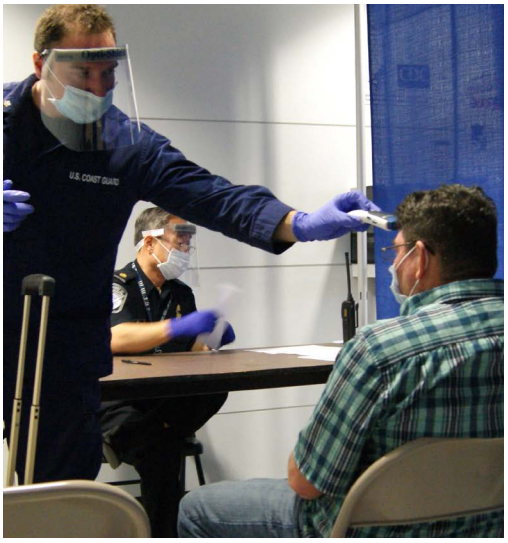
Mission Area Overview

Protection

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

Highlights

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



Frameworks in Action

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

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

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

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

Core Capabilities in the Protection Mission Area

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

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

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

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

By the Numbers

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

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

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

Resilience Innovations

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

Whole Community Accomplishments

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

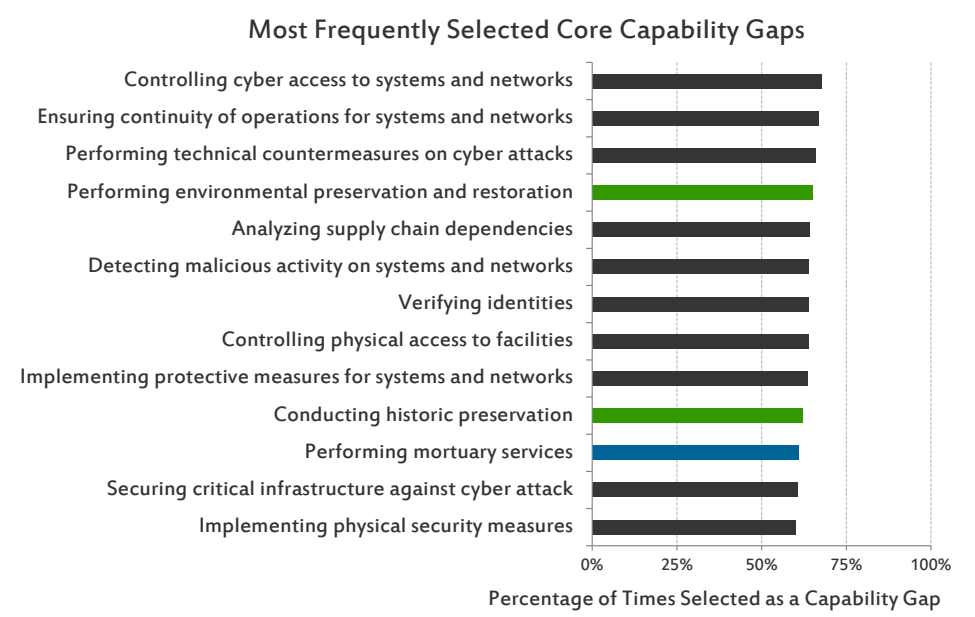
University of California, Berkeley In December 2014, the University of California, Berkeley—in partnership with prevention and environmental nongovernmental organizations—held a series of events to commemorate the 30th anniversary of the Union Carbide gas disaster in India and draw attention to chemical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

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

State Perspectives on Preparedness

2014 State Preparedness Report Results

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



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