

Mission Area Overview

# PROTECTION

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

## ..... Key Finding Highlights .....



- Cybersecurity continues to affect public and private sectors, as breaches threaten Federal and private networks and states increase investments in cyber countermeasures.
- The Nation faces obstacles to securing critical infrastructure and ensuring supply chain resilience across a variety of sectors, including transportation, chemicals, and biomedical research.
- As the threat of terrorism persists and evolves, Federal, state, and local agencies have continued to expand partnerships for countering violent extremism.

## Core Capabilities in Practice .....

The Protection mission area secures the homeland against acts of terrorism and manmade or natural disasters. The *National Protection Framework* (“Protection Framework”) describes 11 Protection core capabilities, including how they operate together to safeguard the Nation against all hazards. Critical infrastructure protection, from the cyber to the physical, plays a central role in the mission area, compounded by the unique risks of aging systems. The second edition of the *National Preparedness Goal*, released in September 2015, directs greater attention toward several threats, two of which hold particular implications for infrastructure: cybersecurity and climate change.

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

Public and private stakeholders apply the remaining steady-state core capability measures, as appropriate. **Access Control and Identify Verification**, for example, controls admittance to critical locations and systems, and is essential for both **Cybersecurity** and **Physical Protective Measures**. **Supply Chain Integrity and Security** helps strengthen

## ..... CORE CAPABILITIES IN THE PROTECTION MISSION AREA

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

the resilience of the Nation's critical supply chains from intentional disruptions or natural hazards. Government officials and private and nonprofit organizations implement all the above capabilities aligned with procedures identified during the **Planning** process, which are then tested and refined during relevant exercises.

The Protection Framework also addresses the need to secure public and private networks and critical infrastructure. The following are examples of actions taken in 2015 that highlight the relationship among a select number of the 11 core capabilities in the Protection Framework:

### Planning

In 2015, the U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) coordinated an update of the Sector-Specific Plans in each of the 16 critical infrastructure sectors. The plans guide and integrate sector-specific efforts to secure and strengthen resilience, as well as each sector's broader contributions to national critical infrastructure security, as outlined in *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*. The updated plans emphasize topics such as the nexus between cyber and physical security; interdependencies among the sectors; and risks associated with climate change and aging and outdated infrastructure. More broadly, efforts to finalize and release a Federal Interagency Operational Plan for the Protection mission area continue to lag. A requirement of *Presidential Policy Directive 8: National Preparedness*, the *Protection Federal Interagency Operational Plan* will describe the concept of operations for integrating and synchronizing Federal capabilities to support state, tribal, territorial, and local protection efforts.

### Access Control and Identity Verification, and Cybersecurity

In fiscal year 2015, DHS received and responded to 20 percent more incidents—295 compared to 245 in fiscal year 2014—related to malicious cyber activity against industrial control systems (as reported by asset owners and incident partners).

### Intelligence and Information Sharing, and Operational Coordination

In 2015, the City of Los Angeles launched the Integrated Security Operations Center, the Nation's first city-wide monitoring and intelligence-sharing platform for cyber threats. The operations center evaluates an average of 30,000 cyber threats per day against the city's network and provides actionable intelligence reports to regional stakeholders.

### Planning, and Risk Management for Protection Programs and Activities

Given the potential effects of extreme weather on infrastructure, all levels of government have collaborated to validate, calibrate, and enhance risk assessments to incorporate climate change. The U.S. Department of the Interior U.S. Geological Survey developed the Coastal Storm Modeling System to help evaluate and manage preparedness resources in coastal communities. In addition, multiple levels of government collaborated in climate and infrastructure tabletop exercises in Maine and Florida in 2015. Efforts like these help practitioners to design exercises and to determine risk reduction strategies, protection planning priorities, and mitigation projects to help advance preparedness across mission areas.

### Supply Chain Integrity and Security, and Public Information and Warning

DHS NPPD conducted a series of Supply Chain Workshops across the Critical Manufacturing and Energy critical infrastructure sectors in 2015. Federal partners, private companies, and university leaders presented various topics to more than 250 state, local, Federal, and private-sector attendees, including Regional Supply Chain Threat Information, Economic Espionage, and Supply Chain Best Practices: An Industry Perspective. Workshops for both sectors took place in Oregon (Portland) and Texas (Midland, Houston, El Paso, and Corpus Christi).

### Physical Protective Measures, and Supply Chain Integrity and Security

The 2011 Strategic National Risk Assessment identified space weather (e.g., solar flares, coronal mass ejections) as posing a significant risk to the security of the Nation. In October 2015, the White House issued the *National Space Weather Strategy*, which outlines six goals to help the Nation prepare for the near- and long-term impacts of space weather. Space-weather events can disrupt various critical infrastructure systems, including transportation, communications, and electrical power. The strategy outlines objectives for protecting against space weather, including strengthening public-private collaborations to enhance understanding about and reduce vulnerabilities, and encouraging industries to adopt standards, business practices, and operational procedures that address space-weather vulnerabilities.



## THEN and Now

### Personal Identity Verification Cards

The 2012 *National Preparedness Report* discussed rapid progress in issuing personal identity verification cards to Federal employees and contractors, but slower progress in implementing these cards to access Federal facilities and networks. Various efforts since then, including a Cyber Sprint in 2015, have increased card implementation tenfold, from 7 percent at the end of fiscal year 2011 to more than 76 percent at the end of fiscal year 2015.

### RadNet

The 2012 *National Preparedness Report* discussed nationwide surveillance systems for biological and radiological agents, including RadNet, a national network of monitoring stations that regularly collects samples to analyze for radioactivity. Over time, the U.S. Environmental Protection Agency has added new stations, as well as upgraded existing ones. RadNet now includes 135 stationary monitors around the country and 40 portable stations for placement in an emergency.

### Regional Resiliency Assessment Program

This program performs assessments of critical infrastructure systems within a particular geographic region. By the end of 2012, DHS NPPD had partnered with stakeholders to complete 27 assessments, which identified critical infrastructure interdependencies, cascading effects, and capability gaps. Since then, DHS has explored ways to adapt the assessment process to address emerging issues, such as climate change, cybersecurity, and electromagnetic-pulse preparedness.

## BY THE NUMBERS

### 1,700 TRAINEES

DHS NPPD provided 1,700 participants from commercial facilities in various critical infrastructure sectors with training on the threat from violent extremism, including courses on “Understanding Violent Extremism and Radicalization” and “Enhancing Security for Violent Extremism.”

### 2,653 FIREARMS INTERDICTED

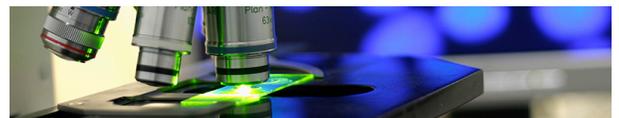
In 2015, the Transportation Security Administration (TSA) screened more than 700 million passengers at airports nationwide, interdicting 2,653 firearms.

### 120 PARTICIPANTS

The National Association of State Energy Officials, in partnership with the Department of Energy and the National Conference of State Legislatures, delivered a State Energy Risk Assessment workshop to 120 state and local energy and emergency-management officials.

### 500 PARTNERS

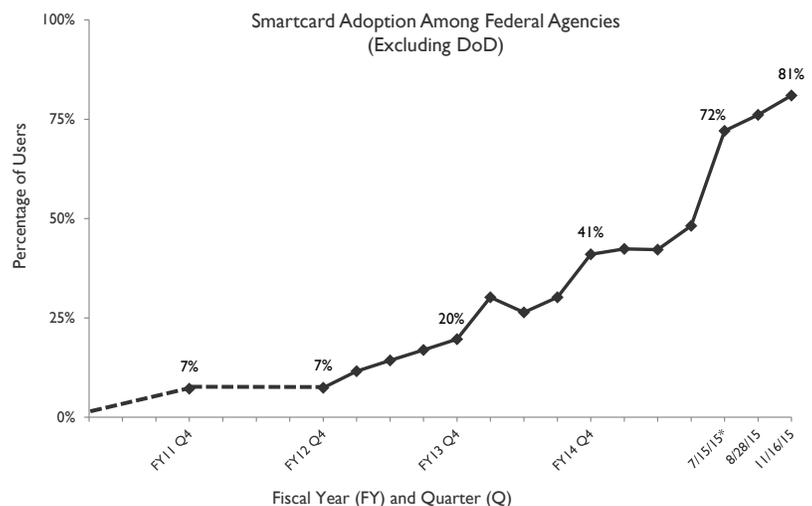
In fiscal year 2015, more than 500 Federal, state, and local partners—including representatives from environmental, law enforcement, public health, and transportation agencies; fire departments; emergency medical services; national laboratories; and National Guard units—participated in BioWatch drills and exercises.



## PREPAREDNESS TRENDS AND FIGURES

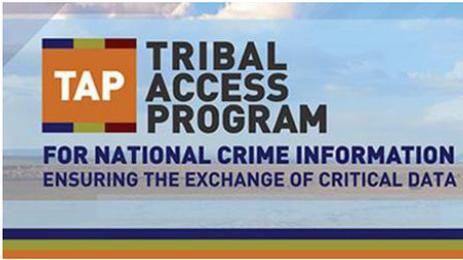
### Access Control and Identity Verification in Federal Agencies

In 2015, a Cyber Sprint initiated by the White House resulted in the single largest increase in the use of secure access to government systems since the adoption of smartcards (i.e., identity badges embedded with computer chips) was mandated in 2004. Ensuing efforts by Chief Information Officers led to an increase in smartcard use in civilian agencies, from 41 percent at the end of 2014 to 81 percent as of November 2015. Improving implementation of smartcards for controlling and validating access to Federal facilities and systems was noted as an area for improvement in the 2015 *National Preparedness Report*, further demonstrating the effectiveness of the Cyber Sprint initiative.



Note: Dashed lines indicate quarters in which data were unavailable.

## PREPAREDNESS SNAPSHOTS



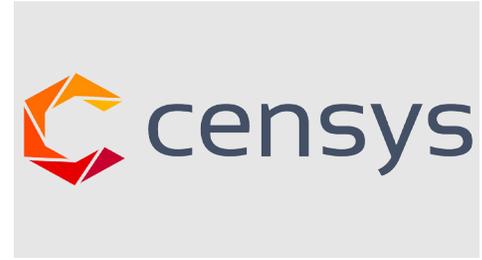
### NATIONAL CRIME INFORMATION SYSTEM

Ten tribes began participating in a trial of the U.S. Department of Justice’s National Crime Information system, which allows them to access and exchange data on crime with Federal and state governments. This pilot project provides tribal law enforcement agencies with direct access to Federal, state, and local criminal records for the first time, thereby enhancing community resilience and the safety of tribal law enforcement.



### NATIONAL CYBER SECURITY AWARENESS MONTH

In October 2015, DHS sponsored the 12th annual National Cyber Security Awareness Month. National Cyber Security Awareness Month—which the White House, 48 states, and 35 local governments have recognized through signed proclamations—engages the public and private sector through events and initiatives to raise cybersecurity awareness and increase the Nation’s resilience to cyber threats. More than



140 events took place across the country, which is 16 percent more than the previous year.

### UNIVERSITY OF MICHIGAN

In October 2015, the University of Michigan and Google launched Censys, a cybersecurity tool that identifies security concerns by tracking networked devices and assessing their level of security. The project has resulted in the enhanced security of more than 100,000 industrial control systems.

## STATE PERSPECTIVES ON PREPAREDNESS

### 2015 State Preparedness Report Results

- Protection core capabilities with higher priority ratings generally had higher proficiency ratings. Cybersecurity, however, was the fifth-highest-rated priority, but the lowest-rated in proficiency among all 31 core capabilities.
- States and territories reported some of the lowest proficiency in the Protection mission area. Of the eight core capabilities specific to Protection, five were among the bottom 10 of all 31 core capabilities.
- Although states and territories rated most Protection core capabilities as lower priority, Cybersecurity and Intelligence and Information Sharing were among the top-10 highest-priority core capabilities.

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

