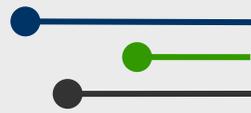


PROTECTION



Highlights

- New guidance, standards, and best practices are promoting enhanced protection of critical infrastructure and cyber systems. (Access Control and Identity Verification, p. 29; Cybersecurity, p. 30)
- Shortfalls in the size and capabilities of the cyber workforce needed to protect critical digital assets and proprietary information continue to challenge the whole community. (Cybersecurity, p. 30)
- The 2013 *National Infrastructure Protection Plan* details an updated approach to strengthen the security and resilience of critical infrastructure through the integration of cyber and physical security efforts. (Physical Protective Measures, p. 31)
- The Federal Government and the private sector have partnered to increase the availability and utility of risk assessment tools and physical security and protection programs. (Risk Management for Protection Programs and Activities, p. 32)
- Government, private-sector, and university researchers are developing and using more secure authentication technologies to improve access to critical facilities and networks. (Access Control & Identity Verification p. 29)

Trends Progress in the Cybersecurity core capability featured prominently in 2013, reflecting nationwide attention to this issue, even as states and territories reported mixed progress in other Protection core capabilities. Previous *National Preparedness Reports* identified the Cybersecurity core capability as a national area for improvement, and 82 percent of states and territories identified it as a high priority. Additionally, ratings for Physical Protective Measures and for Risk Management for Protection Programs and Activities improved, while states and territories reported slight decreases for Access Control and Identity Verification, as well as for Supply Chain Integrity and Security. Through the statewide self-assessments, states and territories also described their remaining capability gaps, including: addressing training needs arising from staffing turnover and attrition; developing and validating plans; and expanding participation from additional partners, such as the private sector.

Across the Protection mission area, multiple levels of government and the private sector worked together to secure the Nation's critical cyber and infrastructure systems. The U.S. Department of Commerce's (DOC) National Institute of Standards and Technology (NIST) worked with hundreds of public and private stakeholders to develop the [Framework for Improving Critical Infrastructure Cybersecurity](#), which highlights voluntary risk-based standards, guidelines, and best practices to manage cybersecurity risks for critical infrastructure. DHS also released [NIPP 2013: Partnering for Critical Infrastructure Security and Resilience](#), which provides an updated approach to critical infrastructure security and resilience across all five mission areas, and a greater focus on integrating cyber- and physical-security efforts. The updated plan also reaffirms the need for all levels of government to work in partnership with the private sector. Additionally, public and private partners continued developing and updating technical standards to improve infrastructure security and resilience by securing [access control](#); [cyber systems](#) and [mobile devices](#); and [technological components from supply chains](#).

In 2013, major policy changes in the Protection mission area occurred at the national level, establishing an integrated approach for infrastructure stakeholders in government and the private sector to enhance infrastructure security and resilience. New policies include [Executive Order 13636: Improving Critical Infrastructure Cybersecurity](#) and [Presidential Policy Directive 21: Critical Infrastructure Security and Resilience](#). Both are in the early stages of implementation.

By the Numbers

The U.S. Secret Service prevented losses of **\$1.1 billion** through successful cyber investigations in fiscal year 2013.

After receiving an assessment from DHS, **70 percent** of infrastructure facilities have implemented or plan to implement security enhancements.

DHS provided **77,028** hours of cybercrime training to law enforcement officers domestically and overseas in fiscal year 2013.

Resilience Innovations

- The Federal Communications Commission's (FCC) [Smartphone Security Checker](#) is an online tool that helps smartphone users secure their mobile device in 10 steps.
- The web-based [Dams Sector Analysis Tool](#), developed by USACE and DHS, provides dam owners and operators with data collection and analysis tools that support screening, prioritization, and risk analysis of dam assets.
- DOE resources through its [Cybersecurity Capability Maturity Model](#) program include toolkits that help stakeholders across all sectors to identify cybersecurity capabilities and needs.

Preparedness in Action

Attacks against the Nation's critical cyber systems remained a major preparedness concern in 2013. Through 2012 and 2013, American financial institutions experienced a sustained campaign of distributed denial-of-service attacks, which disrupted websites for many financial services organizations. Throughout this campaign, the Financial Services Information Sharing and Analysis Center served as a forum for the financial services sector and government to share information and coordinate responses to the cyber attacks. DHS's National Cybersecurity and Communications Integration Center (NCCIC) identified and shared hundreds of thousands of Internet Protocol addresses to help financial institutions improve their defenses. DHS and the FBI also provided onsite technical assistance and classified briefings on the threat and related mitigation strategies to hundreds of security specialists within the financial sector.

Improving protection against chemical incidents was another major focus area. The DHS Office of Health Affairs (OHA) launched the pilot Chemical Defense Program in Baltimore, Maryland, to help protect local communities in large chemical emergencies. During the pilot, OHA developed tailored chemical risk assessment methodologies, provided workshops for stakeholders and vendors in the Baltimore area, and conducted technology assessments. Using these findings, the Maryland Transit Administration improved chemical emergency preparedness plans, community preparedness capabilities, and technologies designed to protect the public from chemical incidents. Since the initial pilot, OHA has extended the program to Boston; New York City; San Francisco; Seattle; and Washington, D.C.

Whole Community Accomplishments

Michigan: The State of Michigan continued the [Merit Network](#)—a research, test, training, and evaluation facility for cybersecurity and cyber defense—in partnership with state universities, local governments, and the private sector. The facility expanded available training, including certificates in cybersecurity incident handling, wireless security, and cybersecurity forensics.

Texas: The Railroad Commission of Texas recently developed a *Supply Disruption Tracking Plan*, which consists of three separate systems to track the efficiency and security of the supply for natural gas, gas processing plants, crude oil pipelines, and refineries.

Oregon: The State of Oregon, with partners from industry and academia, prepared an earthquake risk study for Oregon's critical energy infrastructure hub. The study assessed risk and determined countermeasures to protect the state's energy infrastructure in the event of a catastrophic earthquake.