February 14, 2017

CYBERSECURITY

Actions Needed to Strengthen U.S. Capabilities

Highlights of GAO-17-440T, a testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

Cyber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, 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.

This statement (1) provides an overview of GAO's work related to cybersecurity of the federal government and the nation's critical infrastructure and (2) identifies areas of consistency between GAO recommendations and those recently made by the Cybersecurity Commission and CSIS. In preparing this statement, GAO relied on previously published work and its review of the two recent reports issued by the Commission and CSIS.

What GAO Recommends

Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of February 2017, about 1,000 recommendations had not been implemented.

View GAO-17-440T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII). While previous administrations and agencies have acted to improve the protections over federal and critical infrastructure information and information systems, the federal government needs to take the following actions to strengthen U.S. cybersecurity:

- **Effectively implement risk-based entity-wide information security programs consistently over time**. Among other things, agencies need to (1) implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices; (2) patch vulnerable systems and replace unsupported software; (3) develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis; and (4) strengthen oversight of contractors providing IT services.
- **Improve its cyber incident detection, response, and mitigation capabilities**. The Department of Homeland Security needs to expand the capabilities and support wider adoption of its government-wide intrusion detection and prevention system. In addition, the federal government needs to improve cyber incident response practices, update guidance on reporting data breaches, and develop consistent responses to breaches of PII.
- **Expand its cyber workforce planning and training efforts**. The federal government needs to (1) enhance efforts for recruiting and retaining a qualified cybersecurity workforce and (2) improve cybersecurity workforce planning activities.
- **Expand efforts to strengthen cybersecurity of the nation's critical infrastructures**. The federal government needs to develop metrics to (1) assess the effectiveness of efforts promoting the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* and (2) measure and report on effectiveness of cyber risk mitigation activities and the cybersecurity posture of critical infrastructure sectors.
- **Better oversee protection of personally identifiable information**. The federal government needs to (1) protect the security and privacy of electronic health information, (2) ensure privacy when face recognition systems are used, and (3) protect the privacy of users' data on state-based health insurance marketplaces.

Several recommendations made by the Commission on Enhancing National Cybersecurity (Cybersecurity Commission) and the Center for Strategic & International Studies (CSIS) are generally consistent with or similar to GAO's recommendations in several areas including: establishing an international cybersecurity strategy, protecting cyber critical infrastructure, promoting use of the NIST cybersecurity framework, prioritizing cybersecurity research, and expanding cybersecurity workforces.