United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10 a.m. ET
Tuesday, April, 24, 2018

CYBERSECURITY

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

Statement of Gregory C. Wilshusen, Director, Information Security Issues

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.

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee:

Thank you for the opportunity to appear at today's hearing on how federal government programs implemented by the Department of Homeland Security (DHS) are mitigating cybersecurity risk for federal and private-sector networks. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater.

At your request, I will provide an overview of our work issued since 2016 related to federal programs implemented by DHS that are intended to improve federal cybersecurity and cybersecurity over systems supporting critical infrastructure. My statement highlights our cybersecurity audit findings and recommendations, including recommendations for improving DHS's implementation of its cybersecurity authorities and management of federal programs to mitigate cyber risks on networks.

In developing this testimony, we relied on our previous reports, as well as information provided by DHS on its actions in response to our previous recommendations.[1] We also considered information security related information that the Office of Management and Budget reported to Congress for fiscal year 2017.[2] A more detailed discussion of the

[1]GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018); GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018); GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017); GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017); GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems*, GAO-17-518T (Washington, D.C.: Mar. 28, 2017); GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017); GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, GAO-17-440T (Washington, D.C.: Feb. 14, 2017); GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017); GAO, *Federal Information Security: Actions Needed to Address Challenges*, GAO-16-885T (Washington, D.C.: Sept. 19, 2016); GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016); GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015); and GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[2]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*, (Washington, D.C.: Mar. 2018).

objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications networks, and financial services—are dependent on computerized (cyber) information systems and electronic data to process, maintain, and report essential information, and to operate and control physical processes. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

Yet, computer networks and systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. These systems are often interconnected with other internal and external systems and networks, including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

Furthermore, safeguarding federal computer systems has been a long-standing concern. This year marks the 21st anniversary of when GAO first designated information security as a government-wide high-risk area in 1997.[3] We expanded this high-risk area to include safeguarding the

[3]GAO designates agencies and program areas as high risk due to their vulnerability to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

systems supporting our nation's critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.[4]

Over the last several years, we have made about 2,500 recommendations to agencies aimed at improving the security of federal systems and information. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because they have not implemented many of these recommendations. As of March 2018, about 885 of our prior information security-related recommendations had not been implemented.

Federal Law and Policy Provide DHS with Broad Authorities to Improve and Promote Cybersecurity

DHS has broad authorities to improve and promote cybersecurity of federal and private-sector networks. The federal laws and policies that underpin these authorities include the following:

- **The Federal Information Security Modernization Act (FISMA) of 2014**[5] clarified and expanded DHS's responsibilities for assisting with the implementation of, and overseeing, information security at federal agencies. These responsibilities include requirements to:
  - develop, issue, and oversee agencies' implementation of binding operational directives to agencies, including directives for incident reporting, contents of annual agency reports, and other operational requirements;
  - monitor agencies' implementation of information security policies and practices; and
  - provide operational and technical assistance to agencies, including by operating the federal information security incident center, deploying technology to continuously diagnose and mitigate threats, and conducting threat and vulnerability assessments of systems.

[4]GAO-17-317.

[5]The *Federal Information Security Modernization Act of 2014* was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code.

- **The Homeland Security Cybersecurity Workforce Assessment Act of 2014,** among other things, requires DHS to assess its cybersecurity workforce.[6] In this regard, the Secretary of Homeland Security is to identify all positions in DHS that perform cybersecurity functions and to identify cybersecurity work categories and specialty areas of critical need.
- **The National Cybersecurity Protection Act of 2014**[7] codified the role of the National Cybersecurity and Communications Integration Center (NCCIC)—a center established by DHS in 2009—as the federal civilian interface for sharing information concerning cybersecurity risks, incidents, analysis, and warnings to federal and non-federal entities, including owners and operators of information systems supporting critical infrastructure.
- **The Cybersecurity Act of 2015**, among other things, sets forth authority for enhancing the sharing of cybersecurity-related information among federal and non-federal entities.[8] The act gives DHS's NCCIC responsibility for implementing this information sharing authority. The act also requires DHS to:
  - Jointly develop with other specified agencies and submit to Congress, procedures for sharing federal cybersecurity threat information and defensive measures with federal and non-federal entities.
  - Deploy, operate, and maintain capabilities to prevent and detect cybersecurity risks in network traffic traveling to or from an agency's information system. DHS is to make these capabilities available for use by any agency. In addition, the act requires DHS to improve intrusion detection and prevention capabilities, as appropriate, by regularly deploying new technologies and modifying existing technologies.
- **Long-standing federal policy** as promulgated by a presidential policy directive, executive orders, and the National Infrastructure

[6]*The Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted as section 4 of the *Border Patrol Agent Pay Reform Act of 2014*, Pub. L. No. 113-277 § 4,128 Stat. 2995, 3008-3010 (Dec. 18, 2014); 6 U.S.C. § 146 note.

[7]Pub. L. No. 113-282 (Dec. 18, 2014).

[8]The *Cybersecurity Act of 2015* was enacted into law as Division N of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, 129 Stat. 2935-2985 (Dec. 18, 2015).

Protection Plan have designated DHS as a lead federal agency for coordinating, assisting, and sharing information with the private-sector to protect critical infrastructure from cyber threats.[9]

DHS Has Acted to Improve and Promote the Cybersecurity of Federal and Private-Sector Computer Systems, but Further Improvements Are Needed

We have reviewed several federal programs and activities implemented by DHS that are intended to mitigate cybersecurity risk for the computer systems and networks supporting federal operations and our nation's critical infrastructure. These programs and activities include deploying the National Cybersecurity Protection System, providing continuous diagnostic and mitigation services, issuing binding operational directives, sharing information through the National Cybersecurity and Communications Integration Center, promoting adoption of a cybersecurity framework, and assisting private-sector partners with cyber risk mitigation activities. We also examined DHS's efforts to assess its cybersecurity workforce. DHS has made important progress in implementing these programs and activities. However, the department needs to take additional actions to ensure that it successfully mitigates cybersecurity risks on federal and private-sector computer systems and networks.

DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

DHS is responsible for operating its National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN. NCPS is intended to provide intrusion detection and prevention capabilities to entities across

[9]The White House, *Critical Infrastructure Security and Resilience,* Presidential Policy Directive 21 (Washington, D.C.: Feb. 2013); The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* Exec. Order No. 13800, 82 Fed Reg. 22391 (Washington, D.C.: May 11, 2017); The White House, *Improving Critical Infrastructure Cybersecurity*, Exec. Order No. 13636, 78 Fed Reg. 11739, Vol.78, No. 33 (Feb. 19, 2013); Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013); and Department of Homeland Security, Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, (Dec. 17, 2003).

the federal government. It also is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

In January 2016, we reported that the NCPS was partially, but not fully, meeting most of its stated four system objectives:[10]

- **Intrusion detection:** We noted that NCPS provided DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compared network traffic to known patterns of malicious data, or "signatures," but did not detect deviations from predefined baselines of normal network behavior. In addition, the system did not monitor several types of network traffic and its "signatures" did not address threats that exploited many common security vulnerabilities and, thus was not effective in detecting certain types of malicious traffic.
- **Intrusion prevention:** The capability of NCPS to prevent intrusions (e.g., blocking an e-mail determined to be malicious) was limited to the types of network traffic that it monitored. For example, the intrusion prevention function monitored and blocked e-mail. However, it did not address malicious content from other types of network traffic.
- **Analytics:** NCPS supports a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. In addition, DHS had further enhancements to this capability planned through 2018.
- **Information sharing:** DHS had not developed most of the planned functionality for NCPS's information-sharing capability, and requirements had only recently been approved. Moreover, we noted that agencies and DHS did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on the notifications.

We recommended that DHS take nine actions to enhance NCPS's capabilities for meeting its objectives, better define requirements for

[10]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

future capabilities, and develop network routing guidance. The department agreed with our recommendations; however, as of April 2018, it had not fully implemented 8 of the 9 recommendations. As part of a review mandated by the Federal Cybersecurity Enhancement Act of 2015, we are currently examining DHS's efforts to improve its intrusion detection and prevention capabilities.

DHS Needs to Continue to Advance CDM Program to Protect Federal Systems

The Continuous Diagnostics and Mitigation (CDM) program was established to provide federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that alerts network managers and enables the agency to allocate resources based on the risk.

DHS, in partnership with, and through the General Services Administration, established a government-wide acquisition vehicle for acquiring CDM capabilities and tools. The CDM blanket purchase agreement is available to federal, state, local, and tribal government entities for acquiring these capabilities.

There are three phases of CDM implementation and the dates for implementing Phase 2 and Phase 3 appear to be slipping:

Phase 1: This phase involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the *Cybersecurity Strategy and Implementation Plan*, DHS purchased Phase 1 tools and integration services for all participating agencies in fiscal year 2015.[11]

Phase 2: This phase intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized

[11]Office of Management and Budget, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, OMB Memorandum M-16-04 (Washington, D.C.: Oct. 30, 2015). CSIP identified objectives, key actions, responsibilities, and timeframes for completing actions that were intended to strengthen cybersecurity at federal civilian agencies.

activity. According to the *Cybersecurity Strategy and Implementation Plan*, DHS was to provide agencies with additional Phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of that fiscal year. However, according to the Office of Management and Budget's (OMB) FISMA Annual Report to Congress for Fiscal Year 2017, the CDM program began deploying Phase 2 tools and sensors during fiscal year 2017.[12]

Phase 3: According to DHS, this phase is intended to address boundary protection and event management throughout the security life cycle. It focuses on detecting unusual activity inside agency networks and alerting security personnel. The agency had planned to provide 97 percent of federal agencies the services they need for CDM Phase 3 in fiscal year 2017. However, according to OMB's FISMA report for fiscal year 2017, the CDM program will continue to incorporate additional capabilities, including Phase 3, in fiscal year 2018.

In May 2016,[13] we reported that most of the 18 agencies covered by the CFO Act that had high-impact systems were in the early stages of implementing CDM.[14] All 17 of the civilian agencies that we surveyed indicated they had developed their own strategy for information security continuous monitoring.[15] Additionally, according to the survey responses, 14 of the 17 civilian agencies had deployed products to automate hardware and software asset configuration settings and common vulnerability management.

[12]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*, (Washington, D.C.: 2018).

[13]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016). We surveyed the 18 agencies covered by the Chief Financial Officers (CFO) Act that reported having high-impact systems on a variety of information security-related issues including their implementation of government-wide security initiatives such as the CDM program.

[14]High-impact systems are those where the loss of the confidentiality, integrity, or availability of the information or information system could be expected to have a severe or catastrophic adverse effect on organizations operations, assets, or personnel. For example, it might cause the organization to be unable to perform one or more of its primary functions or result in a major financial loss. Of the 24 CFO Act agencies, 18 reported having high-impact systems at the time of our review.

[15]The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the CDM program.

Further, more than half of these agencies noted that they had leveraged products/tools provided through the General Services Administration's acquisition vehicle. However, only 2 of the 17 agencies reported that they had completed installation of agency and bureau/component-level dashboards and monitored attributes of authorized users operating in their agency's computing environment. Agencies noted that expediting the implementation of the CDM phases could be of benefit to them in further protecting their high-impact systems.

Subsequently, in March 2017, we reported that the effective implementation of the CDM tools and capabilities can assist agencies in overcoming the challenges of securing their information systems and information.[16] We noted that our audits often identify insecure configurations, unpatched or unsupported software, and other vulnerabilities in agency systems. Thus, the tools and capabilities available under the CDM program, when effectively used by agencies, can help them to diagnose and mitigate vulnerabilities to their systems. We reported that, by continuing to make these tools and capabilities available to federal agencies, DHS can also have additional assurance that agencies are better positioned to protect their information systems and information.

Other DHS Services Are Available to Help Protect Systems but Are Not Always Used by Agencies

Beyond the NCPS and CDM programs, DHS also provides a number of services that could help agencies protect their information systems. Such services include, but are not limited to:

- *US-CERT monthly operational bulletins*, which are intended to provide senior federal government information security officials and staff with actionable information to improve their organization's cybersecurity posture based on incidents observed, reported, or acted on by DHS and US-CERT.
- *CyberStat reviews*, which are in-depth sessions attended by National Security Staff, as well as officials from OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration. According to OMB, these interviews are face-to-face,

[16]GAO, Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems, GAO-17-518T (Washington, D.C.: Mar. 28, 2017).

evidence-based meetings intended to ensure agencies are accountable for their cybersecurity posture. The sessions are intended to assist the agencies in developing focused strategies for improving their information security posture in areas where there are challenges.

- *DHS Red and Blue Team exercises* that are intended to provide services to agencies for testing their systems with regard to potential attacks. A Red Team emulates a potential adversary's attack or exploitation capabilities against an agency's cybersecurity posture. The Blue Team defends an agency's information systems when the Red Team attacks, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

In May 2016, we reported that, although participation in these services varied among the 18 agencies we surveyed, most of those that chose to participate reported that they generally found these services to be useful in aiding the cybersecurity protection of their high-impact systems.[17] Specifically,

- 15 of 18 agencies reported that they participated in US-CERT monthly operational bulletins, and most said they found the service very or somewhat useful.
- All 18 agencies reported that they participated in the CyberStat reviews, and most said they found the service very or somewhat useful.
- 9 of 18 agencies reported that they participated in DHS' Red/Blue team exercises, and most said they found the exercises to be very or somewhat useful.

Half of the 18 agencies in our survey reported that they wanted an expansion of federal initiatives and services to help protect their high-impact systems. For example, these agencies noted that expediting the implementation of CDM phases, sharing threat intelligence information, and sharing attack vectors, could be of benefit to them in further protecting their high-impact systems. We believe that by continuing to make these services available to agencies, DHS will be better able to assist agencies in strengthening the security of their information systems.

[17]See GAO-16-501.

DHS Has Issued Binding Operational Directives to Federal Agencies

FISMA authorizes DHS to develop and issue binding operational directives to federal agencies and oversee their implementation by agencies. The directives are compulsory and require agencies to take specific actions that are intended to safeguard federal information and information systems from a known threat, vulnerability, or risk.

In September 2017, we reported[18] that DHS had developed and issued four binding operational directives as of July 2017, instructing agencies to:

- mitigate critical vulnerabilities discovered by DHS's NCCIC through its scanning of agencies' Internet-accessible systems;[19]
- participate in risk and vulnerability assessments as well as DHS security architecture assessments conducted on agencies' high-value assets;[20]
- address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC analysis report within 45 days of the directive's issuance;[21] and
- report cyber incidents and comply with annual FISMA reporting requirements.[22]

Since July 2017, DHS has issued two additional binding operational directives instructing agencies to:

- identify and remove the presence of any information security products developed by AO Kaspersky Lab on their information systems and discontinue the use of such products;[23] and

[18]GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

[19]Department of Homeland Security, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*, BOD-15-01 (Washington, D.C.: May 21, 2015).

[20]Department of Homeland Security, *Securing High Value Assets*, BOD-16-01 (Washington, D.C.: June 9, 2016).

[21]Department of Homeland Security, *Threat to Network Infrastructure Devices*, BOD-16-02 (Washington, D.C.: Sept. 27, 2016).

[22]Department of Homeland Security*, 2016 Agency Cybersecurity Reporting Requirements,* BOD-16-03 (Washington, D.C.: Oct. 17, 2016).

- enhance e-mail by, among other things, removing certain insecure protocols, and ensure public facing web sites provide services through a secure connection.[24]

We plan to initiate work later this year to identify and assess DHS's process for developing and overseeing agencies' implementation of binding operational directives.

DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

In February 2017, we reported that NCCIC had taken steps to perform each of its 11 statutorily required cybersecurity functions,[25] such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities.[26] NCCIC managed several programs that provided data used in developing 43 products and services that the center made available to its customers in the private-sector; federal, state, local, tribal and territorial government entities; and other partner organizations. For example, NCCIC issued indicator bulletins, which could contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents, and helped to fulfill its function to coordinate the sharing of such information across the government. Respondents to a survey that we administered to NCCIC's customers varied in their reported use of NCCIC's products but had generally favorable views of the center's activities.

The National Cybersecurity Protection Act also required NCCIC to carry out its functions in accordance with nine implementing principles, to the extent practicable. However, as we reported, the extent to which NCCIC

[23]Department of Homeland Security, *Removal of Kaspersky-Branded Products*, BOD-17-01 (Washington, D.C.: Sept. 13, 2017).

[24]Department of Homeland Security, *Enhance Email and Web Security*, BOD-18-01 (Washington, D.C.: Oct. 16, 2017).

[25]The National Cybersecurity Protection Act of 2014 requires NCCIC to share information and enable real-time actions to address cybersecurity risks and incidents at federal and non-federal entities, and adhere to nine principles when doing so. The Cybersecurity Act of 2015 added two more functions, for a total of 11 cybersecurity functions that the center is to perform.

[26]GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

adhered to the 9 principles when performing the functions was unclear because the center had not yet determined the applicability of the principles to all 11 functions. It also had not established metrics and methods by which to evaluate its performance against the principles.

We also identified several impediments to NCCIC performing its cybersecurity functions more efficiently. For example, the center did not have a centralized system for tracking security incidents and, as a result, could not produce a report on the status of all incidents reported to the center. In addition, the center did not keep current and reliable customer information and was unable to demonstrate that it had contact information for all owners and operators of the most critical cyber-dependent infrastructure assets.

We made nine recommendations to DHS for enhancing the effectiveness and efficiency of NCCIC. Among other activities, these recommendations called for the department to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments. DHS agreed with the recommendations; however, as of April 2018, all nine recommendations remained unimplemented.

Additional Actions by DHS Are Needed for Promoting and Assessing Private-Sector Adoption of the Cybersecurity Framework

An executive order issued by the President in February 2013 (E.O. 13636)[27] states that sector-specific agencies (SSA),[28] which include DHS, are to review the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (cybersecurity framework) [29] and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

[27]Exec. Order No. 13636, 78 Fed Reg. 11739, *Improving Critical Infrastructure Cybersecurity*, Vol.78, No. 33 (Feb. 19, 2013).

[28] Sector-specific agencies are federal agencies that are to serve as a federal interface for the prioritization and coordination of security and resilience efforts for the critical infrastructure sector for which they have lead roles. The sector-specific agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury; the Environmental Protection Agency; and the General Services Administration.

[29] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014).

In February 2014, DHS launched the Critical Infrastructure Cyber Community Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage adoption of the framework across the critical infrastructure sectors.[30] In addition, DHS, as the SSA and co-SSA for 10 critical infrastructure sectors, had developed framework implementation guidance for some of the sectors it leads.

Nevertheless, we reported weaknesses in DHS's efforts to promote the use of the framework across the sectors and within the sectors it leads. Specifically, in December 2015, we reported that DHS did not measure the effectiveness of cyber community voluntary program to encourage use of the Cybersecurity Framework.[31] In addition, DHS and GSA, which are the co-SSAs for the government facilities sector, had yet to determine if sector implementation guidance should be developed for the government facilities sector. Further, in February 2018, we reported that none of the SSAs, to include DHS, had measured the cybersecurity framework's implementation by entities within their respective sectors, in accordance with the nation's plan for national critical infrastructure protection efforts.[32]

We made two recommendations to DHS to better facilitate adoption of the Cybersecurity Framework across the critical infrastructure sectors and within the government facilities sector. We also recommended that DHS develop methods for determining the level and type of framework adoption by entities across their respective sectors. DHS concurred with the two recommendations. As of April 2018, only the recommendation related to the government facilities sector has been implemented.

DHS Needs to Better Measure Effectiveness of Cyber Risk Mitigation Activities with Critical Infrastructure Sector Partners

Presidential Policy Directive-21 issued by the President in February 2013, states that SSAs are to collaborate with critical infrastructure owners and

[30]Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[31]GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 2015).

[32]GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 2018).

operators to strengthen the security and resiliency of the nation's critical infrastructure.[33]

In November 2015, we reported that the SSAs, including DHS, generally used multiple public-private mechanisms to facilitate the sharing of cybersecurity related information.[34] For example, DHS used coordinating councils and working groups of federal and nonfederal stakeholders to facilitate coordination with each other. In addition, the department's NCCIC received and disseminated cyber-related information for public and private-sector partners.

Nevertheless, we identified deficiencies in critical infrastructure partners' efforts to collaborate to monitor progress towards improving cybersecurity within the sectors.[35] Specifically, the SSAs for 12 sectors, including DHS for 8 sectors, had not developed metrics to measure and report on the effectiveness of their cyber risk mitigation activities or their sectors' cybersecurity posture. This was because, among other reasons, the SSAs rely on their private-sector partners to voluntarily share information needed to measure efforts.

We made two recommendations to DHS—one recommendation based on its role as the SSA for 8 sectors and one recommendation based on its role as the co-SSA for 1 sector—to collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities.[36] DHS concurred with the two recommendations. As of April 2018, DHS has not demonstrated that it has implemented these recommendations.

DHS has taken Steps to Identify its Workforce Gaps; However, It Urgently Needs to Take Actions to Identify Its Position and Critical Skill Requirements

In February 2018, we reported that DHS had taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, as required by the Homeland Security Cybersecurity Workforce Assessment Act of 2014. However, its actions had not been timely and

[33]The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 2013)

[34]GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress,* GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[35]GAO-16-79.

[36]GAO-16-79.

complete.[37] For example, DHS had not met statutorily defined deadlines for completing actions to identify and assign codes to cybersecurity positions or ensured that its procedures to identify, categorize, and code its cybersecurity positions addressed vacant positions, as required by the act. The department also had not (1) identified the individual within each DHS component agency who was responsible for leading and overseeing the identification and coding of the component's cybersecurity positions or (2) reviewed the components' procedures for consistency with departmental guidance.

In addition, DHS had not yet completed its efforts to identify all of the department's cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. In August 2017, DHS reported to the Congress that it had coded 95 percent of the department's identified cybersecurity positions. However, we determined that the department had, at that time, coded approximately 79 percent of the positions. DHS overstated the percentage of coded positions primarily because it excluded vacant positions, even though the act required the department to report such positions.

Further, although DHS had taken steps to identify its workforce capability gaps, it had not identified or reported to the Congress on its department-wide cybersecurity critical needs that align with specialty areas. The department also had not annually reported its cybersecurity critical needs to the Office of Personnel Management (OPM), as required; and it had not developed plans with clearly defined time frames for doing so.

We recommended that DHS take six actions, including ensuring that its cybersecurity workforce procedures identify position vacancies and responsibilities; reported workforce data are complete and accurate; and plans for reporting on critical needs are developed. DHS concurred with the six recommendations and stated that it plans to take actions to address them by June 2018.

In conclusion, DHS is unique among federal civilian agencies in that it is responsible for improving and promoting the cybersecurity of not only its own internal computer systems and networks but also those of other federal agencies and the private-sector owners and operators of critical infrastructure. Consistent with its statutory authorities and responsibilities

[37]GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018).

under federal policy, the department has acted to assist federal agencies and private-sector partners in bolstering their cybersecurity capabilities.

However, the effectiveness of DHS's activities has been limited or not clearly understood because of shortcomings with its programs and a lack of useful performance measures. DHS needs to enhance its capabilities; expedite delivery of services; continue to provide guidance and assistance to federal agencies and private-sector partners; and establish useful performance metrics to assess the effectiveness of its cybersecurity-related activities. In addition, developing and maintaining a qualified cybersecurity workforce needs to be a priority for the department. Until it fully and effectively performs its cybersecurity authorities and responsibilities, DHS's ability to improve and promote the cybersecurity of federal and private-sector networks will be limited.

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, this concludes my statement. I would be pleased to respond to your questions.

GAO Contacts and Staff Acknowledgments

If you or your staffs have any questions about this testimony, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Larry Crosland, Tammi Kalugdan, David Plocher, Di'Mond Spencer, and Priscilla Smith.

102749

Related GAO Products

GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018).

GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017).

GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems*, GAO-17-518T (Washington, D.C.: Mar. 28, 2017).

GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, GAO-17-440T (Washington, D.C.: Feb. 14, 2017).

GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).

GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).