GAO Highlights

Highlights of GAO-17-518T, a testimony before the Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, House of Representatives

March 28, 2017

INFORMATION SECURITY

DHS Needs to Continue to Advance Initiatives to Protect Federal Systems

Why GAO Did This Study

Cyber-based intrusions and attacks on federal systems are evolving and becoming more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

DHS plays a key role in strengthening the cybersecurity posture of the federal government. Among other things, DHS has initiatives for (1) detecting and preventing malicious cyber intrusions into agencies' networks and (2) deploying technology to assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities.

This statement provides an overview of GAO's work related to DHS's efforts to improve the cybersecurity posture of the federal government. In preparing this statement, GAO relied on previously published work, as well as information provided by DHS on its actions in response to GAO's previous recommendations.

What GAO Recommends

In a January 2016 report, GAO made nine recommendations related to expanding NCPS's capability to detect cyber intrusions; notifying customers of potential incidents; providing analytic services; and sharing cyber-related information, among other things. DHS concurred with the recommendations and is taking actions to implement them.

View GAO-17-518T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) is spearheading multiple efforts to improve the cybersecurity posture of the federal government. Among these, the National Cybersecurity Protection System (NCPS) provides a capability to detect and prevent potentially malicious network traffic from entering agencies' networks. In addition, DHS's continuous diagnostics and mitigation (CDM) program provides tools to agencies to identify and resolve cyber vulnerabilities on an ongoing basis.

In January 2016, GAO reported that NCPS was limited in its capabilities to detect or prevent cyber intrusions, analyze network data for trends, and share information with agencies on cyber threats and incidents. For example, it did not monitor or evaluate certain types of network traffic and therefore would not have detected malicious traffic embedded in such traffic. NCPS also did not examine traffic for certain common vulnerabilities and exposures that cyber threat adversaries could have attempted to exploit during intrusion attempts. In addition, at the time of the review, federal agencies had adopted NCPS to varying degrees. GAO noted that expanding NCPS's capabilities, such as those for detecting and preventing malicious traffic and developing network routing guidance, could increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies. By taking these steps, DHS would be better positioned to achieve the full benefits of NCPS.

The tools and services delivered through DHS's CDM program are intended to provide agencies with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. In May 2016, GAO reported that most of the 17 civilian agencies covered by the *Chief Financial Officers Act* that also reported having high-impact systems were in the early stages of CDM implementation. For example, 14 of the 17 agencies reported that they had deployed products to automate hardware and software asset inventories, configuration settings, and common vulnerability management but only 2 had completed installation of agency and bureau/component-level dashboards. Some of the agencies noted that expediting CDM implementation could be of benefit to them in further protecting their high-impact systems. GAO concluded that the effective implementation of the CDM program can assist agencies in resolving cybersecurity vulnerabilities that expose their information systems and information to evolving and pernicious threats. By continuing to make available CDM tools and capabilities to agencies, DHS can have additional assurance that agencies are better positioned to protect their information system and information.

In addition, DHS offered other services such as monthly operational bulletins, CyberStat reviews, and cyber exercises to help protect federal systems. In May 2016, GAO reported that although participation varied among the agencies surveyed, most agencies had found that the services were very or somewhat useful. By continuing to make these services available to agencies, DHS is better able to assist agencies in strengthening the security of their information systems.