April 24, 2018

CYBERSECURITY

DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks

Highlights of GAO-18-520T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

The emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. GAO first designated information security as a government-wide high-risk area in 1997. GAO expanded the high-risk area to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

Federal law and policy provide DHS with broad authorities to improve and promote cybersecurity. DHS plays a key role in strengthening the cybersecurity posture of the federal government and promoting cybersecurity of systems supporting the nation's critical infrastructures.

This statement highlights GAO's work related to federal programs implemented by DHS that are intended to improve federal cybersecurity and cybersecurity over systems supporting critical infrastructure. In preparing this statement, GAO relied on a body of work issued since fiscal year 2016 that highlighted, among other programs, DHS's NCPS, national integration center activities, and cybersecurity workforce assessment efforts.

What GAO Recommends

Since fiscal year 2016, GAO has made 29 recommendations to DHS to enhance the capabilities of NCPS, establish metrics and methods for evaluating performance, and fully assess its cybersecurity workforce, among other things. As of April 2018, DHS had not demonstrated that it had fully implemented most of the recommendations.

View GAO-18-520T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In recent years, the Department of Homeland Security (DHS) has acted to improve and promote the cybersecurity of federal and private-sector computer systems and networks, but further improvements are needed. Specifically, consistent with its statutory authorities, DHS has made important progress in implementing programs and activities that are intended to mitigate cybersecurity risks on the computer systems and networks supporting federal operations and our nation's critical infrastructure. For example, the department has:

- provided limited intrusion detection and prevention capabilities to entities across the federal government;
- issued cybersecurity related binding operational directives to federal agencies;
- served as the federal-civilian interface for sharing cybersecurity related information with federal and nonfederal entities;
- promoted the use of the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*; and
- partially assessed its cybersecurity workforce.

Nevertheless, the department has not taken sufficient actions to ensure that it successfully mitigates cybersecurity risks on federal and private-sector computer systems and networks. For example, GAO reported in 2016 that DHS's National Cybersecurity Protection System (NCPS) had only partially met its stated system objectives of detecting and preventing intrusions, analyzing malicious content, and sharing information. GAO recommended that DHS enhance capabilities, improve planning, and support greater adoption of NCPS.

In addition, although the department's National Cybersecurity and Communications Integration Center generally performed required functions such as collecting and sharing cybersecurity related information with federal and non-federal entities, GAO reported in 2017 that the center needed to evaluate its activities more completely. For example, the extent to which the center had performed its required functions in accordance with statutorily defined implementing principles was unclear, in part, because the center had not established metrics and methods by which to evaluate its performance against the principles. Further, in its role as the lead federal agency for collaborating with eight critical infrastructure sectors including the communications and dams sectors, DHS had not developed metrics to measure and report on the effectiveness of its cyber risk mitigation activities or on the cybersecurity posture of the eight sectors.

GAO reported in 2018 that DHS had taken steps to assess its cybersecurity workforce; however, it had not identified all of its cybersecurity positions and critical skill requirements.

Until DHS fully and effectively implements its cybersecurity authorities and responsibilities, the department's ability to improve and promote the cybersecurity of federal and private-sector networks will be limited.