United States Government Accountability Office

Testimony

Before the Committee on Science, Space, and Technology, Subcommittee on Research and Technology

For Release on Delivery
Expected at 10 a.m EST
Tuesday, February 14, 2017

CYBERSECURITY

Actions Needed to Strengthen U.S. Capabilities

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

February 14, 2017

CYBERSECURITY

Actions Needed to Strengthen U.S. Capabilities

GAO Highlights

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

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.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee:

Thank you for the opportunity to appear before you to discuss issues related to strengthening U.S. cybersecurity capabilities. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater.

Today, I will provide an overview of our work related to the cybersecurity posture of the federal government and the nation's critical infrastructure,[1] and federal efforts to protect the privacy of personally identifiable information (PII).[2] At your request, I will also identify areas of consistency between our cybersecurity-related recommendations and those made in recent reports by the President's Commission on Enhancing National Cybersecurity (Cybersecurity Commission)[3] and the Center for Strategic & International Studies (CSIS).[4]

My statement is based on our previously published work addressing cybersecurity efforts and our review of the two recent reports issued by the Cybersecurity Commission and CSIS. The GAO reports cited in this statement contain detailed discussions of the scope of the work and the methodology used to carry it out.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[1]Critical infrastructure includes systems and assets so vital to the United States that incapacitating or destroying them would have a debilitating effect on national security. Mostly owned and operated by the private sector, these critical infrastructures are grouped by the following industries or "sectors": 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 (IT); nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[3]Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (December 1, 2016).

[4]Center for Strategic & International Studies, *From Awareness to Action: A Cybersecurity Agenda for the 45th President* (Washington, D.C.: January 2017).

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. 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, ineffective controls could have a significant impact on a broad array of government operations and assets. For example,

- resources, such as payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes, including the launching of attacks on others;
- sensitive information, such as intellectual property, national security data, and PII such as taxpayer data, Social Security records, and medical records could be inappropriately added, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- entity missions could be undermined by embarrassing incidents that result in diminished confidence in the entity's ability to conduct operations and fulfill its responsibilities.

Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For

example, the national vulnerability database maintained by the National Institute of Standards and Technology (NIST) has identified 82,384 publicly known cybersecurity vulnerabilities and exposures as of February 9, 2017, with more being added each day.[5] Federal systems and networks are also 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.

In addition, cyber threats to systems supporting the federal government and critical infrastructure are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Risks to cyber assets can originate from unintentional and intentional threats. These include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Ineffectively protecting cyber assets can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety.

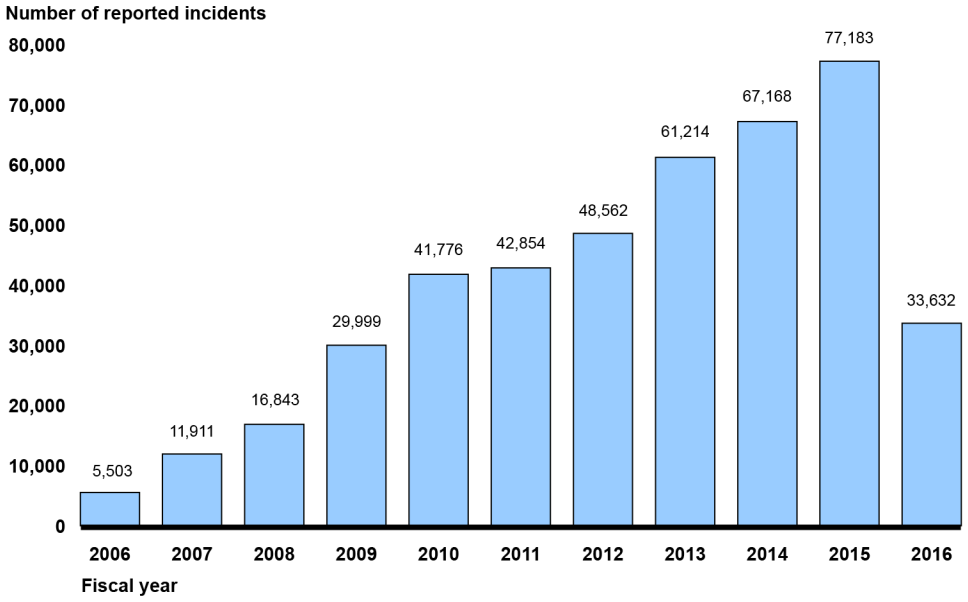
Until fiscal year 2016, the number of information security incidents reported by federal agencies to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT)[6] had steadily increased each year. From fiscal year 2006 through fiscal year 2015, reported security incidents increased from 5,503 to 77,183, an increase of 1,303 percent. However, the number of reported incidents

[5]The national vulnerability database is the U.S. government repository of standards based vulnerability management data. The database includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

[6]US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

decreased by 56 percent in fiscal year 2016 to 33,632, as shown in figure 1.

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2016



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2016.

An official from DHS's National Cybersecurity and Communications Integration Center stated that the decrease in reported incidents for fiscal year 2016 was likely due to revised incident reporting requirements that no longer require agencies to report non-cyber incidents or attempted scans or probes of agency networks. The official also cited the expanded use of the National Cybersecurity Protection System[7] to detect or block potentially malicious network traffic entering networks at federal agencies as another possible reason for fewer reported incidents.

Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—has been a long-standing concern. GAO first designated

[7]The National Cybersecurity Protection System 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. See GAO-16-294 for results of GAO's review of this system.

information security as a government-wide high-risk area[8] in 1997; it then expanded this high risk area to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of PII in 2015.[9]

Over the last several years, GAO has 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 technical security controls over their computer networks and systems. They also include recommendations for agencies to fully implement aspects of their information security programs, as mandated by the *Federal Information Security Modernization Act* (FISMA) of 2014 and its predecessor, the *Federal Information Security Management Act of 2002*,[10] as well as to protect the privacy of PII held on their systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. As of February 2017, about 1,000 of our information security-related recommendations had not been implemented.

Action Is Needed to Address Ongoing Cybersecurity and Privacy Challenges

Our work has identified the need for improvements in the federal government's approach to cybersecurity of its systems and those supporting the nation's critical infrastructures and in protecting the privacy of PII. While previous administrations and agencies have acted to improve the protections over the information and information systems supporting federal operations and U.S. critical infrastructure, additional actions are needed.

Federal agencies need to effectively implement risk-based entity-wide information security programs consistently over time. Since the first FISMA was enacted in 2002, agencies have been challenged to fully

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

[9]See GAO, *High-Risk List: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[10]The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, Dec. 17, 2002). As used here, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

and effectively develop, document, and implement the entity-wide information security program required by FISMA to protect the information and information systems that support their operations and assets, including those provided or managed by another agency or contractor. For example, as of February 7, 2017, 19 of 23 federal agencies covered by the *Chief Financial Officers Act* (CFO Act)[11] that had issued their required annual financial reports for fiscal year 2016[12] reported that information security control deficiencies were either a material weakness or significant deficiency[13] in internal controls over financial reporting for fiscal year 2016. In addition, inspectors general at 20 of the 23 agencies identified information security as a major management challenge for their agencies.

Further, in light of these challenges, we have identified a number of actions to assist agencies in implementing their information security programs.

- *Enhance capabilities to effectively identify cyber threats to agency systems and information.* A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent. The impairments included an inability to recruit and retain

[11]Twenty-four agencies are covered by the CFO Act: Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management (OPM); Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[12]As February 7, 2017, 23 of the 24 CFO Act agencies had issued their annual financial report for fiscal year 2016. The Department of Defense has not issued its annual financial report for fiscal year 2016.

[13]A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a deficiency, or combination of deficiencies, in internal that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

personnel with the appropriate skills, rapidly changing threats, continuous changes in technology, and a lack of government-wide information sharing mechanisms.[14] Addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.

- *Implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices.* We routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. Establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of federal agencies.
- *Patch vulnerable systems and replace unsupported software.* Federal agencies consistently fail to apply critical security patches on their systems in a timely manner, sometimes doing so years after the patch becomes available. We also consistently identify instances where agencies use software that is no longer supported by their vendors. These shortcomings often place agency systems and information at significant risk of compromise, since many successful cyberattacks exploit known vulnerabilities associated with software products. Using vendor-supported and patched software will help to reduce this risk.
- *Develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis.* Federal agencies we reviewed often did not test or evaluate their information security controls in a comprehensive manner. The evaluations were sometimes based on interviews and document reviews, limited in scope, and did not identify many of the security vulnerabilities that our examinations identified. Conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.
- *Strengthen oversight of contractors providing IT services.* As demonstrated by the OPM data breach of 2015, cyber attackers can sometimes gain entry to agency systems and information through the

[14]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

agency's contractors or business partners. Accordingly, agencies need to assure that their contractors and partners are adequately protecting the agency's information and systems. In August 2014, we reported that five of six selected agencies were inconsistent in overseeing the execution and review of security assessments that were intended to determine the effectiveness of contractor implementation of security controls, resulting in security lapses.[15] In 2016, agency chief information security officers (CISOs) we surveyed reported that they were challenged to a large or moderate extent in overseeing their IT contractors and receiving security data from the contractors. This challenge diminished their ability to assess how well agency information maintained by the contractors is protected.[16] Effectively overseeing and reviewing the security controls implemented by contractors and other parties is essential to ensuring that the agency's information is properly safeguarded.

We have several ongoing and planned audit engagements that will continue to assess the effectiveness of agency actions to implement information security programs. These engagements include in-depth assessments of information security programs at individual agencies including OPM and the Centers for Disease Control and Prevention as well as our biennial review of the adequacy of agencies' information security policies and practices and their compliance with the provisions of FISMA.

Also, on an annual basis, we evaluate information security controls over financial systems and information at seven agencies and incorporate the audit results of agency offices of inspector general during our annual audit of the consolidated financial statements of the federal government. In addition, we are currently conducting an assessment of the Federal Risk Authorization and Management Program and have plans to review cyber risk management practices and continuous monitoring programs at federal agencies.

The federal government needs to improve its cyber incident detection, response, and mitigation capabilities. Even agencies or organizations with strong security can fall victim to information security

[15]GAO, Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612, (Washington, D.C.: Aug. 8, 2014).

[16]GAO, Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

incidents due to the existence of previously unknown vulnerabilities that are exploited by attackers to intrude into an agency's information systems. Accordingly, agencies need to have effective mechanisms for detecting, responding to, and recovering from such incidents. We have previously identified various actions that could assist the federal government in building its capabilities for detecting, responding to, and recovering from security incidents.

- *Expand capabilities, improve planning, and support wider adoption of the government-wide intrusion detection and prevention system.* In January 2016, we reported that DHS's National Cybersecurity Protection System (NCPS) had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information. In addition, adoption of these capabilities at federal agencies was limited. We noted that expanding NCPS's capabilities for detecting and preventing malicious traffic, defining requirements for future capabilities, 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.[17]
- *Improve cyber incident response practices at federal agencies.* In April 2014 we reported that 24 major federal agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[18] For example, six agencies reviewed had not determined the impact of incidents or taken actions to address the underlying control weaknesses that allowed the incidents to occur, in part because they had not developed comprehensive policies, plans, and procedures for responding to security incidents, and had not tested their incident response capabilities. By developing comprehensive incident response policies, plans, and procedures for responding to incidents and effectively overseeing response activities, agencies will have increased assurance that they will effectively respond to cyber incidents.
- *Update federal guidance on reporting data breaches and develop consistent responses to breaches of PII.* As we reported in December 2013, eight agencies that we reviewed did not consistently implement

[17]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).

[18]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices,* GAO-14-354 (Washington, D.C.: April 30, 2014).

policies and procedures for responding to breaches of PII.[19] For example, none of the agencies had documented the evaluation of incidents and lessons learned. In addition, we noted that OMB guidance calling for agencies to report each PII-related incident—even those with inherently low risk to the individuals affected—within 1 hour of discovery may cause agencies to expend resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches. We recommended that OMB update it guidance on federal agencies' responses to a PII-related data breach and that the agencies we reviewed take steps to improve their response to data breaches involving PII. Updating guidance and consistently implementing breach response practices will improve the effectiveness of governmentwide and agency data breach response programs.

GAO routinely evaluates agencies' intrusion detection, response, and mitigation activities during audits of agency information security controls and programs. We plan to continue to do so during ongoing and future engagements. In addition, the *Cybersecurity Act of 2015*[20] contains a provision for us to study and publish a report by December 2018 on the effectiveness of the approach and strategy of the federal government to secure agency information systems, including the intrusion detection and prevention capabilities and the government's intrusion assessment plan.

The federal government needs to expand its cyber workforce planning and training efforts. Ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge.

- *Enhance efforts for recruiting and retaining a qualified cybersecurity workforce.* This has been a long-standing dilemma for the federal government. In 2013, agency chief information officers and experts we surveyed cited weaknesses in education, awareness, and workforce planning as a root cause in hindering improvements in the

[19]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[20]*The Cybersecurity Act of 2015* was enacted as *Division N of the Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, Dec. 18, 2015.

nation's cybersecurity posture.[21] Several experts also noted that the cybersecurity workforce was inadequate, both in numbers and training. They cited challenges such as the lack of role-based qualification standards and difficulties in retaining cyber professionals. In 2016, agency chief information security officers we surveyed cited difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; and ensuring that security personnel have appropriate skills and expertise as posing challenges to their abilities to carry out their responsibilities effectively.[22]

- *Improve cybersecurity workforce planning activities at federal agencies.* In November 2011, we reported that only five of eight selected agencies had developed workforce plans that addressed cybersecurity.[23] Further, all eight agencies reported challenges with filling cybersecurity positions, and only three of the eight had a department-wide training program for their cybersecurity workforce.

GAO has two current engagements to further review cybersecurity workforce issues in the federal government. T*he Homeland Security Cybersecurity Workforce Assessment Act of 2014*[24] contains a provision for us to monitor, analyze, and report by December 2017 on the Department of Homeland Security's implementation of the National Cybersecurity Workforce Measurement Initiative. In addition, the *Cybersecurity Act of 2015* calls for us to monitor, analyze, and submit a report by December 2018 on the implementation of this initiative and the identification of cyber-related work roles of critical need by federal agencies.

The federal government needs to expand efforts to strengthen cybersecurity of the nation's critical infrastructures. U.S. critical infrastructures such as financial institutions, energy production and transmission facilities, and communications networks, are vital to the U.S. security, economy, and public health and safety. Similar to federal

[21]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb 14, 2013).

[22]GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

[23]GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination,* GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

[24]*Homeland Security Cybersecurity Workforce Assessment Act of 2014*, Pub. L. No. 113-277, (Dec. 18, 2014).

systems, the systems supporting critical infrastructures face an evolving array of cyber-based threats. To help secure infrastructure cyber assets—most of which is owned and operated by the private sector—federal policy and the *National Infrastructure Protection Plan*[25] provide for a public-private partnership in which federal agencies support or assist their private sector partners in securing systems supporting critical infrastructure. We have identified the following actions that can assist agencies in performing these vital services.

- *Develop metrics to assess the effectiveness of efforts promoting the NIST cybersecurity framework.* In December 2015, we reported that NIST and other agencies had promoted the adoption of the *Framework for Improving Critical Infrastructure Cybersecurity* to critical infrastructure owners and operators and other organizations.[26] Toward this end, DHS established the Critical Infrastructure Cyber Community Voluntary Program to encourage entities to adopt the framework. However, DHS had not developed metrics to measure the success of its activities and programs. In addition, DHS and the General Services Administration had not determined whether to develop tailored guidance for implementing the framework in government facilities sector as other agencies had done for their respective sectors. DHS concurred with our recommendation to develop metrics, but has not indicated that it has taken action, and DHS and the General Services Administration concurred with our recommendation to determine whether tailored guidance was needed.
- *Develop metrics to measure and report on the effectiveness of cyber risk mitigation activities and the cybersecurity posture of critical infrastructure sectors.* In November 2015, we reported that all eight sector-specific agencies reviewed had determined the significance of cyber risk to the nation's critical infrastructures and had taken actions to mitigate cyber risks and vulnerabilities for their respective sectors.[27] However, not all sector-specific agencies had metrics to measure and report on the effectiveness of all their activities to mitigate cyber risks

[25]DHS, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, (December 2013).

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

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

or their sectors' cybersecurity posture. We recommended that agencies lacking metrics develop them and determine how to overcome any challenges to reporting the results of their activities to mitigate cyber risks. Four of the agencies explicitly agreed with our recommendations and identified planned or on-going efforts to implement performance metrics; however, they have not yet provided metrics or reports of outcomes.

GAO has several ongoing and planned engagements that will touch on the cybersecurity of national critical infrastructures. Among these engagements, our study of the "Internet of things" addresses the security and privacy implications of this phenomenon. In addition, the *Cybersecurity Enhancement Act of 2014*[28] contains a provision for us to assess the extent to which critical infrastructure sectors have adopted a voluntary cybersecurity framework to reduce cyber risks and the success of such a framework for protecting critical infrastructure against cyber threats. We also plan to review the cybersecurity of oil and gas pipeline control systems and the Department of Homeland Security's efforts to share cyber information with federal and non-federal entities.

The federal government needs to better oversee protection of PII. Regarding PII, advancements in technology, such as new search technology and data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data and track it across large and numerous databases. In addition, lower data storage costs have made it less expensive to store vast amounts of data. Also, ubiquitous Internet and cellular connectivity make it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of PII being exposed and compromised. Our work has identified the following actions that need to be taken to better protect the privacy of personal information.

- *Protect the security and privacy of electronic health information.* In August 2016, we reported that guidance for securing electronic health information issued by Department of Health and Human Services (HHS) did not address all key controls called for by other federal

[28]*Cybersecurity Enhancement Act of 2014,* Pub. L. No. 113-274, (Dec. 18, 2014).

cybersecurity guidance.[29] In addition, this department's oversight efforts did not always offer pertinent technical guidance and did not always follow up on corrective actions when investigative cases were closed. HHS generally concurred with the five recommendations we made and stated that it would take actions to implement them.

- *Ensure privacy when face recognition systems are used.* In May 2016, we reported[30] that the Department of Justice had not been timely in publishing and updating privacy documentation for the Federal Bureau of Investigation's (FBI) use of face recognition technology.[31] Publishing such documents in a timely manner would better assure the public that the FBI is evaluating risks to privacy when implementing systems. Also, the FBI had taken limited steps to determine whether the face recognition system it was using was sufficiently accurate. We recommended that the department ensure required privacy-related documents are published and that the FBI test and review face recognition systems to ensure that they are sufficiently accurate. Of the six recommendations we made, the Department of Justice agreed with one, partially agreed with two, and disagreed with three. The agency has not yet provided information about the actions it has taken to address the recommendations.
- *Protect the privacy of users' data on state-based marketplaces.* In March 2016, we reported on weaknesses in technical controls for the "data hub" that the Centers for Medicare and Medicaid Services (CMS) uses to exchange information between its health insurance marketplace and external partners.[32] We also identified significant weaknesses in the controls in place at three selected state-based

[29]GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

[30]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[31]Face recognition technology uses biometrics—the automated recognition of individuals based on their biological and behavioral characteristics—to identify the identity of individuals based on a comparison of a photograph of an unknown person against a database of photographs of known persons. Specifically, the technology extracts features from the faces and puts them into a format—often referred to as a faceprint—that can be used for verification, among other things. Once the faceprint has been created, the technology can use a face recognition algorithm to compare the faceprints against each other to produce a single score value that represents the degree of similarity between the two faces.

[32]GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls,* GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

marketplaces established to carry out provisions of the *Patient Protection and Affordable Care Act*.[33] We recommended that CMS define procedures for overseeing the security of state-based marketplaces and require continuous monitoring of state marketplace controls. HHS concurred with our recommendations and stated it has taken or plans to take actions to address these recommendations.

GAO has several ongoing and planned reviews that address actions intended to protect the privacy of PII. For example, we are assessing agency efforts and government-wide initiatives to reduce or eliminate the use of Social Security numbers. In addition, the *Cybersecurity Act of 2015* calls for us to review and report by December 2018 on agency policies and actions taken by the federal government to remove PII from shared cyber threat indicators or defensive measures. Further, the *21st Century Cures Act of 2016* requires us to review and report by December 2018 on the policies and activities of the Office of the National Coordinator for Health Information Technology to ensure appropriate matching to protect patient privacy and security with respect to electronic health records.[34]

Several Recommendations Made by the Cybersecurity Commission and CSIS Are Generally Consistent with GAO's Recommendations for Improving Cybersecurity

Recent reports by the Cybersecurity Commission and CSIS identify topical areas and numerous recommendations for the new administration to consider as it develops and implements cybersecurity strategy and policy. In its study, the Commission focused on 10 cybersecurity topics including international issues, critical infrastructure, cybersecurity research and development, cybersecurity workforce, and the Internet of Things. CSIS addressed similar topics and identified five major issues related to international strategy, securing government agencies and critical infrastructure, cybersecurity research and workforce development, cybercrime, and defending cyberspace.

Over the last several years, GAO has reviewed many of the areas covered by the Commission and CSIS reports. Our conclusions and recommendations are generally directed to specific agencies and may be more limited in scope than the recommendations of the Commission and CSIS. Nevertheless, several of our recommendations are generally

[33]Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the *Health Care and Education Reconciliation Act of 2010*, Pub. L. No. 111-152,124 Stat.1029 (Mar. 30, 2010).

[34]*21st Century Cures Act of 2016,* Pub L. No. 114-255, Div. A, Title IV, Sec. 4007 (December 13, 2016).

consistent with or similar to recommendations made by the Commission and CSIS in the following areas:

- *International cybersecurity strategy.* In July 2010, we identified a number of challenges confronting U.S. involvement in global cybersecurity and governance.[35] These include developing a comprehensive national strategy; ensuring international standards and policies do not pose unnecessary barriers to U.S. trade; participating in international cyber-incident response and appropriately sharing information without jeopardizing national security; investigating and prosecuting transnational cybercrime; and contending with differing laws and norms of behavior. We made five recommendations to the administration's cybersecurity coordinator to address these challenges, to include developing a comprehensive national global cyberspace strategy and defining cyberspace norms. In their recent reports, the Commission and CSIS also identified actions for enhancing international cybersecurity strategy and policies and agreeing on norms of behavior with like-minded nations.
- *Protecting cyber critical infrastructure*. In November 2015, we reported that sector specific agencies—federal agencies that are responsible for collaborating with their private sector counterparts in their assigned critical infrastructure sectors—were acting to address sector cyber risk by sharing information, supporting incident response activities, and providing technical assistance. However, they had not developed metrics to measure and improve the effectiveness of their cyber risk mitigation activities or their sectors' cybersecurity posture.[36] We recommended that the agencies develop performance metrics to monitor and improve the effectiveness of their cyber risk mitigation activities. In their recent reports, the Commission and CSIS also identified actions for enhancing the public-private partnership, including improving information sharing, incident response capabilities, and cyber risk management practices.
- *Promoting Use of the NIST Cybersecurity Framework*. In December 2015, we reported that NIST had developed a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure, known as the *Framework for Improving Critical*

[35]GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

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

Infrastructure Cybersecurity. We also reported that although DHS had established a program dedicated to encouraging the framework's adoption, it had not established metrics to assess the effectiveness of these efforts. We recommended that DHS develop metrics for measuring the effectiveness of efforts to promote and support the framework. Similarly, both the Commission and CSIS have recommended actions to promote and measure use of the framework.

- *Prioritizing cybersecurity research and development (R&D)*. In June 2010, we reported that the federal government lacked a prioritized national R&D agenda and a data repository to track research and development projects and funding, as required by law.[37] We recommended that the Office of Science and Technology Policy (OSTP) take several steps, including developing a comprehensive national R&D agenda that identifies priorities for short-term, mid-term, and long-term complex R&D projects and is guided by input from the public and private sectors. Similarly, in its report, the Commission stated that OSTP, as part of an overall R&D agenda, should lead the development of an integrated government-private-sector cybersecurity roadmap for developing defensible systems.
- *Expanding cybersecurity workforce capabilities.* As discussed earlier in this statement, we have reported that ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge. Consistent with this view, the Commission and CSIS have identified actions to address improving the nation's cybersecurity workforce, including increasing the number of cybersecurity practitioners; implementing a range of education and training programs at the federal, state, and local levels; providing incentives for individuals to enter the workforce; and allocating additional funds at key departments for cybersecurity education and training programs.
- *Combatting cybercrime*. In June 2007, we identified a number of challenges impeding public and private entities efforts in mitigating cybercrime, including working in a borderless environment[38] with laws

[37]GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development*, GAO-10-466 (Washington, D.C.: June 3, 2010).

[38]Cybercriminals are not hampered by physical proximity or borders. Cybercriminals can be physically located in one nation or state, direct their crime through computers in multiple nations or states, and store evidence of the crime on computers in yet another nation or state.

of multiple jurisdictions.[39] We stated that efforts to investigate and prosecute cybercrime are complicated by the multiplicity of laws and procedures that govern in the various nations and states where victims may be found, and the conflicting priorities and varying degrees of expertise of law enforcement authorities in those jurisdictions. In addition, laws used to address cybercrime differ across states and nations. For example, an act that is illegal in the United States may be legal in another nation or not directly addressed in the other nation's laws. Developing countries, for example, may lack cybercrime laws and enforcement procedures. In its recent report, CSIS stated that many countries still do not have adequate cybercrime laws and recommended that (1) countries that refuse to cooperate with law enforcement should be penalized in some way and (2) methods be found to address the concerns of countries not willing to sign an existing treaty addressing cybercrime.

In summary, the dependence of the federal government and the nation's critical infrastructure on computerized information systems and electronic data makes them potentially vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's security, prosperity, and well-being. Nevertheless, the security over these systems is inconsistent and additional actions are needed to address ongoing cybersecurity and privacy challenges. Specifically, federal agencies need to address control deficiencies and fully implement organization-wide information security programs, cyber incident response and mitigation efforts needs to be improved across the government, maintaining a qualified cybersecurity workforce needs to be a priority, efforts to bolster the cybersecurity of the nation's critical infrastructure needs to be strengthened, and the privacy of PII needs to be better protected. Several recommendations made by the Commission and CSIS are generally consistent with previous recommendations made by GAO and warrant close consideration.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, this concludes my statement. I would be happy to respond to your questions.

[39]GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

GAO Contact and Staff Acknowledgments

If you or your staff 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 Michael Gilmore, Nancy Glover, and Kush Malhotra.

Related GAO Products

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, Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority, GAO-16-686. (Washington, D.C.: Aug. 26, 2016).

GAO, Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

GAO, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, GAO-16-267 (Washington, D.C.: May 16, 2016) (Reissued August 3, 2016).

GAO, Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems, GAO-16-501 (Washington, D.C.: May 18, 2016).

GAO, Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls, GAO-16-265 (Washington, D.C.: Mar. 23, 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).

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

GAO, Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

GAO, Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

GAO, Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance, GAO-10-606 (Washington, D.C.: July 2, 2010).