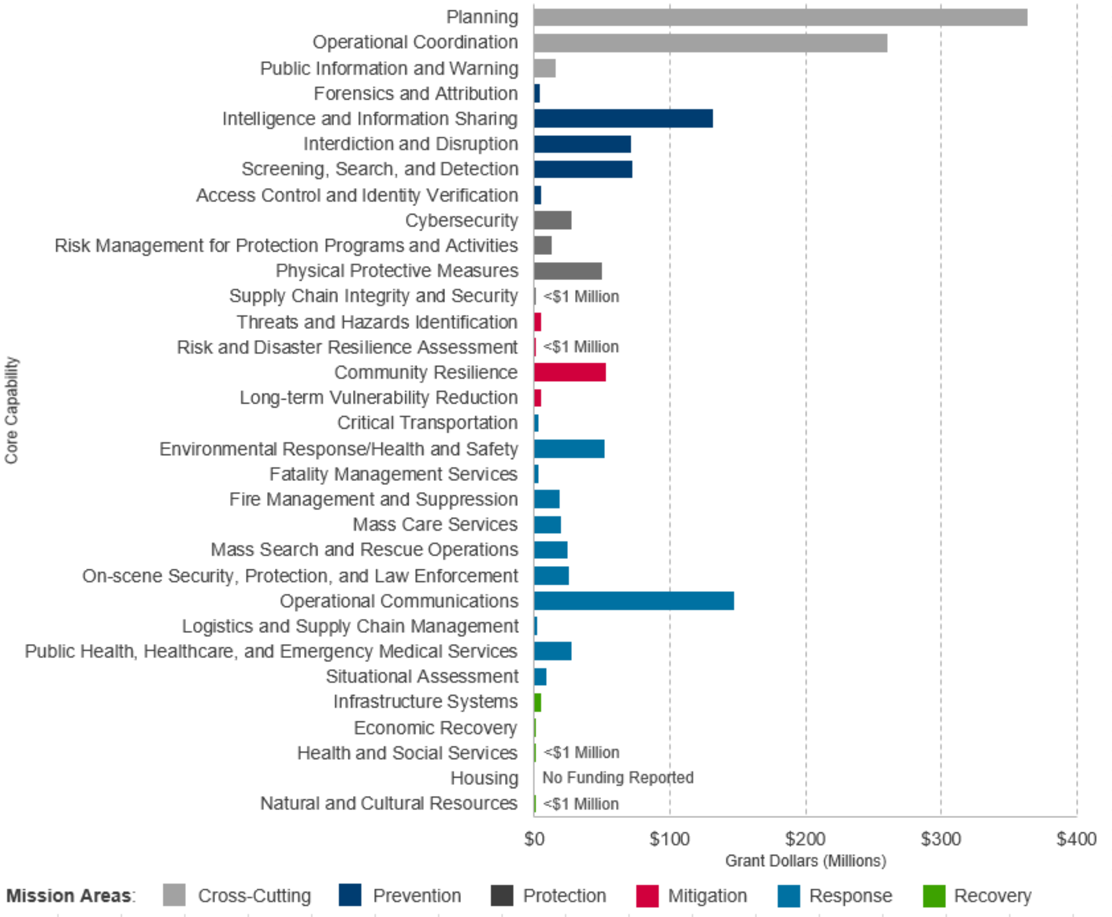


Figure 8. In FY 2017, grant recipients reported the greatest amount of obligated funding to projects supporting Planning, Operational Coordination, and Operational Communications core capabilities. Grant recipients use the Biannual Strategy Implementation Report (BSIR) to track planned and actual grant expenditures. The BSIR is a snapshot of obligated funding for the given reporting period.

In FY 2017, FEMA training programs achieved approximately **2.3 million course completions** across all core capabilities.

In 2017, the Department of Homeland Security (DHS) Domestic Nuclear Detection Office (DNDO) dedicated **$2 million** to deliver several radiological and nuclear detection training courses. In total, these courses trained **949 students** from **27 states** and several federal agencies.[1]

In FY 2017, FEMA awarded over **$650 million** in Hazard Mitigation grants to implement long-term hazard mitigation measures following a major disaster declaration. For project subapplications that required a benefit cost analysis, the average benefit to cost ratio was 1.6, meaning that for every $100 spent the program provided a benefit of $160. [2] In addition, FEMA made nearly **$90 million** available to assist state, tribal, territorial, and local governments to reduce overall risk from future hazards through its Pre-Disaster Mitigation Grant Program. FEMA also made **$160 million** in Flood Mitigation Assistance available to jurisdictions to reduce or eliminate flood risk and claims under the National Flood Insurance Program.

[1] In December 2017, the establishment of the DHS CWMD Office consolidated DNDO and a majority of the Office of Health Affairs.

[2] This value includes FEMA grants awarded between October 1, 2016 and February 28, 2018.

National Capability Trends From 2017 State Preparedness Report Results

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 assessment process.[3] States and territories may change their targets as their capabilities change over time. In the State Preparedness Report, jurisdictions use a five-point rating scale—with a five rating being the highest proficiency—to assess each of these core capabilities in five areas: Planning, Organization, Equipment, Training, and Exercises. Capabilities can take multiple years to build, and therefore year-over-year changes in capability ratings are typically incremental. In 2017, states and territories reported their strongest proficiency ratings (indicated by the percentage of four and five ratings) in the core capabilities that cut across all mission areas (i.e., Planning, Operational Coordination, and Public Information and Warning) and the capabilities that fall under the Response mission area. States and territories reported their lowest proficiency ratings in the capabilities associated with the Recovery and Protection mission areas. State and territory capability levels remained generally consistent with prior years (**Figure 9**).

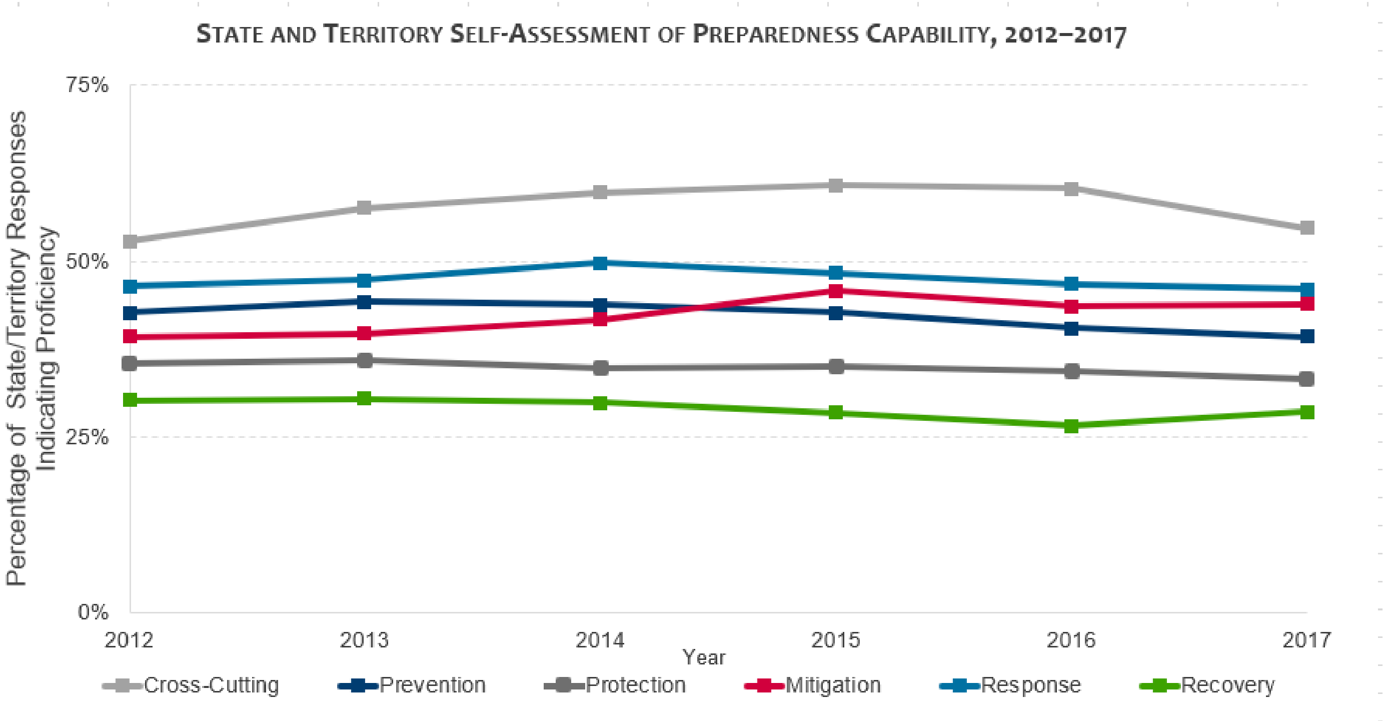


Figure 9. Since 2012, states and territories have reported the highest capability ratings in the cross-cutting core capabilities, and those within the Response mission area.

Figure 10 shows the breakdown of core capability proficiency ratings by mission area from 2017. Notable changes from 2016 to 2017 include:

- **High Proficiency Capabilities:** Threats and Hazards Identification moved into the top 10 capabilities with the highest proficiency ratings; Intelligence and Information Sharing moved out of the top 10.
- **Low Proficiency Capabilities:** Logistics and Supply Chain Management and Supply Chain Integrity and Security joined the bottom 10 capabilities with the lowest proficiency ratings, replacing Health and Social Services and Fatality Management Services.

[3] Prior to 2018, tribes are not required to complete the State Preparedness Report. The State Preparedness Report was renamed the Stakeholder Preparedness Review in 2018.

2017 Core Capability Proficiency Ratings by Mission Area

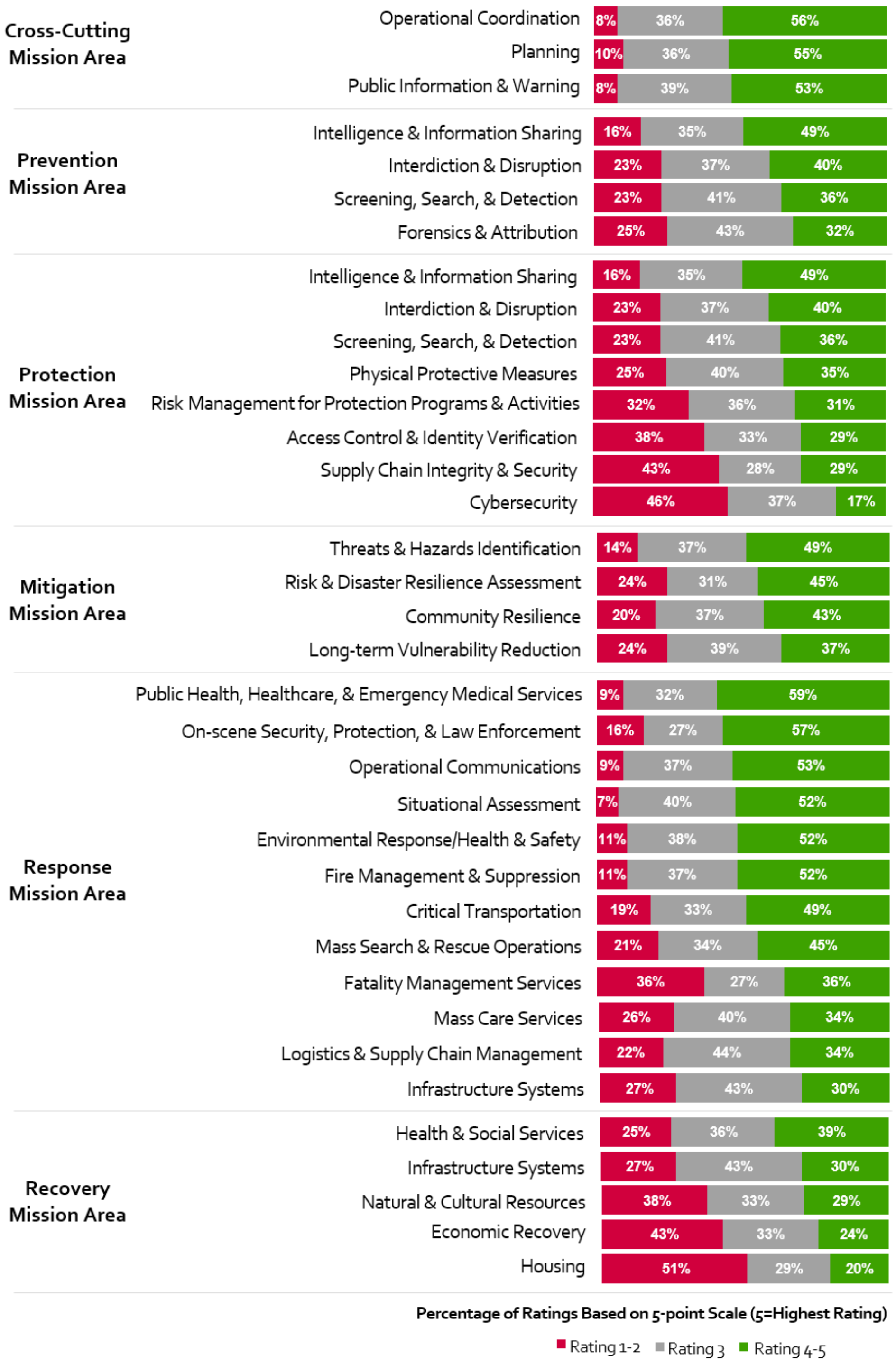


Figure 10. In 2017, states and territories generally report high proficiency in the cross-cutting mission area. States and territories reported their lowest proficiency ratings in the capabilities associated with the Recovery and Protection mission areas.

Learning from Incidents and Improving National Preparedness

The 2017 disaster season introduced unprecedented challenges that tested the Nation's capability to address catastrophic-level incidents.[4] 2017 marked the first time on record that three Category 4 hurricanes (Harvey, Irma, and Maria) hit the United States in the same hurricane season, resulting in destruction across multiple jurisdictions. Moreover, the Nation experienced a particularly widespread and devastating wildfire season that resulted in over 9.7 million acres burned, the third most damaging on record. Lessons learned from 2017 incidents enable the Nation to better understand its capabilities, identify shortfalls, and build preparedness capacity for future large-scale and catastrophic incidents.

This section details significant developments in national preparedness and how major incidents shaped them. These milestones show that building a culture of preparedness requires continuous learning, improvement, and implementation of steps to address shortfalls. Since the 9/11 attacks, the Nation has made significant progress in preparedness. However, the risk landscape continues to evolve, and the Nation must continue to assess and build capabilities to increase readiness for future incidents.

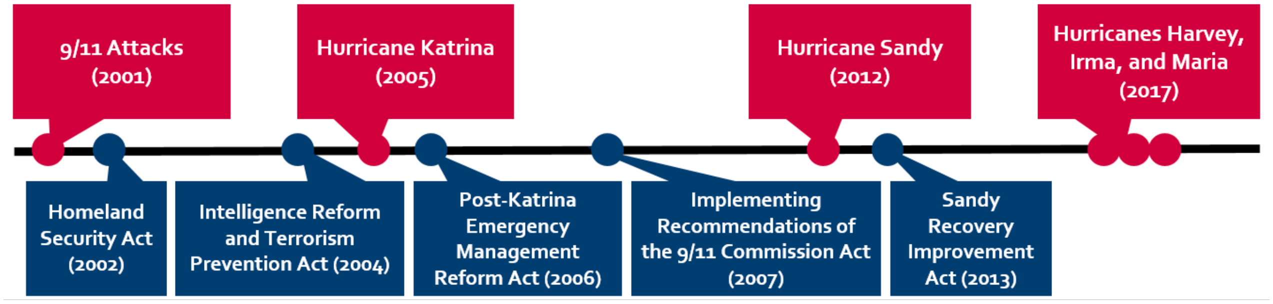
Lessons learned from 2017 incidents enable the Nation to better understand its capabilities, identify shortfalls, and build preparedness capacity

Preparedness Capability Trends

In addition to reporting their capability levels in the State Preparedness Report, states and territories also identify where gaps exist in their capabilities and what those gaps specifically entail. Analyses of these functional area gaps enable stakeholders to identify areas for improvement across the Nation. The ***Preparedness Capability Trends*** in this section highlight areas where states and territories have reported specific functional area gaps in their capabilities.

Major Incidents Impacting National Preparedness

The major disasters of 2017 represent a pivotal moment in the Nation's emergency management history and provide an opportunity to better understand and strengthen capabilities. In the past, incidents such as the 9/11 attacks, Hurricane Katrina in 2005, and Hurricane Sandy in 2012 revealed areas for improvement and prompted subsequent refinements to emergency management (**Figure 11**). A review of the lessons learned from these significant incidents in this section and the persistent preparedness challenges described in the next section is essential for understanding how far the Nation has come and what it needs to advance its security and resilience.



9/11 Attacks (2001)
Hurricane Katrina (2005)
Hurricane Sandy (2012)
Hurricanes Harvey, Irma, and Maria (2017)
Homeland Security Act (2002)
Intelligence Reform and Terrorism Prevention Act (2004)
Post-Katrina Emergency Management Reform Act (2006)
Implementing Recommendations of the 9/11 Commission Act (2007)
Sandy Recovery Improvement Act (2013)

Figure 11. Changes in emergency management and homeland security authorities that have occurred after each major incident since the 9/11 attacks.

[4] The National Response Framework defines a catastrophic incident as any natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions.

9/11 Attacks

On September 11, 2001, the terrorist group al-Qaeda launched a series of four complex coordinated attacks on the United States, killing more than 3,000 people and injuring over 6,000 more. The attacks were collectively the single deadliest incident for first responders—both firefighters and law enforcement officers—in the history of the Nation. More than 400 fire and emergency first responders lost their lives in the response to the 9/11 attacks.

Progress in Intelligence and Information Sharing

In 2006, DHS designated the Homeland Security Information Network (HSIN) as the primary system to share information and collaborate across DHS and its partners. In recent years, HSIN has fostered additional partnerships and emerged as the main platform to share sensitive but unclassified intelligence products, guidebooks, and resources across all levels of government. In 2017, there were over 94,000 HSIN users, up from around 22,000 in 2013.

Lessons from these attacks revealed that the Nation did not have the capabilities to respond to terrorist threats posed by nonstate actors like al-Qaeda. As a result, Congress enacted the *Homeland Security Act of 2002*, which created DHS. President George W. Bush and Congress also created the National Commission on Terrorist Attacks Upon the United States to develop a comprehensive report on the attacks. The report offered several recommendations to enhance national preparedness capabilities, including establishing federal homeland security assistance based on an assessment of risks and vulnerabilities and adopting the Incident Command System (ICS) across the Nation. Since then, the Nation has undertaken efforts to address the report's recommendations, including enhancing nationwide terrorism prevention and protection capabilities by supporting state and major urban area fusion centers and developing and maintaining the National Incident Management System (NIMS). Additional developments include:

- The *Intelligence Reform and Terrorism Prevention Act of 2004* established a National Counterterrorism Center and Director of National Intelligence position to coordinate intelligence efforts across all levels of government.
- The *Implementing Recommendations of the 9/11 Commission Act of 2007* authorized the Homeland Security Grant Program to assist jurisdictions in preventing, preparing for, protecting against, and responding to terrorist acts and established a State, Local, and Regional Fusion Center Initiative to improve intelligence and information sharing within the Federal Government and across all levels of government.
- In December 2017, pursuant to its reorganization authority established in the *Homeland Security Act of 2002*, DHS created the Countering Weapons of Mass Destruction (CWMD) Office to improve DHS efforts to prevent terrorists and other national security threats from using weapons of mass destruction against the United States or its interests. The CWMD Office consolidates several offices—including DNDO and a majority of the Office of Health Affairs—into one component to better prevent, protect against, and respond to weapons of mass destruction threats.

While states and territories have made significant investments in strengthening their fusion centers, capabilities often take multiple years to build. States and territories have reported some remaining areas for improvement related to fusion centers (see **Preparedness Capability Trends: Interoperable Communications, Information Dissemination**).

Preparedness Capability Trends: Interoperable Communications, Information Dissemination

The 9/11 attacks highlighted the need for improved interoperable communications and intelligence and information sharing. Since 2014, states and territories have identified remaining gaps in their ability to accomplish various functions associated with each core capability. In 2017, 63 percent of states and territories selected *interoperable communications between responders* as a gap in ***Operational Communications***, an increase from 2014 when 55 percent of states and territories selected this functional area as a gap. Also in 2017, 44 percent of states and territories identified *disseminating intelligence and information* as a gap within ***Intelligence and Information Sharing***, an increase from 2014 when 34 percent of states and territories identified this functional area as a gap.

Hurricane Katrina

Although Hurricane Katrina was only a Category 1 hurricane when it made its first landfall in Florida, it strengthened to Category 3 by the time it made its second landfall in southeastern Louisiana on August 29, 2005, and became one of the most devastating hurricanes in the history of the Nation. The storm caused an estimated $160 billion[5] in damage and was responsible for approximately 1,833 reported fatalities. The destruction caused by the storm stretched from Louisiana and Mississippi to the western Florida panhandle. In addition to loss of life and property damage, levees in New Orleans breached and flooded at least 80 percent of the city by August 31, 2005.

Federal agencies used ICS developed in the aftermath of the 9/11 attacks to coordinate activities during response operations to Hurricane Katrina. However, the White House released the hurricane after-action report, titled *The Federal Response to Hurricane Katrina: Lessons Learned*, which identified several additional challenges in the Nation's preparedness, including:

- Lack of unified management for a national response;
- Lack of coordination in command and control mechanisms at the federal level;
- Insufficient familiarity with response plans; and
- Weak regional planning and coordination.

Preparedness Capability Trends: Unity of Effort

Hurricane Katrina highlighted a need for better unity of effort to coordinate and implement response across the Nation. Since 2014, approximately 39 percent of states and territories have consistently identified *ensuring unity of effort* as a recurring functional area gap within the ***Operational Coordination*** core capability.

To address gaps in the response to Hurricane Katrina, Congress passed PKEMRA in 2006. PKEMRA included over 300 provisions that established new authorities and clarified responsibilities to strengthen disaster preparedness. Most notably, PKEMRA codified FEMA's role as the lead agency responsible for coordinating the Federal Government's support to state, tribal, territorial, and local efforts to prepare for, respond to, recover from, and mitigate the risks of all natural and man-made disasters. PKEMRA also established the National Preparedness System and called upon FEMA to more widely use NIMS, both of which have enabled jurisdictions at all levels to increase coordination before, during, and after disasters. In addition, PKEMRA established the DHS Surge Capacity Force, a cadre of federal employees from every department or agency in the Federal Government who help to support FEMA's urgent response and recovery efforts in major disasters, including catastrophic incidents like Hurricane Katrina that are severe enough to cause staffing shortfalls. To better support people with disabilities during and after incidents, PKEMRA also created the position of Disability Coordinator. In 2010, FEMA also established the Office of Disability Integration and Coordination and has placed greater focus on integrating individuals with disabilities and others with access and functional needs into all aspects of whole community emergency management.

[5] Damage estimate adjusted for inflation to 2017 dollars.

Hurricane Sandy

Hurricane Sandy formed as a tropical storm in the southwestern Caribbean Sea in October 2012 and strengthened to a hurricane a few days later. Hurricane Sandy moved north along the east coast of the United States, eventually expanding to become the second-largest Atlantic storm on record, affecting 24 states across the Nation. Overall, Hurricane Sandy caused at least 162 fatalities in the United States and over $70 billion in damage to public and private property in the mid-Atlantic region.[6] The storm left 8.5 million customers without electricity and flooded transportation corridors along the Eastern seaboard, resulting in fuel shortages. Moreover, Hurricane Sandy damaged or destroyed at least 650,000 homes, forcing thousands of citizens to relocate to temporary shelters.

In view of the size and magnitude of Hurricane Sandy, the Federal Government built on lessons learned from Hurricane Katrina and activated the Surge Capacity Force for the first time. The Surge Capacity Force played an essential role in this large-scale deployment, contributing to response in the key areas of logistics, community relations, individual assistance, and public assistance. Despite these efforts, Hurricane Sandy revealed several challenges to response and recovery. The *Hurricane Sandy FEMA After-Action Report* identified key areas for improvement, including:

- Enhancing coordination among federal officials, first responders, and recovery personnel;
- Ensuring all survivors—including individuals with disabilities and others with access and functional needs—have equal access to services and reducing the complexity of federal disaster assistance programs;
- Improving coordination among state, local, tribal, and territorial governments; and
- Supporting qualified disaster personnel and ensuring continuity of operations.

In 2013, Congress enacted the *Sandy Recovery Improvement Act* (SRIA) to address many of the challenges associated with Hurricane Sandy response and recovery operations. In particular, SRIA addressed recovery coordination issues revealed after Hurricane Sandy when the Nation implemented the NDRF on a large-scale for the first time. For example, SRIA streamlined recovery support to survivors by creating mechanisms for greater flexibility in using federal funds related to FEMA Public Assistance, hazard mitigation, and future disaster cost reduction. The law also amended the Stafford Act to direct the President to establish an expedited and unified federal review process to improve coordination and consistency for evaluating and approving disaster recovery projects. Further, SRIA enabled federally recognized Indian tribal governments the option to request a presidential emergency or major disaster declaration.

Preparedness Capability Trends:
Equal Access to Services

Lessons learned during Hurricane Sandy in 2012 included the need to ensure equal access to services for all survivors, including individuals with disabilities and others with access and functional needs that may require additional assistance. States and territories continue to identify remaining gaps—such as ensuring equal access—in their ability to accomplish functions associated with the ***Mass Care Services*** core capability. In 2017, 41 percent of jurisdiction responses identified *ensuring access* as a functional area gap in ***Mass Care Services***, signifying an improvement in local and state capabilities in this area since 2014 when 45 percent noted this function as a gap.

[6] Damage estimate adjusted for inflation to 2017 dollars.

The 2017 Hurricane Season

The 2017 Hurricane Season saw three of the most powerful hurricanes in recent U.S. history cause extensive damage to the U.S. Gulf Coast, Puerto Rico, and the U.S. Virgin Islands. Hurricane Harvey made landfall in Texas as a Category 4 hurricane on August 26, 2017, the first major hurricane to reach the United States since Hurricane Katrina in 2005. The extreme rainfall from Hurricane Harvey caused historic flooding in Houston and the surrounding areas, resulting in the evacuation of over 40,000 flood survivors and damage to over 300,000 structures. Soon after, Hurricane Irma impacted Puerto Rico and the U.S. Virgin Islands, inflicting severe damage in both island territories, and then made landfall as a Category 4 hurricane in the Florida Keys on September 10, 2017. Hurricane Irma caused significant wind, storm surge, and flooding damage, destroying 25 percent of buildings and partially damaging an additional 65 percent of structures in the Florida Keys. Hurricane Irma continued north and made landfall on the Florida peninsula as a Category 3 hurricane on September 10. Finally, on September 20, Hurricane Maria made landfall in Puerto Rico as a Category 4 hurricane with winds of 155 miles per hour. Hurricane Maria's high wind speed, extreme rainfall, and flooding destroyed much of Puerto Rico's infrastructure and caused substantial damage to St. John, St. Croix, and St. Thomas within the U.S. Virgin Islands. Recovery efforts on the Gulf Coast and the islands will take decades.

The 2017 hurricanes offered federal, state, tribal, territorial, and local partners opportunities to continue implementing the best practices developed from response operations during Hurricanes Katrina and Sandy, such as employing ICS, positioning disability and equal rights advisors in impacted areas, and using surge staffing. FEMA mitigated staffing shortages during the 2017 hurricanes by deploying over 17,000 FEMA and Surge Capacity Force personnel both before and after the storms. However, the catastrophic scope of the 2017 Hurricane Season greatly stressed the Nation's capabilities, and provided a unique opportunity to continue assessing national preparedness and identifying areas for improvement. FEMA and its interagency partners identified several lessons learned from the incidents, including:

- Federal agencies faced difficulties understanding how and when to integrate sector-specific agencies and the private sector, both at the national and regional level, into disaster operations;
- During disaster response, FEMA and its interagency partners did not always have visibility into the process and status of state-to-state resource requests, leading to a duplication of effort and other coordination challenges;
- To overcome limited situational awareness created by the loss of communications in Puerto Rico, FEMA executed creative solutions to assess the situation and prioritize response activities, including emergency repairs to infrastructure; and
- The Federal Government created new, streamlined housing inspection procedures to reduce inspection delays.

While the response operations in 2017 were among the largest and most complex in history, lessons from these disasters show there is much more to do. Future incidents will yield additional lessons learned, underscoring the fact that national preparedness is an ongoing effort and requires continuous improvement, innovation, and action to build the capabilities needed to address the Nation's evolving risks.

Progress in Healthcare Emergency Preparedness and Response

When Hurricane Harvey's landfall caused catastrophic flooding in August 2017, the SouthEast Texas Regional Advisory Council (SETRAC)—a Houston-area healthcare coalition—was ready to respond. During the 17-day disaster event, SETRAC's Catastrophic Medical Operations Center operated as a single coordinating entity by overseeing information management, brokering requests for assistance and supplies, coordinating patient movement, and providing situational awareness across emergency response disciplines. SETRAC facilitated 1,544 patient movements, 24 hospital evacuations, 20 nursing home evacuations, and 773 health care missions.

The Hospital Preparedness Program (HPP) provided key resources, funding and training that significantly contributed to SETRAC's successful response. HPP prepares the healthcare system to save lives through the development of healthcare coalitions that include critical partners from healthcare, public health, emergency medical services, and emergency management. HPP funding enables SETRAC to conduct regular communication drills, hold regional exercises, and test preparedness and response capabilities.

SETRAC's response showed significant improvement from the region's response to Tropical Storm Allison in 2001, where the lack of a central planning body led to confusion in coordinating resources and communication between hospitals and community partners. Despite SETRAC's successful response to Hurricane Harvey, the 2017 Hurricane Season highlighted that some healthcare coalitions around the country are inconsistent in their ability to operationalize and coordinate a healthcare response to emergencies. This lesson emphasizes the ongoing need for healthcare coalitions and the value of preparing them to be response-ready entities. Opportunities exist for healthcare coalitions to model the success of SETRAC and continue to strengthen the preparedness of the nation's health care system, improve patient outcomes, and enable rapid recovery.

Building Capabilities for Catastrophic Incidents

Each year, FEMA conducts various activities nationwide to support federal, state, tribal, territorial, and local disaster readiness—including planning efforts, exercises, and training deliveries—to better prepare for catastrophic incidents. For example, in April 2017, FEMA sponsored the Gotham Shield Exercise to test the Nation's capabilities to respond to and recover from an improvised nuclear detonation in a major metropolitan area. The event included participants across the whole community, such as local and state emergency management agencies from New York and New Jersey, federal agencies, the U.S. military, and non-governmental organizations. The following infographics highlight additional efforts to improve catastrophic preparedness across FEMA's 10 regions (**Figure 12**).

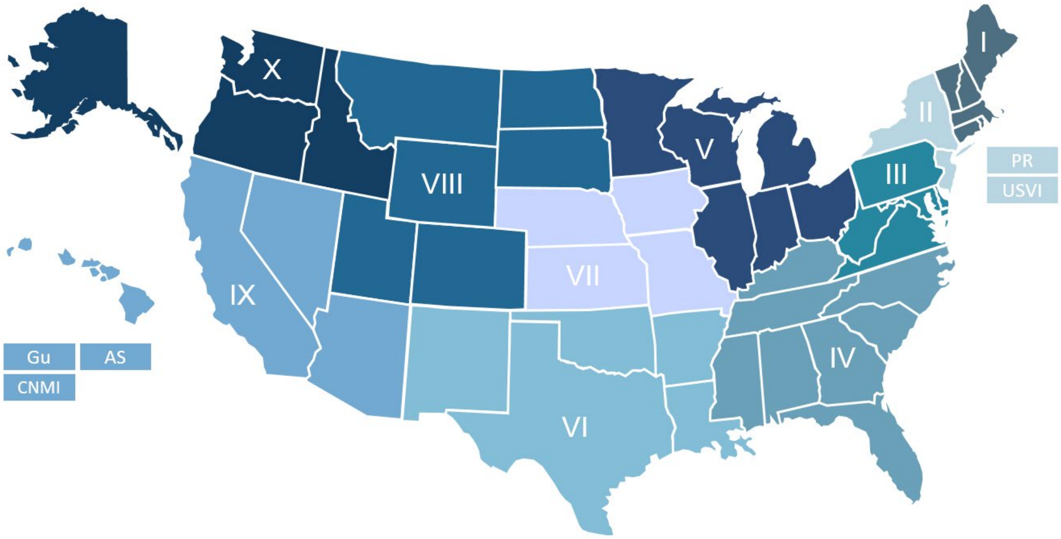
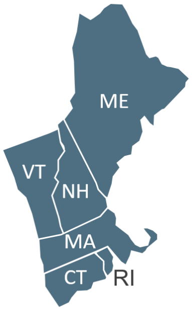


Figure 12. FEMA's 10 Regions and their efforts to improve catastrophic preparedness across the Nation.



Region I

- Conducted the Patriot Response 2017 Exercise to test preparedness for a catastrophic hurricane.
- Hosted a workshop with federal, state, tribal, territorial, local partners, and non-governmental organizations to enhance recovery capabilities for large-scale incidents.

Region II

- In addition to the Gotham Shield Exercise, FEMA supported the Vigilant Guard 2017 Exercise with DoD and U.S. Virgin Islands Territorial Emergency Management Agency partners to test response to a hurricane/tsunami scenario.

Region III

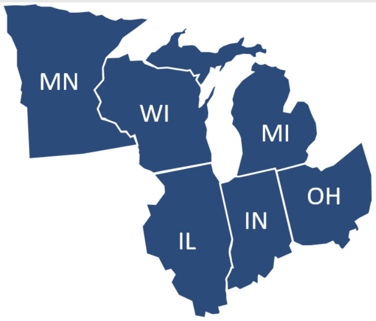
- Completed an update to the Region III All-Hazards Plan to include response to an improvised nuclear device, radiological dispersion device, and fixed nuclear facility incident.
- Developed a Geographic Information System (GIS)-based tool to rapidly support response efforts in the event of a no-notice catastrophic incident.

Building Capabilities for Catastrophic Incidents

KY
NC
TN
SC
GA
MS
AL
FL

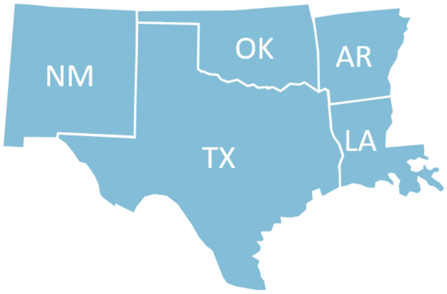
Region IV

- Supported the U.S. Navy's annual Emergency Preparedness Hurricane Exercise to evaluate preparedness for weather hazards in coastal regions.
- Developed various plans and strategies to better execute sheltering and housing operations during a significant disaster.
- Completed its Biological Incident Annex, which included planning for widespread pandemic incidents.



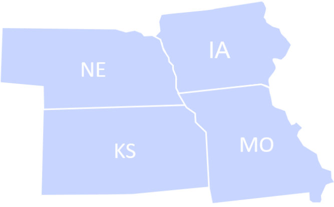
Region V

- Hosted workshops to discuss the impacts of a long-term power outage across the region.
- Tested response capabilities to a hurricane scenario in the Eastern Caribbean during a joint exercise with FEMA Region II.
- Participated in the 2017 Eagle Rising National Logistics Full Scale Exercise, an effort to test incident management and resource coordination across the Nation.



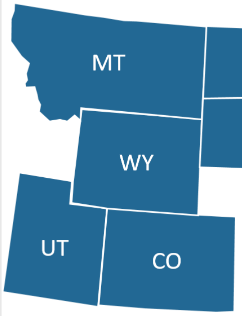
Region VI

- Became the first FEMA region to receive Emergency Management Accreditation Program certification, a voluntary process to build strong emergency preparedness programs.
- Hosted the 2017 Hurricane Charlie State Exercise Series to test Texas' ability to evacuate citizens, develop relationships among whole community partners, and identify lessons learned for continuous improvement.



Region VII

- Revised the Missouri-FEMA Region VII joint operations plan to respond to a New Madrid Seismic Zone Earthquake, scheduled for release in 2018.



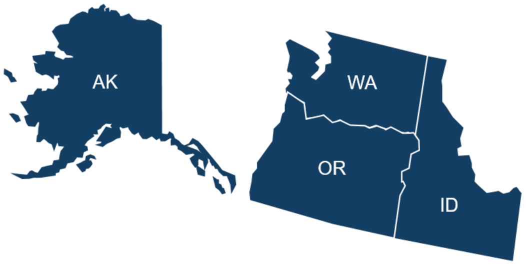
Region VIII

- Supported a total of 28 training courses to prepare staff to respond and recover from a catastrophic incident.
- Developed the National Mass Care Exercise to test and develop strategies for sheltering, mass feeding, evacuation, bulk distribution, and family reunification.

Region IX

- Completed joint catastrophic hurricane/typhoon plans with Guam and the Commonwealth of the Northern Mariana Islands and participated in the annual Typhoon Pakyo Exercise.
- Following an erroneous missile alert in 2018, Hawaii conducted a comprehensive review to identify lessons learned and recommendations to better implement alert and warning systems.
- Conducted Vigilant Guard in 2017, a radiological/nuclear detection, interdiction, and consequence management full-scale exercise in the Bay Area.

NV
CA
AZ
HI
Gu
CNMI
AS



Region X

- Based on lessons learned during the 2016 Cascadia Rising Exercise, delivered the Fractured Grid Exercise Series to increase awareness of potential risks, vulnerabilities, and impacts related to energy infrastructure caused by space weather.
- Provided training to strengthen the capacity of tribal governments across the region to plan and respond to area incidents.

Persistent Preparedness Challenges

Each prior *National Preparedness Report* has identified a set of core capabilities as national capabilities to sustain and areas for improvement based on analyses of the report's key findings, State Preparedness Report results, exercises, preparedness grant funding allocations, and future trends affecting preparedness (See **Methodology Overview: Persistent Preparedness Challenges** and **Appendix C: Research Approach**). This 2018 *National Preparedness Report* presents a revised approach, providing an in-depth evaluation of five core capabilities identified in previous reports as facing persistent preparedness challenges. These five core capabilities include one that was previously identified as a capability to sustain, and four that have been identified as areas for improvement almost every year since 2012.

Methodology Overview: Persistent Preparedness Challenges

The 2018 *National Preparedness Report* focuses on one core capability that has been identified as a capability to sustain and four core capabilities that have been identified as areas for improvement. To be a capability to sustain, the Nation must show proficiency in executing that core capability, but there must also be indications of a potentially growing gap between the future demand for, and the performance of, that capability. To select areas for improvement, FEMA evaluates each of the core capabilities against a set of preparedness indicators. **Appendix C: Research Approach** provides additional details on these methodologies.

Operational Coordination

The Operational Coordination core capability was identified as a capability to sustain in 2015 and 2017. The Operational Coordination core capability establishes and maintains a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of all core capabilities. As a cross-cutting capability, Operational Coordination is implemented across all disaster phases, from initial response to long-term recovery. Key objectives include, but are not limited to, mobilizing critical resources, ensuring information flow, defining roles and responsibilities, ensuring unity of effort, and determining mission priorities and objectives.

Infrastructure Systems

The *National Preparedness Report* has identified Infrastructure Systems as an area for improvement every year since 2012. Infrastructure Systems spans across the Response and Recovery mission areas. During the response phase of a disaster, the Infrastructure Systems core capability focuses on stabilizing critical infrastructure assets, reducing immediate safety threats to citizens from heavily damaged infrastructure, and restoring essential infrastructure functions (e.g., electricity, water) to enhance ongoing response operations. As incident response transitions into recovery, Infrastructure Systems shifts to re-establishing and maintaining systems and services to sustain community functionality.

Persistent Preparedness Challenges

Housing

The *National Preparedness Report* has assessed Housing as an area for improvement every year since 2012. Housing is a core capability in the Recovery mission area. It focuses on identifying and delivering housing solutions for displaced residents and supports long-term recovery for communities. In the short term, the core capability focuses on transitioning survivors out of emergency shelters and into interim or temporary housing. Long term, the Housing core capability aims to repair or reconstruct permanent housing and enhance the resiliency of housing inventory against future disasters.

Economic Recovery

REOPENING
DEC 1ST AT 45 W. RIVER RD. RUMSON
(ACROSS FROM BRENNAN'S DELI)
MARCH 1ST AT OUR NEW PERMANENT LOCATION
AT "BIG YELLOW" 1127 OCEAN AVE. SEA BRIGHT!
THANK YOU FOR YOUR SUPPORT
732-842-9909 / 908-489-0261 BRIAN GEORGE
NORTHSHORE

Apart from 2014, Economic Recovery has been an area for improvement in every *National Preparedness Report* since 2012. The Economic Recovery core capability, which also falls in the Recovery mission area, focuses on returning economic and business activities to a healthy state and developing new business and employment opportunities after disasters. The short-term phase of Economic Recovery typically lasts from six months to one year after an incident and involves delivering immediate support to help businesses reopen. The long-term phase, which can last decades after an incident, involves comprehensive planning to revitalize the local economy and to strengthen and diversify business and employment opportunities.

Cybersecurity

The Cybersecurity core capability has been a national area for improvement in every *National Preparedness Report* since 2012. As a Protection core capability, Cybersecurity protects and, if needed, restores electronic communications systems, information, and services from damage, unauthorized use, and exploitation. The continuing interconnectedness between cyber and physical systems—including transportation, electricity, and water systems—highlights the increased importance of cybersecurity. Efforts to enhance cybersecurity are conducted on a continuous basis, and stakeholders are constantly implementing and revising risk-informed guidelines, regulations, standards, and procedures to detect malicious activity and to maintain the security and reliability of electronic systems.

Through an in-depth analysis of these selected capabilities, the 2018 *National Preparedness Report* focuses on areas that the whole community needs to address to have the greatest impact in strengthening and improving national preparedness. The key findings presented in the next sections review challenges across these five core capabilities, as well as lessons learned and progress made from 2012 through 2017.

Operational Coordination

In 2017, the *National Preparedness Report* identified Operational Coordination as a capability that the Nation has demonstrated proficiency in executing, but that also faced a potentially growing gap between future demand for, and performance of, the core capability. Operational Coordination spans across all mission areas and addresses actions necessary to establish and maintain a unified and coordinated structure for operations as well as processes to integrate all appropriate stakeholders. Between the 2012 and 2017 State Preparedness Report submissions, 23 states and territories declined in proficiency, 20 improved, and 13 remained at the same level of proficiency.

Operational Coordination is crucial to the successful execution of the remaining 31 core capabilities of the *National Preparedness Goal*. In 2017, 85 percent of states and territories rated the capability as a high priority in their State Preparedness Report submissions. Despite its identification as a high priority, State Preparedness Report results highlighted a decrease in the percentage of states and territories reporting proficiency in Operational Coordination each year from 2015 to 2017 (**Figure 13** and **Figure 14**). Lessons learned from recent disasters reflect the continued importance of strengthening coordination structures and processes to quickly act, streamline efforts, and enhance situational awareness. The following key finding summarizes ongoing challenges and initiatives in Operational Coordination.

State and Territory Perspectives

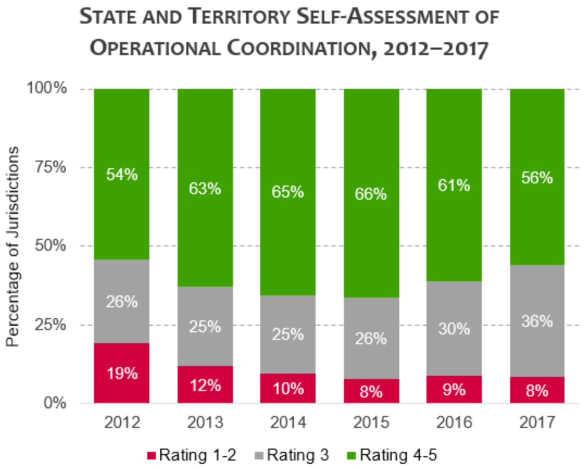


Figure 13. Since 2015, fewer states and territories have reported proficiency (indicated by percentage of 4 and 5 ratings) in Operational Coordination.

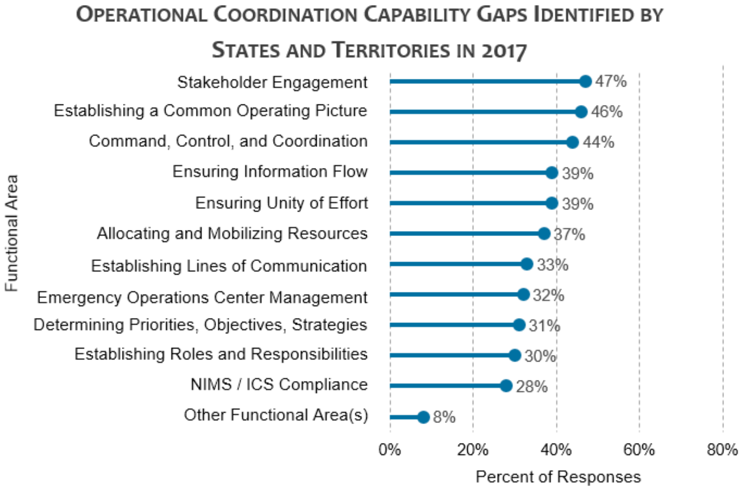


Figure 14. Since 2014, states and territories have identified functional gaps in their annual State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from national preparedness doctrine.

Operational Coordination

Key Finding:

The Nation is advancing the implementation of a National Incident Management System (NIMS), but significant challenges remain in implementing the system during large-scale events in incident command, resource management, staffing, and communications.

Emergency managers and whole community partners use NIMS to deliver a common, unified approach to sustain, manage, and deliver the core capabilities (see **Overview of NIMS**). NIMS, established in 2004, provides the whole community with a common framework for incident command and coordination, resource management, and communications and information management. In 2017, federal, state, tribal, territorial, and local partners worked together to update and expand incident management guidance and tools to advance coordination and interoperability in the Nation. These initiatives include:

- **Revised 2017 NIMS:** The updated NIMS incorporated over 3,000 comments from whole community partners—including state, tribal, territorial, and local governments; non-governmental organizations; and private citizens—that reflected lessons learned from exercises and real-world incidents, best practices, and changes in national policy. The update clarifies that NIMS applies to more than just on-scene responders—it applies to all incident personnel, including senior leaders, elected officials, and those serving in Emergency Operations Centers (EOCs).

Overview of NIMS

NIMS is a comprehensive, national approach to incident management that provides whole community partners with shared vocabulary, systems, and processes that facilitate collaboration and coordination during disasters and emergencies. NIMS is applicable to national, state, tribal, territorial, and local governments, as well as the private sector and nonprofit organizations, and provides a template for the management of incidents regardless of size, scope, or cause. Consistent application of NIMS enables responders at all jurisdictional levels and across disciplines to work together when responding to disasters.

- **The National Qualification System (NQS):** NQS aims to assist stakeholders, such as local and state emergency managers, in qualifying personnel to ensure interoperability when disaster strikes. The system provides guidance and minimum qualifications for national incident workforce personnel. NQS promotes communication and coordination by establishing a common language for defining emergency management titles, allowing for jurisdictions and organizations to plan for, request, and have confidence in the capabilities of personnel deployed from any location or agency.
- **New NIMS-typed Resources:** NIMS provides guidance on how to type resources so jurisdictions can use a common language to describe resources' capabilities. A public Resource Typing Library Tool (RTLT) provides a database of typed resource definitions for incident operations and mutual aid coordination. In 2017, there were 193 documents added to the library, bringing the total to 463 resource documents for the Nation. Over the past three years, states and territories reported that more than 55 percent of sub-jurisdictions typed and inventoried their response and recovery resources using NIMS each year.[7]
- **Advancing the Emergency Management Assistance Compact (EMAC):** EMAC defines a non-federal, state-to-state system for sharing resources across state lines during an emergency or disaster. The compact provides a process that allows states to send resources—including personnel, equipment, or commodities—to other states. Emergency managers from local, state, and federal agencies convened an EMAC Summit in August 2017. Summit participants identified several initiatives to improve the resource request process between state and federal jurisdictions, including better integrating resource typing into EMAC reporting and operationalizing deployment of the NQS to improve the efficiency of mutual aid processes.

EMAC by the Numbers

Fifty-four out of 56 states and territories have enacted legislation to become EMAC members. Over 2014–2017, 41 states and territories provided aid, and 26 states and territories received aid, according to available data. In addition, states and territories made **237 EMAC requests** for **3,292 personnel, 3,006 pieces of equipment, and 160 teams**.

Despite these developments, lessons learned from 2017 incidents highlight several ongoing challenges with the following NIMS elements: incident command, resource management, staffing, and communications.

[7] FY 2017 results do not include data from four states.

Incident Command

The magnitude of the 2017 Hurricane Season required coordinated response and recovery efforts across state, tribal, territorial, and local governments; federal agencies; nonprofit organizations; and the private sector. For example, FEMA partnered with other federal agencies and the private sector to move resources, such as generators and bucket trucks, from the mainland United States to Puerto Rico and the U.S. Virgin Islands. FEMA also coordinated with the governments of Puerto Rico and Florida and nonprofit partners to maintain a warehouse in Florida to consolidate resources before shipping them to Puerto Rico. In Puerto Rico, FEMA took a more active role in coordinating whole community logistics operations to deliver resources to disaster survivors. Additionally, in support of state, tribal, territorial, and local response efforts to Hurricanes Irma and Maria, FEMA transitioned its internal incident management from regional to national control. According to FEMA guidance, transitioning incident support responsibilities helps facilitate resource planning, create unity of command, and apply regional resources to incident management needs more effectively. While this transition is frequently exercised and leadership communication performed according to the guidance, confusion existed between regional and national incident command staff on roles and responsibilities. Stakeholders reported there were times when it was not clear which department or agency was best suited to carry out a task.

Local governments also reported challenges with incident command and coordination during the 2017 Hurricane Season. For example, a Hurricane Harvey after-action report by Harris County, Texas, noted that public safety officials were not able to share search and rescue dispatch information across agencies, which led to response agencies conducting operations under their own organizational structure—rather than a unified response structure—creating duplication of effort, as well as command and control issues. Local and state governments have engaged in efforts to improve coordination, such as working from the same location. For example, Florida officials reported that Hurricane Matthew in 2016 served as the first test that fully integrated the EOC between numerous entities and over multiple operations, leading to improved coordination and situational awareness during response efforts. For instance, emergency medical services staff in Flagler County, Florida, were assigned to the EOC, leading to improved medical coordination and planning. Similarly, during Hurricane Irma in 2017, officials from Naples, Florida, reported that co-location of representatives from various agencies in the EOC—including utilities, community services, storm water, and city government entities—improved coordination during incident response.

Resource Management

The response during the 2017 Hurricane Season included an unprecedented need to coordinate resources. For example, due to the widespread geographic impacts of Hurricane Harvey, local officials in Texas needed to incorporate state and federal assets into response efforts. Despite efforts to coordinate, officials reported inadequate resource coordination and situational awareness between local, state, and federal partners. Federal agencies also conducted extraordinary resource coordination efforts during 2017. For example, the Federal Government used *Defense Production Act* authorities to expedite the delivery of critical goods and services during the 2017 Hurricane Season. Across Hurricanes Harvey, Irma, and Maria, FEMA issued 515 priority-rated contracts from August 24 to November 30, 2017. In comparison, Hurricane Katrina and Hurricane Sandy each had one priority-rated contract awarded. The 2017

Hurricane Season also highlighted challenges processing, mobilizing, and tracking resources during large-scale incidents. The Federal Government faced challenges coordinating, moving, and delivering supplies to Puerto Rico and the U.S. Virgin Islands due to the geographic distance from the mainland United States, widespread transportation infrastructure outages, and immediate resource needs that exceeded locally stored supplies. For example, distribution activities following Hurricane Irma created an immediate deficit of local commodities, requiring the transport of additional items in the days immediately prior to and following Hurricane Maria's landfall. FEMA also worked extensively with private-sector entities, non-governmental organizations, and other federal agencies such as DoD to coordinate air and maritime transportation to repeatedly move commodities roughly 1,000 miles between the mainland United States to Puerto Rico. However, the distance and widespread infrastructure damage to Puerto Rico's seaports, airports, and roads increased transit times for resources. The U.S. Army Corps of Engineers (USACE) reported similar challenges delivering resources such as generators, equipment, and repair materials. FEMA's system to track resources was not interoperable with systems of federal and state partners, associated voluntary agencies, and private-sector vendors, limiting situational awareness. Limited training and guidance on the resource request process led to some delays in processing certain requested activities and resources.

Staffing

The 2017 disaster season also identified challenges and opportunities to test innovative approaches to mobilizing and deploying emergency management personnel across multiple, concurrent disasters. FEMA faced a shortage of qualified and trained staff, leading to inefficiencies in carrying out response and recovery programs. As part of the Federal Government's response, FEMA deployed over 17,000 personnel, and nearly 14,000 staff from DoD operating under the Defense Support of Civil Authorities process. To address disaster workforce staffing shortages, FEMA also augmented its incident workforce with local and state emergency management personnel. Personnel from four non-impacted states—Iowa, New Hampshire, Utah, and Massachusetts—were deployed to support FEMA personnel in Puerto Rico, Texas, Florida, and at FEMA's National Processing Service Center. SBA also utilized the Surge Capacity Force to supplement its disaster workforce with employees from other federal agencies. Similarly, in 2017, over 15,000 local and state incident management personnel supported disaster operations through state-to-state mutual aid agreements. Other federal agencies also reported limitations with workforce staffing in 2017. For example, the U.S. Forest Service and the U.S. Department of the Interior were unable to fully support hurricane response activities because its resources were committed to wildland fire missions, such as the 2017 California wildfires. Insight from these experiences will guide future efforts to further enable the NQS to more easily share personnel across jurisdictions and levels of government. These efforts will maximize the existing workforce by allowing every emergency manager and first responder to contribute, regardless of agency or jurisdiction.

Communications

Maintaining resilient communications involves continuity of communications processes, systems, and interoperability before, during and after disasters. Effective incident management relies on timely and accurate communications capabilities so that leadership and partners can fully understand the situation, collect and receive data to inform decisions and actions, and quickly communicate these activities to direct support where it is most needed. The 2017 Hurricane Season demonstrated successes and challenges in maintaining communications. For example, FEMA used crowdsourcing as an alternative information collection method to gain situational awareness on critical infrastructure, which helped responders understand the extent of damage in Puerto Rico after Hurricane Maria. However, Hurricane Maria also challenged communications needed to maintain an accurate and updated flow of information to support decision-making in Puerto Rico. Federal, territorial, and local response personnel were unable to use traditional communication platforms—

including commercial cellphones as well as web-based information management systems—to relay information regarding impacts, priorities, or resource needs from incident management teams in the field to the incident support teams and leadership in headquarters. While FEMA provided satellite phones to hospitals and municipalities in Puerto Rico, phones were not always an effective method for two-way communication due to weather impacts and user inexperience. Similarly, response officials reported communications-related difficulties in identifying the location of mass care shelters and in providing commodities. Local emergency management agencies also faced challenges communicating information—including GIS and operational weather data—across response agencies during Hurricane Harvey. For example, infrastructure impacts hindered access to e-mail and other information sharing software systems which prevented response agencies from understanding the impacts of Hurricane Harvey.

Corrective Actions

Government agencies initiated several after-action reviews and working groups in late 2017 to assess lessons learned and identify corrective actions. For example, FEMA conducted a review of the 2017 Hurricane Season with a focus on response and immediate recovery operations, and the Puerto Rico Emergency Management Agency is conducting a similar effort to better prepare for future disasters. Similarly, the Emergency Support Function Leadership Group—a national level interagency coordination body—established a corrective actions working group to discuss and implement actions to improve federal coordination and delivery of response support, such as enhancing coordination and information sharing with the private sector through the National Business Emergency Operations Center (NBEOC) and Sector Specific Agencies. Other federal agencies—such as DoD, Department of Energy (DOE), Department of Transportation (DOT), USACE, and several components of DHS—have also conducted reviews to identify lessons learned to improve future coordination efforts.

Local and State Innovations and Best Practices in Operational Coordination

- **Non-traditional Emergencies**: In response to the ongoing opioid crisis, Maryland and Pennsylvania issued statewide emergency declarations allowing the states to establish opioid crisis-focused command centers embedded in their state emergency management agencies.
- **Emergency Management Training***:* In recent years, Ohio has grown its EMAC practice to respond to the increase in the number of disasters. To help local and state officials better understand the EMAC process, Ohio developed a one-hour training course to provide information on request dissemination, resource deployment, mission ready package development, cost documentation, and reimbursements.
- **Coordination with Whole Community Partners***:* Louisiana developed a toolbox to manage volunteers and cost share tracking during disasters. This toolbox is scalable to any emergency and level of government and is available in print or online for quick reference. The toolbox outlines activities and tasks that must be completed by each entity involved throughout the disaster cycle, from pre-incident planning to the after-action report process.
- **Simultaneous Response and Recovery Planning***:* In Texas, the Harris County Office of Homeland Security and Emergency Management used a dual operational planning cycle during Hurricane Harvey. While response agencies were coordinating search and rescue missions and sheltering operations, county agencies were building the recovery plan. Due to Hurricane Harvey's widespread geographic impacts, the dual operational planning enabled areas of the county to seamlessly transition into recovery while other parts of the county were still in response operations. This ensured the most effective response and recovery operations for the residents of Harris County, Texas.

Infrastructure Systems

The *National Preparedness Report* has identified Infrastructure Systems as an area for improvement every year since 2012. Between the 2012 and 2017 State Preparedness Report submissions, 15 states and territories declined in proficiency, while 15 other states and territories improved. State Preparedness Report results also highlight a decrease in the percentage of states and territories reporting proficiency in Infrastructure Systems each year from 2015 to 2017 (**Figure 15** and **Figure 16**). The core capability focuses on stabilizing impacted critical infrastructure during and after a disaster. Infrastructure Systems has different goals for the response and recovery phases of an incident. During response, the goals include addressing immediate infrastructure-related threats to the affected population, re-establishing infrastructure services necessary for ongoing response operations, and coordinating debris removal. During recovery, the focus of Infrastructure Systems is on the long-term restoration of essential services and planning for infrastructure redevelopment and strengthening of infrastructure resilience.

Damage to critical infrastructure can have catastrophic consequences for response and recovery activities and can lead to other hazards. For instance, Hurricane Sandy caused power outages that forced some hospitals in affected areas to evacuate, which reduced medical services to survivors. Similarly, Hurricane Harvey stalled over parts of southeastern Texas resulting in flooding and weather conditions that temporarily closed ports, airports, and roads, and prevented access to the disaster area. Hurricane Maria destroyed the cellular networks that emergency personnel typically use to communicate with each other, which hindered their ability to coordinate response and recovery efforts. The following key findings describe ongoing challenges in Infrastructure Systems.

State and Territory Perspectives

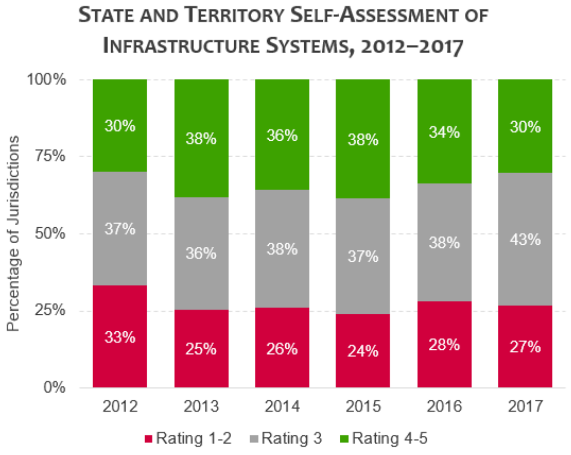


Figure 15. Since 2015, fewer states and territories have reported proficiency (indicated by percentage of 4 and 5 ratings) in Infrastructure Systems.

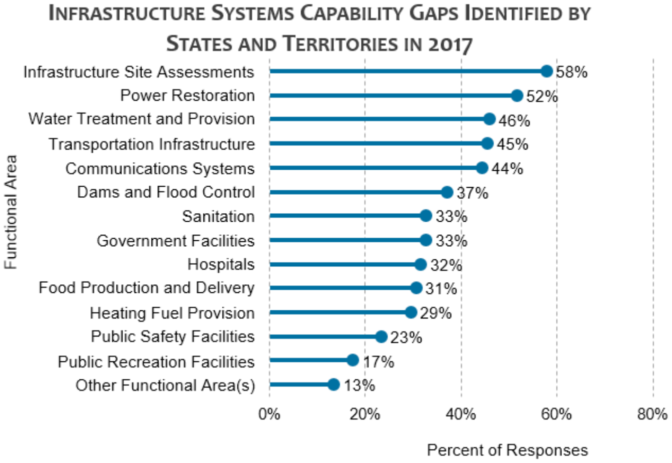


Figure 16. Since 2014, states and territories have identified functional gaps in their annual State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from national preparedness doctrine.

Infrastructure Systems

Key Finding:

Interdependencies between energy and other infrastructure systems present challenges in response and recovery; efforts to mitigate disruptions and to help communities learn from and plan for these challenges are growing.

Critical infrastructure systems often depend upon one another to function properly, which increases the likelihood of simultaneous disruptions across multiple systems during disasters. Critical infrastructure assets have become more interdependent over time. In addition, the connection between cyber and physical infrastructure creates the potential for a more serious vulnerability today than in the past, since physical systems are increasingly integrated with computer networks and the Internet. Cyber incidents can have the same effect as a natural disaster in disrupting infrastructure systems. Interdependencies involving energy infrastructure have particularly significant implications for response and recovery, since nearly all critical lifeline sectors—including healthcare, transportation, communications, and water and wastewater—rely on energy to function.

What is Critical Infrastructure?

Critical infrastructure sectors are those that are so vital to the Nation that failure in these systems would have a devastating effect on security, the economy, and public health. *Presidential Policy Directive 21* defines 16 discrete critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation
- Water and Wastewater

In Puerto Rico, the 2017 Hurricane Season demonstrated the cascading effects resulting from disruptions to the power grid. The damage to the energy infrastructure by Hurricane Maria (and, to a lesser extent, Hurricane Irma) was unprecedented. When Hurricanes Irma and Maria hit Puerto Rico, the territory was burdened with $74 billion of debt and an economy that had contracted nearly 15 percent over the last 10 years. Puerto Rico's financial crisis before the storm limited its ability to invest in and maintain its critical infrastructure, including the power grid. As a result, the storm caused extensive damage to Puerto Rico's electric transmission and distribution systems, disrupting power and negatively affecting nearly all citizens and local businesses that relied on electricity. The scale of damage to the electric grid necessitated a coordinated effort between USACE, the Puerto Rico Electric Power Authority (PREPA), DOE, FEMA, USDA, and private-sector industry partners to facilitate restoration. A report published by the New York Power Authority, PREPA, Puerto Rico Energy Commission, and several other entities and stakeholders, estimated the cost of rebuilding Puerto Rico's electrical grid will total $17.6 billion. After Hurricane Maria, USACE also conducted its largest temporary power mission ever in the United States. In October 2017, only 10 percent of Puerto Ricans had restored power. That number had risen to over 60 percent by January 2018 and 90 percent by March 2018. Immediately following Hurricane Maria, many hospitals were forced to operate without grid power. For example, nearly two weeks after Hurricane Maria made landfall in Puerto Rico, only nine out of 68 hospitals were running on grid power. In addition, nearly six weeks after the storm many hospitals were still operating at reduced capacities due to power limitations and damages. Lack of power also impacted individuals on power-dependent equipment, such as power wheelchairs, in-home dialysis, and oxygen concentrators. Prior to landfall, HHS emPOWER Program Medicare claims data identified approximately 30,633 individuals in Puerto Rico on power-dependent equipment, which are predominately older adults.

Puerto Rico also struggled to rebuild its water and wastewater services, which had stopped functioning due to the severe damage to the electrical grid. In early November, two months after Hurricane Maria hit, approximately a third of households (or about one million citizens) did not have reliable drinking water at home. The delay in restoring water system service was partially due to generators running out of fuel or breaking down, which resulted in some water systems not functioning. Moreover, the lack of power and fuel constraints limited responders' ability to conduct critical debris removal activities beyond daylight hours in the early phases of response. Significant amounts of debris impeded access to affected areas and caused delays to power restoration, which led to cascading impacts on the delivery of response and recovery services. For example, long-term power outages resulted in setbacks to the delivery of food assistance benefits to survivors in Puerto Rico since the primary methods of delivering these benefits—such as electronic benefit transfers—relied on electricity to function.

Hurricanes Irma and Maria also caused power disruptions in the U.S. Virgin Islands. The government of the U.S. Virgin Islands was already struggling with significant debt prior to the storm, an issue now exacerbated by the cost of infrastructure recovery. The Governor has estimated that repairing the power grid could cost about $385 million, and that strengthening its resilience to future storms could require an additional $850 million. The storm left about 90 percent of residents without electricity in September 2017. In addition, recovery officials were particularly concerned about access to safe drinking water due to inoperable water treatment systems. Further, without operational systems, hazardous materials spills can contaminate water and lead to illness when used for drinking and bathing. The lack of power and water also prevented public schools from operating. The schools on St. Croix and St. Thomas in the U.S. Virgin Islands did not reopen until October 24, 2017, and schools could not always run air conditioning as they were operating on generator power. Power disruptions also led to the evacuation of 781 individuals who could not receive their life sustaining dialysis treatments that rely on power. As of January 2018, USACE installed 180 generators across the three main U.S. Virgin Islands, providing temporary power to critical infrastructure such as schools, police stations, fire stations, wastewater treatment plants, water pump stations, and hospitals.

Although the Gulf Coast states and tribes affected by Hurricanes Harvey and Irma did not experience the same severe damage to electrical infrastructure as did Puerto Rico and the U.S. Virgin Islands, more than 300,000 Texans and over six million customers in Florida (59 percent of the state's total) were left without power during the peak of the outages. In addition, although a majority of Florida's hospitals sustained minimal damage from Hurricane Irma, power outages caused many hospitals, nursing homes, and medical centers to operate on generator power. Further, power outages challenged the ability of healthcare facilities to access and share information on operational status and power needs. Hurricane Harvey also caused significant infrastructure damage to major ports in the Texas Gulf Coast and Florida, impacting the fuel supply and distribution across the region.

Federal departments and agencies have launched efforts to provide information and tools that will enable communities to strengthen the resilience of the power grid. Enhancing energy sector resilience reduces vulnerability to disruptions that natural disasters or cyber incidents can cause. This, in turn, mitigates damage to electrical infrastructure and allows critical lifeline sectors that are dependent on the power grid to resume normal operations more quickly after a disaster. Notable federal initiatives include:

- USACE developed the Emergency Power Facility Assessment Tool (EPFAT) in 2013 to speed the process of installing generators following major disasters. Infrastructure owners and operators can use the online tool to upload information on the system requirements for installing generators at public critical infrastructure facilities throughout the Nation. The availability of pre-installment assessment data in advance of an incident helps first responders provide power to affected citizens more quickly. Critical infrastructure owners and operators have conducted approximately 1,000 assessments in EPFAT, and USACE added an additional 2,800 facilities into EPFAT from facility assessments conducted in Texas, Florida, the U.S. Virgin Islands, and Puerto Rico during the 2017 Hurricane Season.

- Through its Resilient Electric Grid Program, DHS partnered with private company American Superconductor (AMSC) to develop a new superconductor cable that mitigates disruptions to the power grid by connecting multiple urban substations, thus creating several paths for electricity to flow if one of the substations loses power. DHS and AMSC piloted the cable project in Chicago in 2015–2016, and continued to monitor the cable's performance for one additional year after the conclusion of the pilot.
- In March 2016, the U.S. Environmental Protection Agency (EPA) released the Power Resilience Guide for Water and Wastewater Utilities to help increase resilience to power outages. The guide provides information and case studies from water utilities, electric utilities, and other federal agencies in the following seven areas: communications, power assessments, generators, fuel, energy efficiency, on-site power, and funding.
- In 2017, FEMA released a guidance document titled *Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage*, which describes federal responsibilities for providing response and recovery support to state, tribal, territorial, and local areas in the event of a power outage so severe that utility companies cannot restore electricity in a timely manner. The document also describes the cascading effects on critical lifeline sectors caused by a mass power outage, as well as the roles that electricity providers play in restoring and distributing electricity after an incident.

Federal agencies held several exercises in 2017 to address power resiliency and interdependencies. In April 2017, DOE, FEMA, and the nonprofit Electric Infrastructure Security Council hosted the Emergency All-Sector Response Transnational Hazards Exercise to validate federal capabilities to address a large-scale, long-term power outage affecting multiple states and millions of customers. The exercise helped identify strengths and areas for improvement in the Nation's resilience to long-duration disruptions to energy infrastructure. In early 2017, DOE also hosted Clear Path V in Houston, Texas, bringing officials together across all levels of government and the private sector. The exercise examined response across and interdependencies between electricity, oil and natural gas, and communication sectors during a major hurricane impacting the Gulf Coast. Relationships and lessons learned from Clear Path V better prepared these sectors to coordinate and respond to Hurricane Harvey in 2017.

Key Finding:

The whole community has taken steps to increase the resilience of infrastructure, but challenges remain.

Infrastructure systems face deterioration and potential performance and reliability issues due to several factors such as system age, design, construction, and maintenance issues. For instance, most drinking water pipe systems in the United States date back to the mid-20th century and were designed to be functional for 75–100 years, which means many of them are nearing the end of their serviceable lifespan. Human, environmental, organizational, and industry factors can also play a role in the complex chain of events leading to infrastructure failure. For example, in February 2017, flooding caused the primary spillway of California's Oroville Dam—already damaged by erosion—to become structurally compromised, threatening a potential spillway failure and causing the evacuation of over 180,000 people. An independent assessment by the Association of State Dam Safety Officials and the United States Society on Dams found that there was no single root cause of the incident. Instead, a concatenation of factors contributed to the incident.

Infrastructure Systems

Infrastructure deterioration exacerbates the damage that systems sustain during disasters, which has severe and negative consequences for both incident response and long-term recovery. The longer it takes to restore essential services to a community, the more prolonged the post-disaster recovery process. For instance, how quickly a jurisdiction can get power and transportation systems up and running directly affects the time it will take to restore essential social services functions that rely on those systems, such as education and public health. Activities to strengthen the resilience of infrastructure—for instance, constructing stronger bridges or designing structures according to modern building codes—reduce these risks. These activities also decrease the damage disasters can cause and the likelihood of fatalities.

Emergency Relief for Transportation Infrastructure

After Hurricane Sandy in 2012, the Federal Transit Administration (FTA) established the Emergency Relief Program to help states and public transportation systems access the funding needed to protect, repair, and replace infrastructure damaged by a disaster. The program enables FTA and DHS to coordinate funding for public transit providers. The Emergency Relief Program provided over $10 billion to Hurricane Sandy transit response, recovery, and resilience projects. For example, the New York Metropolitan Transportation Authority used Emergency Relief funding for a rehabilitation project to address Hurricane Sandy damages to the Canarsie Tunnel. In addition, the program facilitated deployment of personnel to conduct damage assessments of transit assets in the areas affected by Hurricanes Harvey, Irma, and Maria in 2017.

Since 2012, the Federal Government and non-governmental partners have launched widespread efforts to improve research on and solutions for improving infrastructure resilience:

- DoD, in partnership with DOE, DHS, and five of the National Laboratories, launched a four-year pilot project in 2011 to develop and demonstrate new microgrid projects focused on enhancing electrical grid resiliency. The projects—which took place on military bases—successfully demonstrated system reliability and efficiency, including reduction of cyber vulnerabilities.
- In 2014, the Federal Government established the Sandy Regional Infrastructure Resilience Coordination Group to apply lessons learned from Hurricane Sandy to large-scale regional infrastructure projects. As of 2016, the group had created a database of federally supported infrastructure projects, which enables members to generate maps showing which projects require interagency coordination. Jurisdictions have also noted that the group has served as a helpful forum for coordinating complex infrastructure projects.
- The Federal Highway Administration (FHWA) conducted 19 state and local pilot projects from 2010–2015 to further research ways to improve the resilience of transportation infrastructure, including roads and bridges. The pilots helped states and territories develop new approaches to strengthen their infrastructure assets. For example, FHWA helped the Iowa Department of Transportation create a methodology to conduct vulnerability assessments of bridges and integrate that information into monitoring and alert systems.
- In 2016, DHS rolled out the Infrastructure Development and Recovery Program to provide critical infrastructure protection and recovery guidance, expertise, and other educational resources to communities. As of December 2016, DHS completed pilot projects to inform planning and resilience strategies in Alabama, California, and Colorado.

However, major obstacles remain in maintaining and increasing the resilience of infrastructure systems for both the private and public sectors. The private sector owns and operates a majority of all U.S. critical infrastructure assets, which creates challenges with information sharing and coordinating infrastructure resilience efforts with the Federal Government. In addition, funding remains a significant barrier to strengthening infrastructure. ASCE estimated in 2017 that an additional

10-year investment of $2 trillion more than the current level of investment is necessary to maintain a good state of repair for all infrastructure systems nationwide. Similarly, a 2013 report by the EPA estimated that an investment of $384 billion over 20 years would be required for water systems alone to continue functioning in the long term. Local, state, and federal governments already spend hundreds of billions of dollars on infrastructure every year, with the large majority of funding going to operations and maintenance.

In response to these ongoing funding challenges, federal departments and agencies have launched innovative mechanisms for encouraging infrastructure investments:

- In 2015, EPA established the Water Infrastructure and Resiliency Finance Center, whose mission is to offer resources to local and state governments, as well as the private sector, to access federal grants for water infrastructure. Through the Center's website, stakeholders can access finance webinars, technical assistance programs, and information on water infrastructure affordability programs.
- DOT launched the Build America Transportation Investment Center—a hub that enables stakeholders to better integrate federal guidance and programs into resilient transportation infrastructure projects.
- USDA created the Rural Opportunity Investment Initiative in 2015 to help communities obtain private-sector funding in addition to existing USDA grants to support essential infrastructure projects in rural areas, such as water treatment and wastewater management systems. USDA also launched a public-private collaboration initiative to increase funding for rural infrastructure, which created a $10 billion investment fund for infrastructure projects.

The 2017 Hurricane Season highlighted the continuing challenges deteriorating infrastructure poses to response and recovery. For example, Puerto Rico and the U.S. Virgin Islands were already facing decaying energy and transportation infrastructure, dams, ports, hospitals, and water treatment systems before Hurricanes Irma and Maria. The already fragile nature of infrastructure on these islands, which were among the areas hit hardest during the 2017 Hurricane Season, exacerbated the extent of the resulting damage. The National Oceanic and Atmospheric Administration (NOAA) included Hurricanes Harvey, Irma, and Maria in its "Billion-Dollar Weather and Climate Disasters"—the highest number of hurricanes to appear on that list in a single year since 2008. Texas departments and agencies submitted a request for $61 billion in federal assistance to repair public infrastructure after Hurricane Harvey. Similarly, research firm Moody's Analytics estimated that Hurricane Irma caused $12 billion in infrastructure damage in the United States. Meanwhile, HUD allocated nearly $7.4 billion of CDBG-DR funds appropriated in 2017 to support long-term recovery efforts in Texas (over $5 billion), Puerto Rico and the U.S. Virgin Islands (nearly $1.75 billion in total), and Florida (nearly $616 million). As part of infrastructure restoration activities, grantees can use CDBG-DR funds to harden electrical infrastructure against future hazards.

Housing

Similar to Infrastructure Systems, the *National Preparedness Report* has identified the Housing core capability as a national area for improvement every year since 2012. State Preparedness Report results show a decrease in the percentage of states and territories reporting proficiency in Housing since 2015 (**Figure 17** and **Figure 18**). Between 2012 and 2017 State Preparedness Report submissions, 19 states and territories declined in proficiency, while only seven states and territories improved. The Housing core capability focuses on implementing affordable and accessible post-disaster housing solutions that support the needs of the community and contribute to its sustainability and resilience.

Housing recovery involves multiple entities and extended timelines. Most survivors with homes damaged or destroyed by disasters will turn to insurance and personal resources to fund repairs or reconstruction. If the insurance payout does not fully cover the repair or replacement value of their home and belongings, survivors will often use savings to help fill that gap when a disaster strikes. Alternatively, financial institutions and SBA provide loans to support housing repair or replacement. Some communities can also access support from local governments, nonprofits, and philanthropic organizations to support recovery needs when insurance and private funds are not sufficient or available. Neighbors, faith-based groups, and community organizations also play major roles in communities by providing housing recovery assistance to individuals and families. In limited circumstances, federal programs may also be available to provide modest grants to meet immediate basic needs as well as low-interest loans for repairs, but these programs are not designed to provide for complete disaster recovery. Past disasters highlight several ongoing issues that continue to challenge the Nation's ability to restore housing. The following key findings summarize ongoing challenges in Housing.

State and Territory Perspectives

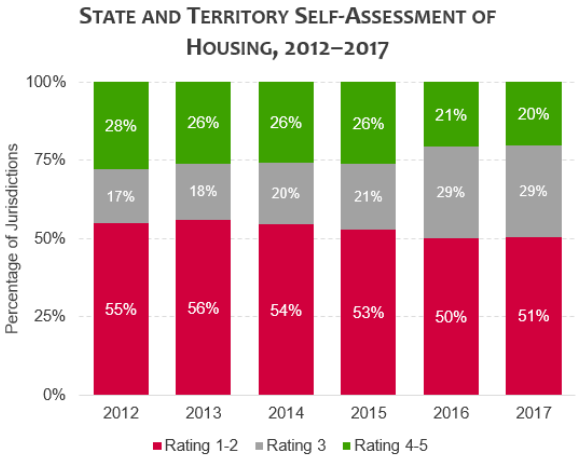


Figure 17. Since 2012, fewer states and territories have reported proficiency (indicated by percentage of 4 and 5 ratings) in Housing.

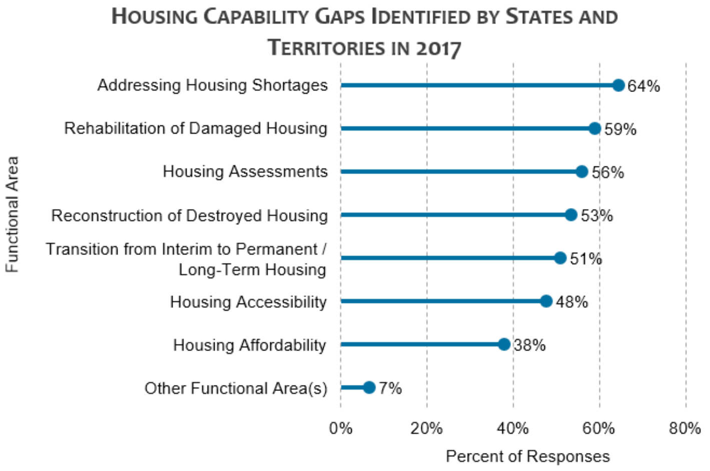


Figure 18. Since 2014, states and territories have identified functional gaps in their annual State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from national preparedness doctrine.

Housing

Key Finding:

The Nation continues to face challenges with delivering disaster housing and is exploring innovative programs to address capability gaps.

The National Disaster Housing Strategy notes that local governments have the primary responsibility for responding to and recovering from disasters with state governments fulfilling a vital supporting role. Local governments, with potential assistance from the state, lead the coordination of efforts across their communities to implement recovery plans, which includes providing disaster housing assistance to their constituents based on the scope and nature of the disaster. For example, after severe flooding occurred in Louisiana in 2016, Baton Rouge officials worked with the Louisiana Housing Corporation—the agency responsible for coordinating housing policy across the state—to deliver housing assistance programs including rental assistance, financing for housing stock restoration, and case management services for households. When appropriated, HUD CDBG-DR funding supports these locally-driven efforts by providing grant assistance to states and local governments to develop programs designed to meet their unique housing recovery needs.

Local governments face many critical challenges with organizing and providing disaster housing services and long-term housing recovery solutions. Impacts from severe disasters that span multiple jurisdictions can cause large-scale structural damages and significantly reduce the local housing supply for the short and long term. Lack of accessible housing both pre- and post-disaster can impact the ability of people with disabilities to successfully recover. Communities with insufficient housing capacity are not able to support disaster survivors that require interim and long-term housing. This can lead to temporary displacement of individuals due to a lack of available, accessible, or affordable housing options. Housing instability following a disaster can have direct impacts on the health and economic stability of a household, complicating a family's ability to quickly recover and rebuild.

Many states and territories continue to identify additional challenges with disaster housing. In their 2017 State Preparedness Report submissions, states and territories ranked Housing as the second least proficient core capability. Fifty-one percent of states and territories rated the Housing core capability as a 1 or a 2 out of 5 (a score of 5 representing the highest level of proficiency). Since 2012, Housing has ranked consistently as one of the least proficient capabilities. Approximately 50 percent of states and territories identified capability gaps in six of the Housing capability functional areas—such as conducting housing assessments, rehabilitating damaged or destroyed structures, and transitioning survivors from interim to permanent housing. Furthermore, states and territories have reported that they rely more on federal assistance to carry out disaster housing capabilities. In 2017, 53 percent of states and territories viewed Housing as mostly or entirely a federal responsibility, up from 41 percent in 2014. While some federal resources exist to support state, tribal, territorial, and local governments to implement disaster housing, many federally funded programs are temporary in nature and limited in amount and application.

The NDRF emphasizes the need for a flexible and collaborative approach to housing recovery that incorporates partners from the whole community. Aligning with this principle, communities are employing a variety of innovative engagements with nonprofit, philanthropic, and private-sector partners to address capability gaps. For example, after Hurricane Harvey impacted Houston, the Houston Chronicle reported that a nonprofit—Eight Days of Hope—began organizing a group of over 4,000 volunteers to help the city rebuild approximately 700 damaged homes. Nonprofit organizations, such as members of the National Voluntary Organizations Active in Disasters (NVOAD), regularly deploy to disasters to support communities with disaster clean up, repair and construction, and other long-term recovery efforts. For example, in Florida, over 45,000 volunteers provided approximately 1.5 million hours of support to response and recovery efforts after Hurricane Irma.

The philanthropic and private sectors also provide resources to support housing recovery. For example, after Hurricane Maria, elected officials in New York and Puerto Rico worked with a nonprofit to launch UNIDOS Disaster Relief and Recovery Program, a philanthropy to support Puerto Ricans affected by the storm. Through the program, Puerto Rico received approximately $15 million in commitments to support emergency relief and recovery projects, such as investing $100,000 to repair 200 roofs in the Caimito and Playita neighborhoods in San Juan. Similarly, the Center for Disaster Philanthropy established the Hurricane Harvey Recovery Fund, raising over $14 million to help organizations serving survivors in Texas. These local nonprofits provide a wide range of recovery support, including assistance finding temporary housing options and help rebuilding damaged structures. Help! I'm Hurting Inc., a nonprofit in Port Arthur, Texas, received funding to address the long-term recovery needs of uninsured and under-insured residents who have been unable to secure assistance with recovery needs. The private sector is also continuing to expand their role in recovery efforts. Since 2013, AirBnB has provided a tool to help displaced residents in disaster-affected communities find free, temporary lodging with existing AirBnB hosts. In the five years of this service, AirBnB has provided more than 16,000 overnight stays in over 7,400 homes to displaced disaster survivors. Local businesses are also providing support. In Houston, a local major furniture store provided shelter and meals to individuals displaced by flooding from Hurricane Harvey.

At the federal level, agencies are exploring ways to improve their support to state, tribal, territorial, and local governments with disaster housing. In early 2017, FEMA launched the Housing Assistance Initiative to enhance housing capabilities across jurisdictions and explore flexible housing solutions that align to the needs of local communities. Through the initiative, the agency implemented innovative solutions aimed at overcoming shortages of available rental resources in areas impacted by the 2017 hurricanes. These disaster housing innovations include providing direct leasing services, direct housing repair services, and recreational vehicles as temporary housing options; expediting the delivery of direct housing assistance to qualified survivors; and supporting a unique state-led housing mission. FEMA is planning to assess the impact of these solutions in the later phases of the recovery.

Key Finding:

Challenges remain with efforts to coordinate timely and efficient housing damage assessments for survivors after large-scale disasters.

Lessons from recent disasters revealed that the Federal Government faced many challenges when assessing housing damages following a large-scale disaster. After a disaster, most homeowners will look to savings and insurance to fund the repair of their homes. If insurance is insufficient to meet homeowners' repair needs, federal programs by FEMA or SBA can supplement private and state housing repair assistance. Receiving federal support begins with the homeowner or resident completing an inspection of their home to determine the needed repair services and to estimate the resources required to rebuild and reconstruct homes. However, when disasters are significant or span large geographical areas, damage inspectors may be unable to complete assessments quickly. In addition, a limited pool of available inspectors and a lack of accessible communication support (e.g., absence of a qualified sign language interpreter for a hearing-impaired homeowner) also can exacerbate delays. To meet the historically high need for inspections across all disaster-affected regions in 2017, FEMA contracted additional inspectors to supplement existing inspection staff. Still, FEMA experienced inspection staffing challenges that resulted in housing damage inspection backlogs across the Nation. For example, due to inspection delays, on October 1, FEMA advised applicants in Texas that the inspection wait time may reach up to 45 days.

The Federal Government is implementing innovative methods that reduce the timeframe of inspections and deliver assistance to eligible survivors faster. Both SBA and FEMA developed updated approaches to significantly reduce the need for in-person inspections. In 2016, SBA expanded the use of desktop reviews, which are completed using third-party resources and phone interviews with property owners rather than requiring an in-person inspection. Using desk reviews during the 2017 Hurricane Season, SBA reduced the average inspection time of a loan application to just six days, down from 12 days during Hurricane Sandy. Similarly, FEMA streamlined the inspection processes for IHP applicants by using phone calls to collect basic home damage information and then used this information to determine which applicants required an in-person inspection. In addition, FEMA reduced the time needed to complete in-person inspections by assessing overall damage to the home, rather than a line-by-line assessment of damage. Further, FEMA made immediate decisions without on-site inspections for applicants who stated they had no property damage but that their home was inaccessible or lacked essential utilities. In addition, FEMA applied remote sensing imagery and GIS data with other data to quickly assess the impacts of Hurricanes Harvey, Irma, and Maria. Specifically, in 2017, FEMA used remote sensing imagery, in coordination with open-source housing and occupancy data, to identify applicants residing in areas damaged or destroyed by the disaster. FEMA used GIS data to identify flood depths in areas within a flooding event. Employing these innovative approaches enabled FEMA to quickly identify heavily damaged areas, qualify some homeowners for housing assistance automatically, and optimize the deployment of inspection personnel.

Key Finding:

While research shows that incorporating mitigation strategies in rebuilding can yield positive benefits, limited incentives exist to encourage resilient home reconstruction after a disaster.

Incorporating resiliency—measures that improve the ability to absorb the impact of and to recover from disasters—can help build homes back stronger. Adding energy efficiency measures can further increase a home's sustainability. Resilient home construction standards and floodplain management regulations can minimize the damage and cost of future disasters for both homeowners and the government. A recent study by the National Institute of Building Sciences noted that federal mitigation grants save $6 for every $1 spent on mitigation strategies for all hazards, including riverine floods, hurricane surges, wind damage, earthquakes, and wildland-urban interface fires (see **Natural Hazard Mitigation**). Furthermore, higher building standards can, in specific circumstances, save $4 for every $1 spent on all hazards.

Building codes and regulations play a key role in promoting housing resiliency. For example, in 2001, Florida required new construction to comply with national standards for wind and flood resistance. Between 2001 and 2010, compliant homes saw a 53 percent reduction in paid insured losses from windstorm hazards. Moreover, assessments conducted after Hurricane Irma showed that Florida's statewide building code and Hurricane Loss Mitigation Program greatly decreased the overall damage to people and property. In 2017, however, the state revised its requirements for updating the Florida Building Code, changing from a full adoption of recommendations released by the International Code Council to a case-by-case adoption of only the recommendations deemed necessary. This change raised concerns that Florida's statewide code would grow weaker over time. Building codes can vary significantly by jurisdiction, which can lead to uneven implementation of housing resiliency across the Nation. For example, Texas does not have a statewide building code and allows local jurisdictions to set their own regulations.

Housing

A report by the National Institute of Building Sciences found that tenants and building owners accrue the most benefits from resilient building codes. However, property developers—who may hold initial responsibility for building design and construction—receive the smallest return on investment from costly mitigation measures, especially since they often sell the buildings after construction is complete. While mitigation measures can save communities money over the long term, developers have little incentive to make the necessary up-front investment to make their buildings more resilient to disasters.

While federal programs play a role in promoting resiliency in rebuilding and restoring damaged homes after a disaster, most federal programs do not impose resiliency requirements as a condition of receiving disaster housing assistance. For example, FEMA's Hazard Mitigation Grant Program can provide funding to individuals and other recipients that may be used to improve the resiliency of homes subject to, or in danger of, recurring damage. These improvements may include, elevating homes to protect structures from flooding and structural retrofitting to improve protection against floods, wildfires, or earthquakes. In addition, households may obtain SBA disaster repair loans to restore structures to current state building requirements. These loans can also support mitigation upgrades to structures, such as elevating a home in a flood zone. HUD's CDBG-DR program also promotes resiliency in housing reconstruction efforts, including activities that lead to restoring and improving housing stock.

Natural Hazard Mitigation

The *Natural Hazard Mitigation Saves: 2017 Interim Report*, completed by the National Institute of Building Sciences, found that federally funded natural hazard mitigation, as well as efforts to build beyond code requirements, result in national cost benefits for all hazards. For example, the Nation will ultimately save $6 for every $1 spent on up-front mitigation cost funded through federal programs. Similarly, designing new construction to exceed selected code requirements—including the 2015 *International Building Code*, 2015 *International Residential Code*, and 2015 *International Wildland-Urban Interface Code*—result in a national benefit of $4 for every $1 invested. The following table provides a detailed overview of these cost benefits for all hazards and by different hazard categories.

Hazard Type	Benefit-Cost Ratio	
	Federally-Funded	Beyond Code Requirements
Riverine Flood	7:1	5:1
Hurricane Surge	Too few grants	7:1
Wind	5:1	5:1
Earthquake	3:1	4:1
Wildland-Urban Interface Fire	3:1	4:1
All Hazards	6:1	4:1

Rebuilding Texas

In the wake of Hurricane Harvey, Texas established the Governor's Commission to Rebuild Texas, which is responsible for coordinating statewide efforts to rebuild public infrastructure damaged by the storm. Rebuild Texas serves as a one-stop shop for local jurisdictions, providing information on federal programs and advocating for citizens' interests during recovery activities. The commission partnered with public, private, and academic sector partners to identify risks to critical infrastructure and tailor mitigation planning to meet the needs of local jurisdictions. The Commission's website also directs individuals in need of housing assistance to www.texasrebuilds.com, a comprehensive repository of all housing recovery-related information for communities affected by Hurricane Harvey.

Economic Recovery

The *National Preparedness Report* has identified the Economic Recovery core capability as a national area for improvement for multiple years since 2012. Between the 2012 and 2017 State Preparedness Report submissions, 17 states and territories declined in proficiency, while 15 states and territories improved. More recently, State Preparedness Report results show a slight increase in the percentage of states and territories reporting proficiency in Economic Recovery from 2016 to 2017 (**Figure 19** and **Figure 20**). The capability focuses on the ability to return a community's economy to a healthy state following the impact of disasters or emergencies.

Natural disasters can devastate the economies of affected communities. In 2017, Hurricane Harvey impacted more than 565,000 businesses and caused an estimated $126 billion in total damages, according to NOAA.[8] In addition, storm-related rain and flooding affected rice, cattle, cotton, and sugarcane industries across Texas, Louisiana, Arkansas, and Mississippi. A study by Texas A&M University found that in Texas alone, Hurricane Harvey caused an estimated $200 million in agricultural losses. Meanwhile, NOAA reported that Hurricane Irma disrupted more than 2.1 million businesses and caused an estimated $50 billion in total damages in 2017. The Florida Department of Agriculture estimated over $2.5 billion in total agricultural losses, including cotton, broiler chicken, cattle, and egg assets. Finally, NOAA found that Hurricane Maria impacted over 18,000 businesses across Puerto Rico and the U.S. Virgin Islands, and caused approximately $90 billion in total damages in 2017. Federal and non-federal partners can coordinate resources to ensure continuity of services and support to meet the needs of affected community members who have experienced the hardships of financial, emotional, and physical impacts of devastating disasters. Past disasters highlight several challenges with restoring economic activity to a healthy state in communities. The following key findings summarize ongoing challenges in Economic Recovery.

State and Territory Perspectives

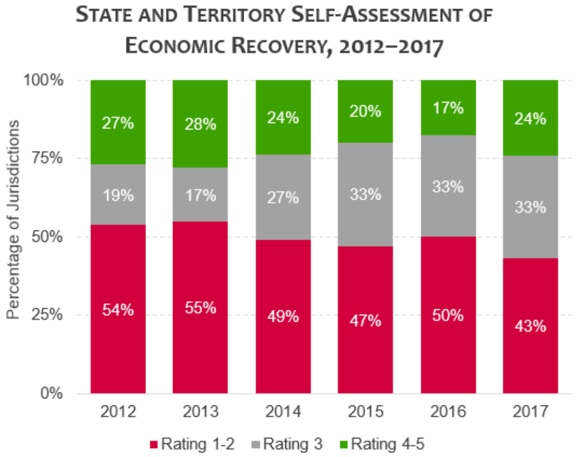


Figure 19. Compared to 2012, fewer states and territories have reported proficiency (indicated by percentage of 4 and 5 ratings) in Economic Recovery.

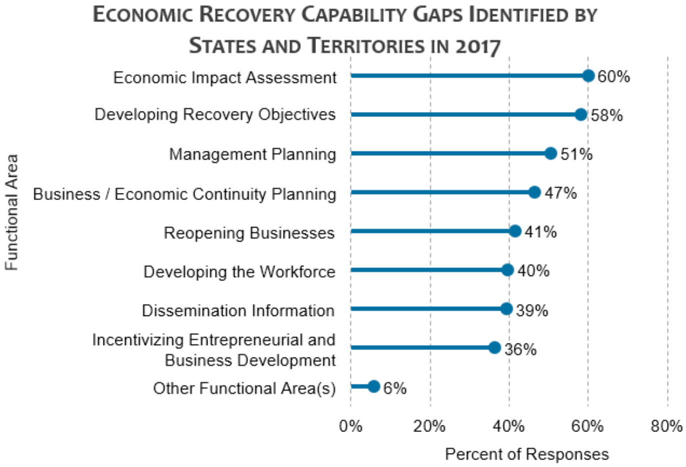


Figure 20. Since 2014, states and territories have identified functional gaps in their annual State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from national preparedness doctrine.

[8] NOAA estimates the total, direct costs of weather and climate incidents including physical damage to buildings, material assets, business interruption costs, vehicles and boats, offshore energy platforms, public infrastructure, agricultural assets, and disaster restoration and wildfire suppression costs.

Key Finding:

Partners across the whole community have engaged in recent efforts to build business planning capabilities, though many small businesses lack business continuity plans.

Building a culture of preparedness starts with individuals, communities, and businesses understanding and managing risks. Businesses that understand and manage risks through initiatives such as business continuity planning are better able to recover and restore business operations, which contributes to quickly returning a community's economy to a normal state. Business continuity planning involves an assessment of risks and identification of mitigation strategies to reduce post-disaster losses and facilitate a quick restoration of business operations. Disasters can often affect businesses in multiple ways. For example, disasters can cause damage to physical facilities, forcing businesses to temporarily or permanently suspend operations. Disasters can also displace a business' workforce and customer base, which can lead to lost income, jobs, and productivity for communities. Additionally, disasters can impact the business' supply chain. Continuity planning enables businesses to mitigate these impacts and facilitates a return of healthy economic activities in communities.

Business Continuity Planning in Oklahoma

In 2013, fewer than 30 percent of small businesses in central Oklahoma reported having continuity plans in place. Recovery efforts for a severe weather incident in May 2013 highlighted a need for pre-disaster recovery planning to prioritize economic needs and coordinate with stakeholders before an incident to better enable effective recovery efforts. To improve future small business continuity planning, the Oklahoma Small Business Development Center developed its Ready Now Small Business Survival Planning Program to assist small business emergency preparedness.

Most small businesses across America lack a business continuity plan to maintain or quickly return business operations to normal after a disaster and consequently are particularly at risk for permanent closure. For example, a 2016 survey of over 500 small business owners in the United States found that 68 percent of owners did not have a written business continuity or information technology/disaster recovery plan (IT/DR). Small businesses report several factors that hinder their ability or willingness to develop continuity plans. Many owners do not believe their businesses will be impacted by a natural disaster and therefore do not develop plans. In addition, small businesses do not perceive the development of continuity plans as a high priority compared to day-to-day operations, such as making payroll, covering rent, and paying vendors or suppliers. Additionally, while large businesses tend to have resources to conduct continuity and IT/DR planning, small businesses may not be able to expend the resources necessary to assess their risks and develop plans. To address these challenges, government and nonprofit agencies across the whole community have worked to engage businesses in pre-disaster continuity planning. Examples of recent initiatives include:

- After Hurricane Harvey impacted many small- and medium-sized businesses across Texas in 2017, IBM partnered with the U.S. Chamber of Commerce Foundation to provide continuity and IT/DR planning support to local businesses. In this capacity, IBM hosted three Texas Disaster Resiliency Workshops to help businesses implement continuity planning concepts and develop continuity plans for both current and future recovery efforts.
- The Insurance Institute for Business & Home Safety developed a severe weather emergency preparedness and response planning toolkit in 2016 to help small business owners plan before a disaster strikes. The guide enables businesses to plan for various disasters to lessen property damage and economic loss.
- In 2017, SBA provided a short guide for small businesses in its Disaster Preparedness and Recovery Plan to improve business resilience and continuity.
- In 2017, a collaborative partnership between The UPS Foundation, the U.S. Chamber of Commerce Foundation, the World

Economic Forum, and the Disaster Resistant Business Toolkit Workgroup developed the *Resilience in a Box* program to assist businesses in planning for disasters. *Resilience in a Box* provides several tools, including a Business Preparedness Checklist, Top 20 Tips for Business Preparedness, and a Business Disaster Resilience 101 Workbook that provide guidance to implement and test business continuity planning.

- DHS, the National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP), FEMA, and several large private-sector firms partnered to develop Business Continuity Planning software. The software helps companies to create actionable continuity plans against a broad range of threats, such as the impact of natural disasters, widespread serious illness, or human-caused hazards such as accidents, acts of violence or terrorism, and technology-related hazards like the failure or malfunction of systems, equipment or software. Several of NIST MEP centers have also added business continuity services to small manufacturers. In places like Iowa and New Jersey, over 50 companies have taken advantage of those services.
- FEMA's *Ready Business Program* helps small businesses and community-based organizations identify their risks, develop a plan, and act to mitigate and prepare for disasters through toolkits and local workshops. The *Ready Business Program* hosted four workshops across the Nation focusing on earthquake, hurricane, power outage, and flood risks in FY 2017.

In addition to these initiatives, U.S. Department of Commerce Economic Development Administration's (EDA) Resiliency Planning Evaluation Tool, developed in 2014, provides recommendations to improve pre-disaster economic development planning. These recommendations include promoting the development of pre-disaster business continuity plans and connecting businesses to mitigation and preparedness planning efforts.

Key Finding:

While federal agencies have made efforts to streamline disaster recovery assistance, businesses continue to face challenges navigating post-disaster economic recovery programs.

After a disaster, communities access assistance through a range of programs administered by both government and non-governmental organizations. In particular, economic assistance can provide a crucial lifeline to businesses in the wake of a disaster. Agencies across the Federal Government offer various types of economic assistance—from SBA Disaster Assistance Loans to USDA Business and Industry Guaranteed Loan Programs to HUD CDBG-DR (see **Federal Disaster Assistance to Businesses and Communities**). These programs provide businesses with sources of financial assistance to rebuild and reopen operations, enabling a community to restore employment opportunities and revitalize its local economy. For example, in response to 2017 Hurricanes Harvey, Irma, and Maria, SBA Office of Disaster Assistance approved over $6.4 billion through nearly 120,000 loans to survivors, including home and business owners as of March 20, 2018. Additionally, in February 2018, Congress appropriated $600 million to EDA in Economic Adjustment Assistance Program funds to help communities experiencing economic distress or other economic harm resulting from hurricanes, wildfires, and other federally declared natural disasters occurring in calendar year 2017.

Federal Disaster Assistance to Businesses and Communities

After a disaster, agencies across the Federal Government provide aid to businesses and communities to restore economic activity across impacted areas. These programs include:

- **EDA Economic Adjustment Assistance Program**: Provides a wide range of technical, planning, public works, and infrastructure assistance—including funding the hiring of Disaster Recovery Coordinators—to communities experiencing adverse economic impacts
- **HUD CDBG-DR:** Provides grants to communities to support economic revitalization activities such as retaining and creating jobs
- **SBA Business Physical Disaster Loan:** Provides loans to businesses and nonprofit organizations to repair or replace disaster-damaged property, including real estate, inventories, supplies, and equipment
- **SBA Economic Injury Disaster Loan:** Provides working capital loans to small businesses or private, nonprofit organizations to help cover operating expenses and financial obligations
- **USDA Business and Industry Guaranteed Loan:** Guarantees loans for rural businesses for several eligible uses, including to repair or modernize businesses and create or save jobs
- **USDA Emergency Community Water Assistance Grants**: Helps eligible communities prepare for, or recover from, an emergency that threatens the availability of safe, reliable drinking water

Economic Recovery

The variety of disaster programs can make identifying and selecting the most optimal opportunities confusing and time-consuming after a disaster. Since 2013, the Federal Government and its partners have worked to streamline delivery of programs and increase awareness and navigation of economic recovery programs for local businesses and communities. For example:

- In 2013, the Hurricane Sandy Rebuilding Task Force recognized the need to institute a "No Wrong Door" approach to ensure that businesses and the community could effectively search and access program information and resources. As a result, FEMA's Disaster Assistance Improvement Program, in cooperation with its interagency partners, launched the Community Recovery Resource portal to provide a comprehensive list of federal assistance programs and resources after a disaster.
- SBA has undertaken several efforts to improve knowledge of its disaster loan programs and increase applications for assistance. For example, SBA published a loan program reference guide in 2015 to increase awareness of available assistance and updated its Disaster Loan Assistance Portal in 2016 that provides applicants with quick and easy access to their application status, filing requirements, and document uploads. These efforts modernized loan processes, allowing SBA to maintain shorter business loan processing times in recent disaster recovery efforts such as Hurricane Matthew and the 2016 Louisiana floods. Similarly, in January 2017, SBA began conducting desktop verifications on all home disaster loan applications and most business disaster loan applications to streamline loan processing and deliver services to survivors better and faster. As a result, using desktop verifications during the 2017 Hurricane Season enabled SBA to cut the inspection cycle time in half when completing nearly triple the number of loss verifications.
- In September 2017, USDA took steps to improve its crop insurance program after Hurricane Harvey. In advance of the storm, USDA waived certain reporting requirements and fast-tracked damage compensation payments to policy holders in affected counties across Texas and Louisiana. Through this effort, USDA quickly distributed aid to local crop and agricultural-centric economies.

Business Outreach in Pioneer Valley

In the wake of Hurricane Irene and a severe snow storm in 2011, the Pioneer Valley Planning Commission (PVPC), an urban planning department in Massachusetts, reported that few known resources were available to help businesses prepare for and recover from a disaster. Based on these findings, PVPC conducted a series of outreach meetings to better understand how businesses receive information before, during, and after a disaster and to identify resources available to them. This research intends to help businesses access the information they need, including grant and loan processes in future recovery efforts.

Despite these efforts, businesses face challenges navigating federal recovery programs and remain unfamiliar with the range of programs and resources available to assist them. In 2010, the International Economic Development Council (IEDC) and National Association of Development Organizations (NADO) identified that economic development organizations, chambers of commerce, and business assistance organizations are frequently unaware of available federal programs and subsequent application requirements. In 2016, the U.S. Government Accountability Office (GAO) recommended that SBA improve disaster-related information on its web portals, such as requirements of the loan process and financial terminology used in loan applications. Since then, SBA has made improvements to better communicate information on its programs. Recent disasters also highlight challenges with federal loan programs. During the 2017 Hurricane Season, businesses in Puerto Rico reported challenges with understanding the loan application process. Without a clear understanding of loan programs, small businesses may not know key information and requirements needed to apply and may be unsuccessful in securing federal assistance. To mitigate these challenges in Puerto Rico, SBA hired, trained, and deployed over 440 personnel to staff more than 150 recovery centers to ensure better messaging of its disaster loan programs and the application process. SBA also conducted outreach with the media, chambers of commerce, federal and local stakeholders, and faith-based organizations to improve recovery efforts.

Economic Recovery

Key Finding:

Post-disaster, communities often struggle to effectively communicate and coordinate with the private sector, and efforts to address these challenges are ongoing.

Communication is essential to the process of collecting and exchanging information to inform and coordinate economic recovery efforts, such as business resumption and infrastructure restoration. Effective communication includes the appropriate stakeholders, forum, and messaging. After a disaster, key entities—such as emergency managers, business owners, the government, and private-sector representatives—communicate on economic impacts and needs. Successful partnerships between local, state, and federal partners as well as the private sector and non-governmental organizations enable communities to integrate local knowledge and resources to support post-disaster recovery. Forums, such as specialized working groups or business emergency operations centers (BEOCs), further enable these stakeholders to exchange information for situational awareness, coordinate operations, and facilitate decision-making.

Economic Recovery and Resilience Coordination in Florida

After Hurricane Irma struck Florida as a Category 4 hurricane on September 10, 2017, Florida received a major presidential disaster declaration. The Economic Recovery Support Function (RSF), led by EDA, was activated in late September to serve alongside FEMA and other RSFs in the Joint Field Office in Orlando Florida. From October 2017 through March 2018, EDA worked with several federal, state, and regional partners to support post-disaster recovery efforts. Most recently, the Economic RSF worked with the state's Regional Planning Councils, Florida Department of Economic Opportunity, the International Economic Development Council, and federal partners to host workshops that shared best practices and fostered connections among participants.

Communities can struggle to identify and convene the appropriate recovery stakeholders, including business owners, local governments, and emergency managers. Although local governments and emergency management agencies fulfill a legal responsibility to address disasters, local business owners, for example, do not readily recognize their role in local disaster preparedness and recovery. Similarly, the emergency management community is often unaware of economic development partners, which leads to disconnect before and after a disaster. Without the awareness or inclusion of these stakeholders—including economic development organizations, chambers of commerce, and business and trade associations—decision-making may not account for the potential impact on the community's economic recovery. For example, closing streets could negatively affect the workforce and economy by forcing businesses to close or driving customers and residents away.

While recent initiatives have established additional forums for communication, local officials and community stakeholders continue to report limitations with communications in the economic recovery process, including insufficient mechanisms for communicating private sector concerns upwards to official decision-makers and relaying recovery priorities downwards to business community stakeholders. Since 2012, several local, state, and federal entities have established forums to improve communication during disasters:

- In 2012, FEMA established the NBEOC to facilitate two-way information sharing and collaboration between public- and private-sector stakeholders during disaster response and recovery. The NBEOC is a network of national corporations, infrastructure owners and operators, government officials, and trade associations that have an interest in business continuity, stabilizing disruptions for disaster response and recovery, and public-private partnerships. During the response to the 2017 Hurricane Season, FEMA activated the NBEOC for over 60 consecutive days. NBEOC participants identified processes to facilitate access to impacted areas, enable business resumption, and channel awareness of private sector challenges and priorities supporting infrastructure restoration.
- In 2013, the Oklahoma Office of Emergency Management and Oklahoma Department of Commerce created the Business Emergency and Communication Optimization Network (BEACON). BEACON focuses on developing a platform for business resilience collaboration, communication, and technical assistance through several efforts, including a business toolkit for pre-and post-disaster communications, a messenger service for crisis communications, and connections to NVOAD.

- In September 2017, Puerto Rico and FEMA implemented a collaborative model based on the NBEOC to establish the Puerto Rico Business Emergency Operations Center (PR BEOC). The PR BEOC included industry representatives from 13 key economic areas as well as representatives from federal, territorial, and nonprofit entities from the Joint Field Office. The PR BEOC provided a forum for dialogue and coordination between government, business, and industry leaders to address critical concerns—such as supply chain stabilization, power restoration, and tourism revitalization—benefitting both response and recovery activities.
- In 2017, the Naples Florida Accelerator—typically focused on supporting young companies and startups—transitioned into a business recovery center in the wake of Hurricane Irma. In addition to helping businesses quickly get short-term emergency loans from the Florida Small Business Emergency Bridge Loan Program and disaster loans from SBA, the recovery center communicated information with local companies, such as when they could expect debris pickups and when water restrictions would be lifted.

Communities that have developed effective communication channels before and during a disaster are better able to connect and rapidly distribute relevant information after a disaster. However, more work is needed to improve forums to support communications between emergency management and businesses. For example, after Hurricane Maria impacted Puerto Rico in 2017, both the private sector and federal agencies identified a need for a mechanism to better communicate economic impacts and priorities across the whole community. While different agencies had particular pieces of information and insight, there was no mechanism to share this data among relevant partners. In addition, in the 2017 State Preparedness Report, 40 percent of states and territories identified disseminating information as a gap within the Economic Recovery core capability.

Creating consistent, clear, accessible, and accurate messages among multiple sources—including business owners, economic development organizations, chambers of commerce, emergency managers, and local community members—remains a challenge. A 2015 report by IEDC found that one of the biggest impediments to economic recovery is uncertainty among stakeholders, in part due to inadequate or inaccurate information. For example, if business owners do not know the status of recovery efforts, such as when key infrastructure systems will be restored or when debris will be removed, businesses may be unsure whether to reopen, rebuild elsewhere in the same community, or move to a new community. Similarly, misinformed customers can also impede a return to regular business operations. For example, after Hurricane Sandy in 2012, some media reports gave the incorrect impression that the entire Atlantic City boardwalk was destroyed.

Federal agencies have provided guidance and recommendations to improve recovery-related communications for business and local communities. EDA recommended that jurisdictions develop and distribute resource guides to communicate post-disaster recovery resources and availability, including contact information for updates on recovery efforts. Similarly, HUD recommended that local jurisdictions identify processes or mechanisms to communicate between businesses, emergency management officials, and the local community. HUD identified several potential communication systems such as 211 call centers—a dialing code reserved for community information services—and/or BEOCs to improve communication efforts. Finally, IEDC recommended that businesses establish a crisis communications plan to ensure that clear, accurate, and up-to-date messages are provided to the whole community from trusted sources.

Economic Recovery

Key Finding:

Financial disruptions from disasters can disproportionately affect less-resourced communities, prolonging their return to economic viability.

Disasters can result in lost income and financial instability, which can be particularly challenging for low-income individuals and families and prolong a community's return to economic normalcy. After Hurricane Sandy struck New York and New Jersey in 2012, unemployment insurance claims rose to over 100,000 new claims per week, significantly higher than the weekly average of 35,000. The claims remained elevated for four weeks after the storm. In 2017, Hurricane Harvey resulted in initial unemployment claims of over 65,000 in the week ending on September 2, nearly five times the level seen in the previous week. Research findings show that people of low socioeconomic status are more vulnerable to disasters and are more likely to suffer more serious consequences from their impacts (see **Impact of Disasters on Less-Resourced Communities**).

While access to financial resources has proven to be a strong predictor of how well someone can cope after a disaster, individuals across the Nation continue to lack adequate financial preparedness. For example, a 2017 Federal Reserve report found that around 40 percent of Americans do not have enough cash savings to cover a sudden unexpected expense, such as those caused by natural disasters. In addition to insufficient savings, preparedness actions—such as purchasing flood or earthquake insurance—can be costly for people with limited income. As a result, these communities can face greater losses from disasters.

Federal agencies can help minimize some of the immediate economic disruptions that disasters cause, but this assistance has limited ability to address long-term financial instability. Federal agencies often aim to address the more immediate financial needs of individuals. For example, the U.S. Department of Labor provides Disaster Unemployment Assistance (DUA) to eligible individuals unemployed as a direct result of a presidentially-declared major disaster as well as Disaster Dislocated Worker Grants (DWG) for temporary employment to provide disaster clean-up. In addition, FEMA's Individual Assistance program provides eligible individuals and households funds for uninsured, disaster-related necessary expenses. Finally, USDA provides the Disaster Supplemental Nutrition Assistance Program to offer short-term financial food assistance. However, these programs are temporary and do not provide for complete financial recovery. For instance, DUA is generally only available for up to 26 weeks after the date of a disaster declaration. In addition, although DWG assistance allows some flexibility for the length of time, due to limited appropriations extended assistance is generally not available. Strategies for better enhancing personal economic resiliency will require a more targeted effort between the Federal Government, partners in the education and financial sectors, and local community-based organizations, to promote financial wellness and savings to mitigate economic disruptions, such as those caused by disasters.

Impact of Disasters on Less-Resourced Communities

Recent economic studies have analyzed the impact of disasters on communities. In 2017, the National Bureau of Economic Research studied the effects of natural disasters on economic activity and found that counties that had severe disasters experienced greater out-migration, lower home prices, and higher poverty rates. Persistent disaster risk could decrease demand to live in an area, which may lower rent prices and create a draw for low income populations. Additionally, a 2017 report by the Substance Abuse and Mental Health Services Administration highlighted the disproportionate effects of disasters on people of low socioeconomic status. The report found that these individuals are more likely to live in disaster-prone housing or areas, may be more vulnerable to economic losses, and face many barriers to receiving aid after a disaster.

Cybersecurity

Since 2012, states and territories have consistently reported Cybersecurity as their least proficient capability (**Figure 21** and **Figure 22**). Between the 2012 and 2017 State Preparedness Report submissions, 16 states and territories declined in proficiency, while 13 improved. Many Americans rely on cyber systems and networks for daily practices, including communication, banking, and energy systems. The adoption of cyber systems in cities is improving individual convenience, quality of life, and the efficient use of resources. However, greater connectivity also expands the risk and impact of cyber incidents. For example, the 2015 intrusion of the U.S. Office of Personnel Management (OPM) and the 2017 Equifax data breach exposed the personally identifiable information of millions of Americans. Additionally, the 2017 WannaCry ransomware attack, discussed in the following section, affected several U.S. hospitals and healthcare facilities, locking files and delaying medical care.

The increased connectivity of physical systems in critical infrastructure—such as electric grids and water treatment facilities—increases the threat that vulnerabilities in cybersecurity pose (see **Improving Cybersecurity in Physical Systems**). Cyber incidents are a rapidly evolving threat, joining nation-state threats and terrorism as an area of significant public concern. As of 2016, 12 states and territories created partnership organizations to respond to a cyber incident, indicating increased awareness of the growing threats in cybersecurity. However, several persistent challenges to cybersecurity continue to affect the Nation's ability to protect, and if needed, restore computer systems. The following key findings summarize ongoing challenges in Cybersecurity.

Improving Cybersecurity in Physical Systems

Through the public-private partnership program, Cybersecurity Capability Maturity Model (C2M2), DOE helps organizations improve their cybersecurity capabilities. The model provides cybersecurity best practices, and enables stakeholders to evaluate, prioritize, and improve their capabilities to protect the energy sector from cyber incidents. C2M2 includes tailored versions of the model for the electricity, oil, and natural gas subsectors, and a sector-neutral version for cross-sector use. Since its inception in 2012, over 1,200 energy sector organizations have used the tool.

State and Territory Perspectives

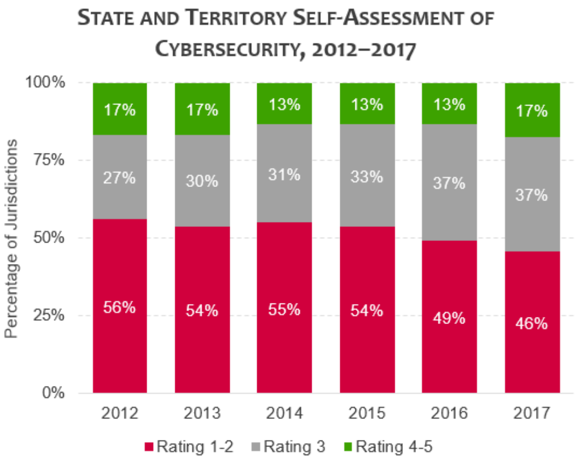


Figure 21. Since 2012, states and territories have reported a low level of proficiency (indicated by percentage of 4 and 5 ratings) in Cybersecurity.

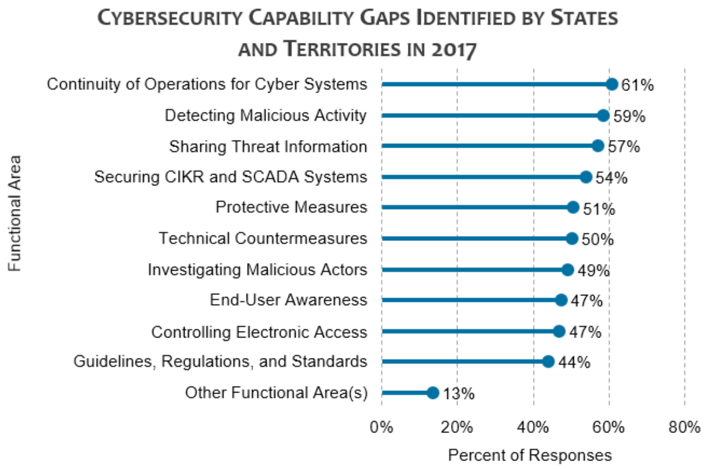
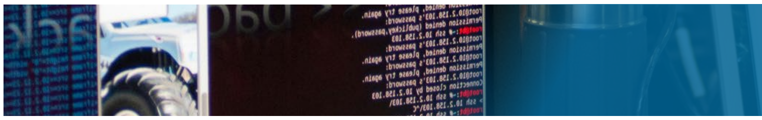


Figure 22. Since 2014, states and territories have identified functional gaps in their annual State Preparedness Report responses. Functional areas break down core capabilities into more granular-level functions, which were identified from national preparedness doctrine.



Cybersecurity

Key Finding:

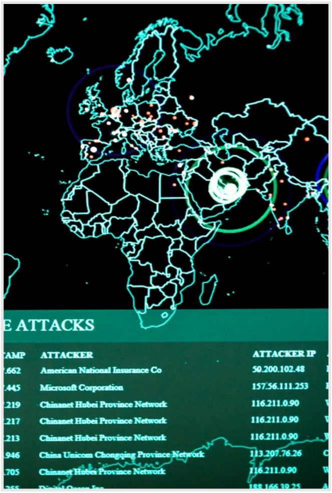
Evolving cyber threats continue to outpace the development of protective practices; at the same time, technology users often fail to implement precautionary measures to safeguard their cyber systems.

Cyber threats have continued to evolve in recent years. Malicious actors continue to use ransomware—a form of software that locks files on the infected computer system or network and demands a payment from the user to regain access to their files (see **2017 WannaCry Ransomware Attack**). In recent years, these malicious actors have increasingly turned to phishing attacks to gain access to computer networks. In a phishing attack, a malicious actor will pretend to be a trusted entity to trick users into revealing login credentials or downloading malicious software onto a closed network. In 2017, phishing attacks accounted for the majority of all data breaches with an identified attack vector. These attacks continue to target all levels of government, critical infrastructure, private businesses, nonprofit organizations, and individuals.

2017 WannaCry Ransomware Attack

In May 2017, hospitals in the United Kingdom and U.S. experienced a ransomware attack known as WannaCry. WannaCry infected hospital systems by exploiting a vulnerability in Windows server software. Following this incident, the National Cybersecurity and Communications Integration Center (NCCIC) developed an exercise template for healthcare facilities to exercise preparing for and responding to an incident like WannaCry, and coordinated with more than 40 information technology and cybersecurity companies to convey knowledge about the threat.

The expansion of largely unsecured Internet of Things (IoT) devices has also increased cyber vulnerabilities through an increased number of entry points for malicious actors to attack. Use of the IoT—which includes automated technology that collects information, communicates it over a network, and can act on that information—has greatly increased, ranging from smart televisions to automated industrial control systems. By 2020, there is predicted to be an estimated 50 billion IoT devices in use, up from approximately 13 billion in 2013. This increase includes both devices for personal use and those at critical infrastructure facilities, which pose risks to multiple interconnected sectors. The interconnectivity of IoT devices creates more avenues for attacks—as malicious actors can use widely available search tools to find devices connected to the Internet and infiltrate them. Multiple critical sectors are vulnerable to this threat, such as water and wastewater systems, energy, and healthcare. In the healthcare sector, the risk of potential cybersecurity threats has grown as the volume of Internet-connected medical devices and automated medication delivery systems—such as glucose monitors or insulin delivery systems—increased.



AMP	ATTACKER	ATTACKER IP
.662	American National Insurance Co	50.200.102.48
.445	Microsoft Corporation	157.56.111.253
.219	Chinanet Hubei Province Network	116.211.0.90
.217	Chinanet Hubei Province Network	116.211.0.90
.213	Chinanet Hubei Province Network	116.211.0.90
.946	China Unicom Chongqing Province Network	113.207.76.26
.705	Chinanet Hubei Province Network	116.211.0.90
.255	Digital Ocean Inc	188.166.39.25

Adoption of cybersecurity safeguards have not kept pace with the increased use of IoT devices and the associated vulnerabilities. In November 2016, DHS released strategic principles on how to secure IoT devices and applications. NIST also issued extensive guidance to federal agencies, including a catalog of security and privacy controls to protect information and systems. Organizations, such as the Institute of Electrical and Electronics Engineers, have developed information security standards that address specific areas, such as encryption and storage. However, standards specific to IoT technologies are still in development or not widely adopted. Further, many technology manufacturers do not consider or implement these principles when designing IoT devices (see **2016 Mirai Botnet IoT Attack**). Experts note a lack of incentives for manufactures to adopt these security principles and practices, as manufacturers often focus on price and features to bring devices to the market. As a result, manufacturers do not consider cybersecurity to be as high as a priority until after the device is released for sale.

2016 Mirai Botnet IoT Attack

Once a malicious actor locates IoT devices using a web search engine, the actor can use factory default credentials to gain access to the device. These unsecured IoT devices allow malicious actors to infiltrate a residential or commercial network and put them at risk of becoming a botnet—that is, part of a network of devices that a single computer can remotely control. In 2016, Mirai Botnet was responsible for a series of Distributed Denial of Service (DDoS) attacks. The Mirai Botnet scanned the Internet looking for IoT devices, such as routers, DVRs, and web cameras, that used factory default credentials and created a malicious network capable of attacking online targets with large loads of traffic until the target could no longer support legitimate web traffic. Source code for the Mirai Botnet was released online, allowing anyone to build their own botnet using infected IoT devices. Malicious actors then used the Mirai Botnet to attack the Internet infrastructure firm Dyn, shutting down access to popular websites like Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix.

In addition to IoT vulnerabilities, another emerging issue facing local, state, and federal agencies is the vulnerability of voter registration and election systems to a cyber incident. Prior to the 2016 presidential election, DHS received reports of Internet scans of election agency websites in several states, raising concerns about the susceptibility of election systems. In October 2016, the DHS Office of Intelligence and Analysis identified that Internet-connected election networks, including websites, in 21 states, were potentially targeted by malicious cyber actors. However, federal officials noted there was no evidence votes were changed or otherwise impacted. Because of these incidents, the Federal Government took several steps to safeguard election systems, including:

- Designating voting systems as critical infrastructure to facilitate federal cybersecurity assistance;
- Establishing an election security task force in October 2017 to help strengthen local and state voting infrastructure; and
- Establishing a Cybersecurity Services Catalog for Election Infrastructure that provides information on services and resources available to the election infrastructure community, including cybersecurity assessments, consulting, information sharing and threat analysis, cyber and communications incident response, and network protection.

In addition, National Guard units have provided cybersecurity vulnerability assessments to state, tribal, territorial, and local agencies and private industry critical infrastructure owners, including assessments of voting systems.

Finally, end users also present a large vulnerability through a lack of adherence to cybersecurity best practices. Computer users have not widely adopted cybersecurity principles and best practices—such as using strong passwords and installing software patches and updates—that would mitigate potential cyber threats and vulnerabilities. For example, young adults (the largest demographic of computer users) often report that while they are aware of general cybersecurity principles, they do not fully grasp the urgency of cybersecurity and do not fully follow these principles.

Key Finding:

Insufficient information sharing between the public and private sectors has hindered the Nation's effectiveness in defending against cyber threats.

Information sharing across different stakeholders is a key element of cybersecurity, facilitating collaboration and enabling a coordinated response to better protect against cyber threats. For example, the private sector provides the Federal Government with technical information on cyber intrusions as they occur. Meanwhile, the Federal Government gives the private sector situational awareness, analysis, and solutions to defend their cyber systems. These complementary strengths make effective information sharing crucial to protecting the Nation from cyber threats. Ineffective information sharing delays responses to cyber incidents, allowing malicious actors to cause further harm.

Cybersecurity

Several factors inhibit information sharing between the public sector and private sector. First, private-sector critical infrastructure operators often cannot receive timely cyber threat information due to a lack of appropriate security clearances among their personnel and a lack of facilities that can receive classified information. The Federal Government often does not declassify information on cyber threats quickly enough to be actionable. Organizations within the healthcare and public health sectors have noted the lack of clearances hinders their ability to prepare for emergencies. To address these challenges, DHS provides the Enhanced Cybersecurity Services program, which is intended to be a quick and scalable way to protect U.S-based public and private entities by using sensitive unclassified and classified cyber threat indicators. Within this model, a small number of service providers have the requisite facilities, clearances, and accredited systems required to protect and defend their customers. The program's success, however, will continue to rely on the sourcing of timely and actionable indicators as well as increased awareness of the program's offerings across a wide stakeholder base.

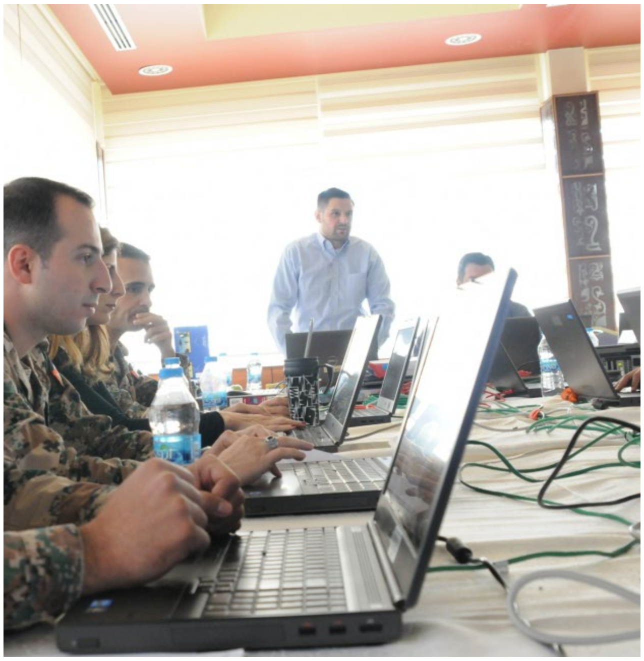
Conversely, many organizations in the private sector are hesitant to share data with or grant system access to the Federal Government due to concerns over the use and protection of their data. To address these concerns, DHS facilitates information sharing through its Automated Indicator Sharing program—which uses machine-to-machine information sharing to automatically share data between computers without the need for a human operator. Since its inception, DHS has shared approximately 1.4 million unique indicators of computer intrusion with federal and private-sector partners. However, a 2017 DHS Office of the Inspector General report found that private-sector firms identified several technical and resource-related concerns with participation in the program. The program faces other challenges as well, as information released through the Automated Indicator Sharing program often lacks detail on how to stop or mitigate cyber threats. Some sectors—the energy sector in particular—have created ways to combine the knowledge of the public and private sectors. For example, to address these concerns, DOE and the Electricity Information Sharing and Analysis Center developed the Cybersecurity Risk Information Sharing Program (CRISP). CRISP facilitates the timely bi-directional sharing of threat information and provides situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.

Key Finding:

The Federal Government faces persistent challenges in the recruitment and retention of cybersecurity personnel, though it has taken steps to improve cybersecurity training for the Nation.

Cybersecurity personnel work to prevent and mitigate vulnerabilities that allow malicious actors to access and harm computer networks by finding and patching system vulnerabilities before cybercriminals can exploit them. Their services are critical to national security. Maintaining an effective cybersecurity workforce requires recruitment, retention, and training of individuals with the specialized knowledge, skills, and abilities to prevent, detect, and respond to evolving threats.

Federal Recruitment Challenges



In recent years the Federal Government's cybersecurity workforce has grown significantly, but federal agencies continue to struggle to attract cybersecurity personnel from the academic and private sectors. Further, the Federal Government must compete with the private sector for a limited pool of highly trained cyber personnel, creating a shortage of cybersecurity expertise. Federal positions often have long hiring timelines, partially due to the need for security clearances, resulting in candidates pursuing private-sector positions that have a faster process. In addition, compensation for federal cybersecurity professionals is not competitive with equivalent private-sector positions. Further, cybersecurity is still a relatively new field and federal positions often lack standard job titles that match industry positions. This leads to confusion in the hiring process for both hiring managers and potential candidates—meaning positions remain unfilled because qualified candidates are not applying to appropriate job openings.

To address the issue of non-competitive compensation, OPM developed and implemented special hiring authorities. OPM also educated agencies on additional benefits, such as special pay rates, recruitment incentives, and increased accrual of leave. For example, OPM released "Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals" and a course titled "Pay and Leave Flexibilities for Recruitment and Retention." In response to confusion about cybersecurity positions, NIST partnered with DHS and DoD in August 2017 to issue a new version of the National Initiative for Cybersecurity Education Workforce Framework to provide employers (in both the public and private sectors) and educators with "a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role." The Framework seeks to improve the government hiring process by matching government cybersecurity positions with language used in academia and the private sector. In January 2017, OPM issued guidance on the adoption of the Framework. This guidance includes the requirement for agencies to assign job codes that match their positions to the Framework's language, allowing for more strategic recruitment of these critical positions. In August 2017, GAO reported that DHS has taken actions to identify and categorize all cybersecurity positions in accordance with the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, with 79 percent of positions categorized.

Federal Retention Challenges

Beyond hiring-related challenges, federal agencies face challenges retaining qualified cybersecurity personnel they already employ. Since 2011, the percentage of cybersecurity employees—those classified as computer engineers, computer scientists, and information technology managers—with four or fewer years of federal service who are quitting the Federal Government has risen and continues to be higher than any other group (i.e., 5–14 years, 15–24 years, and 25 or more years). The Federal Government recognizes that there is increasing competition with the private sector for top cybersecurity personnel. As the Federal Government cannot match private-sector compensation, retention of cybersecurity professionals requires specialized career paths tailored to the individuals that focus on developmental and training opportunities, as well as creating a flexible work culture that offers the autonomy that can be found in the private sector. For example, through its Cyber-Pay program, DHS grants some personnel additional pay for receiving industry certifications in cybersecurity.

National Cybersecurity Training

In 2016, OPM and the White House released the Cybersecurity National Action Plan which identified cybersecurity education as critical to building a long-term cybersecurity workforce, noting that not enough students receive the training needed for cybersecurity work. ISACA[9]—the international information technology and security professionals' association—predicts that by 2019, there will be a global shortage of two million cybersecurity professionals. Moreover, there is no common knowledge base among cybersecurity students and as a result, organizations often spend limited training funds to close skills gaps. To address these issues the Federal Government has undertaken several initiatives:

- Through the Federal Virtual Training Environment platform, which has received over 200,000 registrations as of January 2018, the Government has provided free online cybersecurity training to territorial, tribal, local, state, and federal government employees.
- In FY 2017, the NCCIC stood up the National Cybersecurity Training and Exercise Center of Excellence to manage ICS-focused technical training and exercise capabilities.
- In FY 2017, the U.S. Secret Service (USSS) trained over 1,000 state and local law enforcement personnel on cyber-crime investigations. In addition, the *Strengthening State and Local Cyber Crime Fighting Act of 2017* authorized USSS to operate the National Computer Forensics Institute to instruct state and local law enforcement officers, prosecutors, and judges on cyber crime.
- DHS manages several cybersecurity education programs to equip students and teachers with the skills, knowledge, and abilities needed for adequate cyber training. Through the Cybersecurity Education and Training Assistance Program, DHS provides K-12 educators with science, technology, engineering, and math curricula and professional development resources. In 2017, the cyber training grant program—provided through National Cybersecurity Preparedness Consortium members, including Texas A&M Engineering Extension Service—delivered cybersecurity training to 9,869 individuals. At the collegiate level, DHS partners with the National Security Agency to jointly sponsor the National Centers of Academic Excellence program in Cyber Defense. More than 200 colleges and universities nationwide have earned this designation.
- Some academic institutions offer the Scholarship for Service program, which provides scholarships in the form of tuition and stipends for students studying fields related to cybersecurity. The program requires students to serve in government upon graduation, thus filling federal cybersecurity positions with qualified candidates. DHS sponsors job fairs to connect students in this program with government employers. More than 1,200 students, government agency representatives, and educational institution representatives attended the Scholarship for Service Job Fair held in Washington, D.C. in January 2018.
- DOE held the second Annual DOE Cyber Defense Competition at Argonne National Laboratory for teams of over 100 undergraduate and graduate students seeking to defend simulated infrastructure networks against attacks. The competition helps advance workforce development and builds knowledge of infrastructure-specific cybersecurity challenges among future professionals.

[9] Originally known as the Information Systems Audit and Control Association, the organization now goes by ISACA to better reflect the wide range of IT governance professionals it represents.

The Path Forward

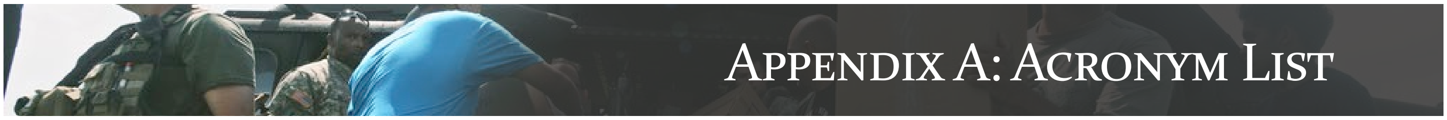
Since 2012, the *National Preparedness Report* has evaluated progress made in meeting the *National Preparedness Goal* of a secure and resilient Nation. Each year, the report has identified challenges across the Nation while also demonstrating that individuals and communities, private and nonprofit sectors, faith-based organizations, and all levels of governments continue to build, sustain, and deliver core capabilities. The 2018 *National Preparedness Report* builds on this work, providing in-depth analyses of persistent preparedness challenges from 2012 to 2017 and highlighting lessons learned from incidents in 2017. Through an in-depth analysis of selected core capabilities, the report aims to provide targeted areas for the whole community to address to have the greatest impact on strengthening national preparedness. The 2018 *National Preparedness Report* serves as an inflection point, providing an overview of the challenges and progress in preparedness over the past six years before employing a revised approach for assessing preparedness in future reports.

Going forward, the *National Preparedness Report* will update its approach and include an assessment of progress against objectives that state, tribal, and local partners set through the revised Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) methodology.[10] The revised THIRA/SPR methodology addresses community feedback and will provide more specific and quantitative data for preparedness analysis through standardized targets to set goals and measure progress over a three-year period. Data from the revised methodology will allow FEMA to conduct a rigorous analysis of how states, territories, urban areas, and tribal governments are performing, in the aggregate, to meet their targets. Future editions of this report will feature analyses that draw on data from the updated methodology. Through this analysis, the report will provide the whole community with a comprehensive assessment of national preparedness—while also informing planning and exercise priorities, tracking national progress in closing capability gaps, and supporting decision-making to build and sustain the core capabilities required to become a prepared and resilient Nation.

[10] The State Preparedness Report was renamed the Stakeholder Preparedness Review in 2018.

Appendix A: Acronym List

Acronym	Definition
ASCE	American Society of Civil Engineers
BEACON	Business Energy and Communication Optimization Network
BEOCs	Business Emergency Operations Centers
BSIR	Biannual Strategy Implementation Report
CDBG-DR	Community Development Block Grant Disaster Recovery
CDC	Centers for Disease Control and Prevention, HHS
CRISP	Cybersecurity Risk Information Sharing Program
C2M2	Cybersecurity Capability Maturity Model
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
DUA	Disaster Unemployment Assistance
DWG	Dislocated Worker Grant
EDA	U.S. Economic Development Administration
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
EPA	U.S. Environmental Protection Agency
EPFAT	Emergency Power Facility Assessment Tool
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
FY	Fiscal Year
GAO	U.S. Government Accountability Office
GIS	Geographic Information System
HHS	U.S. Department of Health and Human Services
HPP	Hospital Preparedness Program
HSIN	Homeland Security Information Network
HUD	U.S. Department of Housing and Urban Development
ICS	Incident Command System
IED	Improvised Explosive Device
IEDC	International Economic Development Council
IHP	Individuals and Households Program



Appendix A: Acronym List

Acronym	Definition
IoT	Internet of Things
ISACA	International Information Technology and Security Professionals' Association
ISIS	Islamic State of Iraq and al-Sham
IT/DR	Information Technology/Disaster Recovery
MEP	Manufacturing Extension Partnership
NADO	National Association of Development Organizations
NBEOC	National Business Emergency Operations Center
NCCIC	National Cybersecurity and Communications Integration Center
NDRF	National Disaster Recovery Framework
NEP	National Exercise Program
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NQS	National Qualification System
NVOAD	National Voluntary Organizations Active in Disasters
OBP	Office for Bombing Prevention
OPM	U.S. Office of Personnel Management
PKEMRA	Post-Katrina Emergency Management Reform Act
PR BEOC	Puerto Rico Business Emergency Operations Center
PREPA	Puerto Rico Electric Power Authority
PVPC	Pioneer Valley Planning Commission
RSF	Recovery Support Function
RTLT	Resource Typing Library Tool
SBA	U.S. Small Business Administration
SETRAC	SouthEast Texas Regional Advisory Council
SPR	Stakeholder Preparedness Review (previously known as the State Preparedness Report)
SRIA	Sandy Recovery Improvement Act
THIRA	Threat and Hazard Identification and Risk Assessment
USACE	U.S. Army Corps of Engineers
USDA	U.S. Department of Agriculture
USSS	U.S. Secret Service

Appendix B: Mission Area Overview

Prevention

Protection

Mitigation

Response

Recovery

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					●

Prevention Mission Area

The Prevention mission area focuses on the activities relevant to ensuring the Nation is optimally prepared to avoid, prevent, or stop an imminent incident within the United States.

To effectively prevent an incident, preparedness officials and first responders implement critical tasks, as identified through **Planning** efforts. Critical actions and strategies are implemented through **Operational Coordination** to ensure tasks are carried out in an organized fashion. Through **Public Information and Warning**, officials deliver clear, actionable, and accessible messages about relevant threats and hazards to the whole community.

Preventing a threat begins with **Intelligence and Information Sharing**, the ability to develop situational awareness, conduct analysis, and share information associated with the actor(s), method(s), means, weapon(s), and/or target(s) related to a possible threat. After identifying a threat, officials conduct **Screening, Search, and Detection** operations to identify and locate hostile actors and their weapons. In addition, law enforcement officials carry out **Interdiction and Disruption** operations to locate and neutralize threats and their operations. **Forensics and Attribution** allows law enforcement to identify threats and their sponsors and prevent initial or follow-on attacks.

Protection Mission Area

The Protection mission area focuses on the steady-state operations necessary to secure the Nation against all threats and hazards. The end state of this mission area is the physical and cyber protection of people and infrastructure.

To protect against an incident, emergency management officials, first responders, and private and nonprofit organizations implement critical tasks, as identified through **Planning** efforts.

Steady-state **Intelligence and Information Sharing** and **Risk Management for Protection Programs and Activities** create an understanding of the everyday threat environment and the likelihood of a threat against an asset, individual, or event. **Screening, Search, and Detection** and **Interdiction and Disruption** operations are ongoing functions as part of the intelligence and risk-management cycles. Once a possible threat vector is identified and its risk is understood, emergency managers disseminate **Public Information and Warning**, as needed, to deliver clear, actionable, and accessible messages to the whole community.

Through **Access Control and Identity Verification**, public- and private-sector officials apply necessary measures to control admittance to critical locations and systems. These measures include both **Physical Protective Measures**, a range of physical, technological, and cyber countermeasures and policies that protect people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors, as well as **Cybersecurity**, activities—such as partnerships between cybersecurity and physical systems experts—that protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Supply Chain Integrity and Security helps strengthen the resilience of the Nation's critical supply chains from intentional disruptions or natural hazards. Preparedness officials and first responders deliver these core capabilities through **Operational Coordination** to ensure tasks are carried out in an organized fashion.

Mitigation Mission Area

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

The first step to effectively mitigate risks is **Threats and Hazards Identification**, which includes understanding the frequency and magnitude of a community's threats and hazards. Communities then conduct **Risk and Disaster Resilience Assessments** to understand the consequences these threats and hazards would have if they occurred. Based on this knowledge, community officials can begin **Planning** to manage the risk, and provide **Public Information and Warning** to residents. These plans also enable **Long-term Vulnerability Reduction** through one or more of the following strategies:

- Risk avoidance – Preventing exposure to an incident (e.g., using zoning rules to prevent construction in high-risk areas);
- Risk reduction – Minimizing vulnerabilities (e.g., adopting and enforcing disaster-resistant building codes); and

- Risk transfer – Eliminating or limiting liability for harm (e.g., purchasing flood insurance).

Avoiding risks entirely is not always possible, so the Framework encourages leadership, collaboration, partnership building, education, and skill building before an incident through **Community Resilience**, with the goal of supporting other capabilities and building resilience. The *National Mitigation Framework* also encourages communities to build and sustain capability in **Operational Coordination** to integrate critical stakeholders to support efforts during and after an incident.

Response Mission Area

The Response mission area encompasses the capabilities necessary to save lives, protect property and the environment, and meet basic human needs immediately following an incident. Under the *National Response Framework*, there are 15 core capabilities that work together to guide the Nation's response to disasters and emergencies.

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

During the response, trained personnel deliver traditional and atypical **Mass Search and Rescue Operations** to locate and rescue persons in distress. During mass fatality incidents, **Fatality Management Services** provides recovery of remains, victim identification, and bereavement counseling. Officials protect both response workers and the public through **Environmental Response/Health and Safety** operations and **On-scene Security, Protection, and Law Enforcement**. For incidents involving fires, **Fire Management and Suppression** efforts may also be necessary to save and protect lives, property, and the environment.

Public, private, and community-based organizations provide **Mass Care Services and Public Health, Healthcare, and Emergency Medical Services** to address the basic needs of survivors, including those with disabilities and other access and functional needs. Furthermore, officials use **Critical Transportation** and **Logistics and Supply Chain Management** to ensure that essential commodities, equipment, and services reach affected communities. This aids owners and operators of **Infrastructure Systems** in restoring systems and services for the community and transitioning to the recovery phase.

Recovery Mission Area

The Recovery mission area has eight core capabilities that work together to repair and restore infrastructure and services needed to support the physical, emotional, and financial well-being of survivors and disaster areas. Under the *National Recovery Framework*, these eight core capabilities work together to guide the Nation's recovery from disasters and emergencies.

To effectively recover from an incident, emergency management officials identify critical tasks through **Planning** efforts. Effective **Operational Coordination** ensures public, private, and non-governmental recovery stakeholders execute critical tasks in a timely and organized manner. Through **Public Information and Warning**, officials deliver clear, actionable, and accessible information about relevant threats, hazards, and recovery initiatives to the whole community.

The repair of **Infrastructure Systems** returns essential services—such as power and safe drinking water—to disaster zones, providing a foundation for rebuilding communities. Re-establishing **Health and Social Services** allows for the restoration of healthcare facilities and networks, which promotes the well-being and independence of the whole community. Implementing temporary and permanent **Housing** solutions for displaced residents moves survivors out of emergency shelters and transitions them into long-term recovery. Experts work with the whole community to preserve, conserve, rehabilitate, and restore **Natural and Cultural Resources**. In the long-term, communities lead **Economic Recovery** programs to return economic and business activities, including food production and agriculture, to a healthy state.

Appendix C: Research Approach

Overall Approach

FEMA coordinates the development of the *National Preparedness Report* by incorporating qualitative and quantitative data to assess the Nation's progress in meeting the *National Preparedness Goal*. 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 among the five persistent preparedness challenges from 2012 to 2017;
- Analyzing 2017 THIRAs from 115 urban areas, states, territories, tribes, and FEMA Regions, as well as 2017 State Preparedness Report submissions from all 56 states and territories, to identify national shifts in the threats and hazards that states and territories 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 five persistent preparedness challenges;
- 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 incidents occurring or reported in 2017—including interviews with response and recovery personnel, storm impact data, and federal agency after-action findings from the 2017 Hurricane Season—to identify preparedness outcomes and lessons learned; and
- Engaging federal departments, agencies, and senior interagency coordination groups to review and supplement report content.

Persistent Preparedness Challenges

The 2018 *National Preparedness Report* focuses on selected capabilities that previous reports have identified as a capability to sustain or area for improvement. The following subsections provide additional details on the process for identifying capabilities to sustain and areas for improvement.

Identifying Capabilities to Sustain

Since 2014, the *National Preparedness Report* has identified a subset of the core capabilities as capabilities to sustain. FEMA used a two-part analysis to identify capability to sustain candidates. To qualify as a capability to sustain, a core capability must first show signs of proficiency and maturity. In the first part of the analysis, each core capability was scored against preparedness indicators to identify candidates that were relatively proficient (in delivery) and mature. Examples of these indicators included:

- Do the key findings in the *National Preparedness Report* indicate this capability is an area of strength?
- Do the State Preparedness Report results indicate proficiency in this core capability nationwide?
- Is this core capability exercised frequently?
- Do data indicate strong participation in relevant training courses for this core capability?
- Do various assessments indicate the core capability is relatively mature?

In addition, capability to sustain candidates must be at risk of a growing gap between future demand for the capability and resources available. In the second part of the analysis, FEMA scored each core capability against additional indicators. Examples of these indicators included:

- Do trends in State Preparedness Report results indicate a decreasing ability to meet performance targets for this core capability nationwide?
- Has this core capability experienced a significant drop in grant funding that may result in a future decline in capability levels?
- Do federal strategic plans indicate that increasing demand for this core capability may exist in the future?
- Do various drivers influencing change in emergency management indicate that increasing gaps in this core capability may exist in the future?

Identifying Areas for Improvement

Since 2012, the *National Preparedness Report* has identified specific capabilities as national areas for improvement. In previous *National Preparedness Reports*, FEMA used a set of preparedness indicators to identify area for improvement candidates. FEMA reviewed all scores as part of its final selection process. This review sets the threshold for a capability to be considered an area for improvement. If a core capability's score was above the required threshold points with no discrepancies identified, FEMA selected that core capability as an area for improvement. Examples of preparedness indicators included:

- Do the key findings in the *National Preparedness Report* indicate this capability exhibits major deficiencies in its performance nationally?
- Do the State Preparedness Report results indicate low proficiency in this core capability nationwide?
- Is this core capability infrequently exercised?
- Do data indicate low numbers of relevant training courses for this core capability?
- Is there evidence of progress in assessing and validating core capability performance?
- Has this core capability experienced a significant drop in grant funding that may result in a future decline in capability levels?
- Do various drivers influencing change in emergency management indicate that increasing gaps in this core capability may exist in the future?

Selected Core Capabilities in the 2018 National Preparedness Report

Core Capability	National Preparedness Reports					
	2012	2013	2014	2015	2016	2017
Operational Coordination	--	--		●		●
Infrastructure Systems	□	□	□	□	□	□
Housing	□	□	□	□	□	□
Economic Recovery	□	□		□	□	□
Cybersecurity	□	□	□	□	□	□

● Capability to Sustain
□ Area for Improvement