United States Government Accountability Office

Report to Congressional Committees

September 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

GAO-18-622

GAO Highlights

Highlights of GAO-18-622, a report to congressional committees

September 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

This report provides an update to the information security high-risk area. To do so, GAO identified the actions the federal government and other entities need to take to address cybersecurity challenges. GAO primarily reviewed prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. GAO also reviewed recent cybersecurity policy and strategy documents, as well as information security industry reports of recent cyberattacks and security breaches.

What GAO Recommends

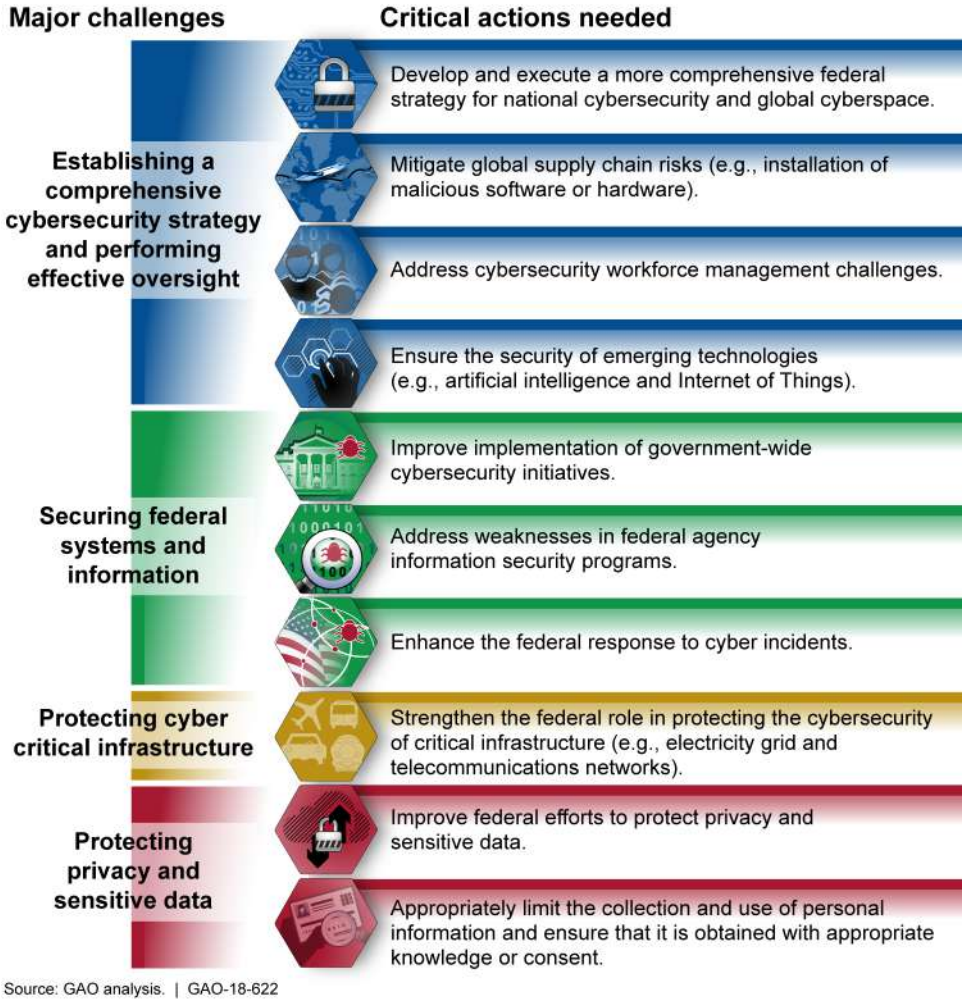
GAO has made over 3,000 recommendations to agencies since 2010 aimed at addressing cybersecurity shortcomings. As of August 2018, about 1,000 still needed to be implemented.

View GAO-18-622. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them. GAO continues to designate information security as a government-wide high-risk area due to increasing cyber-based threats and the persistent nature of security vulnerabilities.

Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Source: GAO analysis. | GAO-18-622

GAO has made over 3,000 recommendations to agencies aimed at addressing cybersecurity shortcomings in each of these action areas, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Although many recommendations have been addressed, about 1,000 have not yet been implemented. Until these shortcomings are addressed, federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist.

Contents

Tables

Figures

Abbreviations

CFO	Chief Financial Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
DHS	Department of Homeland Security
DOD	Department of Defense
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
HHS	Department of Health and Human Services
IRS	Internal Revenue Service
IT	information technology
IoT	Internet of Things
NCCIC	National Cybersecurity and Communications Integration Center
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
SSN	Social Security number
US-CERT	United States Computer Emergency Readiness Team

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 6, 2018

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Trey Gowdy
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Federal agencies and our nation's critical infrastructures[1]—such as energy, transportation systems, communications, and financial services—are dependent on information technology (IT) 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 national security, prosperity, and well-being.

Many of these systems contain vast amounts of personally identifiable information (PII),[2] thus making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents, when they occur. Underscoring the importance of this issue, we continue to designate information security as

[1]The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). 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.

[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.

a government-wide high-risk area in our most recent biennial report to Congress—a designation we have made in each report since 1997.[3]

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

In particular, foreign nations—where adversaries may possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Rapid developments in new technologies, such as artificial intelligence and the Internet of Things (IoT),[4] makes the threat landscape even more complex and can also potentially introduce security, privacy, and safety issues that were previously unknown.

Compounding these risks, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities 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. This is illustrated by significant security breaches reported by the Office of Personnel Management (OPM) in 2015 that resulted in the loss of PII for an estimated 22.1 million individuals and, more recently, in 2017, a security breach reported by Equifax—one of the nation's largest credit bureaus—that resulted in the loss of PII for an estimated 148 million U.S. consumers.

[3]See GAO, *High-Risk Series: An Update*, GAO-17-317 (Washington, D.C.: February 2017) and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[4]IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

This report provides an update to the information security high-risk area by identifying actions that the federal government and other entities need to take to address cybersecurity challenges facing the nation. To do so, this report reflects work we conducted since the prior high-risk update was issued in February 2017, among other things.[5] We also plan to issue an updated assessment of this high-risk area in February 2019.

In conducting the work for this update, we first identified cybersecurity areas in which the federal government has experienced challenges. To do so, we primarily reviewed our prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas (see appendix I for a list of our prior work).

We also reviewed recent cybersecurity policy and strategy documents issued by the current administration, such as Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*;[6] the National Security Strategy;[7] and the Department of Homeland Security's (DHS) May 2018 cybersecurity strategy.[8] We then analyzed these documents to determine the extent to which they included GAO's desirable characteristics of a national strategy.[9] We also reviewed recent media and information security industry reports of cyberattacks and security breaches. Based on these actions, we identified four cybersecurity areas in which federal agencies had experienced challenges.

[5]GAO-17-317.

[6]Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

[7]The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: Dec. 2017).

[8]DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018). DHS has broad authorities to improve and promote cybersecurity of federal and private-sector networks. Specifically, long-standing federal policy as promulgated by a presidential policy directive, executive orders, and the National Infrastructure 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]In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

To identify the actions needed to address each challenge area, we reviewed the findings of our work specific to each challenge, the status of our prior recommendations to the Executive Office of the President and federal agencies, and any actions taken by these entities to address our recommendations. In reviewing the status of prior recommendations, we also determined which recommendations had not been implemented and what additional actions, if any, the Executive Office of the President and federal agencies needed to take in order to address them. We then summarized the actions needed and the status of our prior recommendations. We also identified our ongoing work related to each action.

We performed our work at the initiative of the U.S. Comptroller General. We conducted this performance audit from February 2018 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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 a reasonable basis for our findings and conclusions based on our audit objectives.

Background

IT systems supporting federal agencies and our nation's critical infrastructures are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including the Internet. This increases the number of avenues of attack and expands their attack surface. As systems become more integrated, cyber threats will pose an increasing risk to national security, economic well-being, and public health and safety.

Advancements in technology, such as data analytics software for searching and collecting information, have also made it easier for individuals and organizations to correlate data (including PII) and track it across large and numerous databases. For example, social media has been used as a mass communication tool where PII can be gathered in vast amounts. In addition, ubiquitous Internet and cellular connectivity makes 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.

Cybersecurity incidents continue to impact entities across various critical infrastructure sectors. For example, in its 2018 annual data breach investigations report,[10] Verizon reported that 53,308 security incidents and 2,216 data breaches were identified across 65 countries in the 12 months since its prior report. Further, the report noted that cybercriminals can often compromise a system in just a matter of minutes—or even seconds, but that it can take an organization significantly longer to discover the breach. Specifically, the report stated nearly 90 percent of the reported breaches occurred within minutes, while nearly 70 percent went undiscovered for months.

These concerns are further highlighted by the number of information security incidents reported by federal executive branch civilian agencies to DHS's U.S. Computer Emergency Readiness Team (US-CERT).[11] For fiscal year 2017, 35,277 such incidents were reported by the Office of Management and Budget (OMB) in its 2018 annual report to Congress, as mandated by the Federal Information Security Modernization Act (FISMA).[12] These incidents include, for example, web-based attacks, phishing,[13] and the loss or theft of computing equipment.

[10]Verizon, *2018 Data Breach Investigation Report-11th Edition* (April 2018).

[11]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.

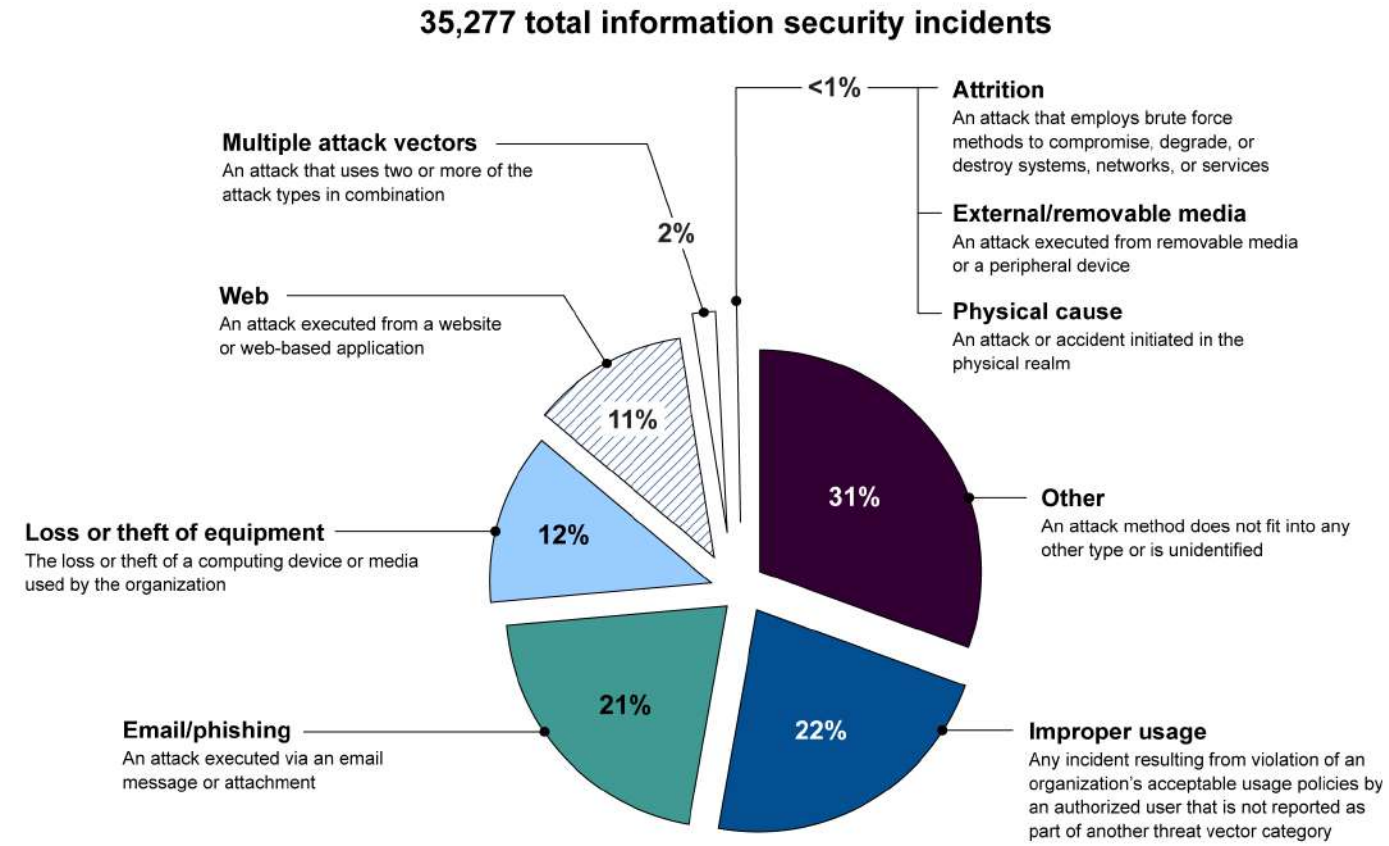
[12] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[13]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

Different types of incidents merit different response strategies. However, if an agency cannot identify the threat vector (or avenue of attack),[14] it could be difficult for that agency to define more specific handling procedures to respond to the incident and take actions to minimize similar future attacks. In this regard, incidents with a threat vector categorized as "other" (which includes avenues of attacks that are unidentified) made up 31 percent of the various incidents reported to US-CERT. Figure 1 shows the percentage of the different types of incidents reported across each of the nine threat vector categories for fiscal year 2017, as reported by OMB.

[14]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack. US-CERT's Federal Incident Notification Guidelines specify nine potential attack vectors agencies should use to describe incident security incidents during reporting.

Figure 1: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2017



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2017. | GAO-18-622

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. The following examples highlight the impact of such incidents:

- In March 2018, the Mayor of Atlanta, Georgia, reported that the city was victimized by a ransomware[15] cyberattack. As a result, city government officials stated that customers were not able to access

[15]According to DHS, ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

multiple applications that are used to pay bills or access court related information. In response to the attack, the officials noted that they were working with numerous private and governmental partners, including DHS, to assess what occurred and determine how best to protect the city from future attacks.

- In March 2018, the Department of Justice reported that it had indicted nine Iranians for conducting a massive cybersecurity theft campaign on behalf of the Islamic Revolutionary Guard Corps. According to the department, the nine Iranians allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 U.S. companies, and five federal government agencies, among other entities.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation (FBI)[16] stated that, since at least March 2016, Russian government actors had targeted the systems of multiple U.S. government entities and critical infrastructure sectors. Specifically, the alert stated that Russian government actors had affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.
- In July 2017, a breach at Equifax resulted in the loss of PII for an estimated 148 million U.S. consumers. According to Equifax, the hackers accessed people's names, Social Security numbers (SSN), birth dates, addresses and, in some instances, driver's license numbers.
- In April 2017, the Commissioner of the Internal Revenue Service (IRS) testified that the IRS had disabled its data retrieval tool in early March 2017 after becoming concerned about the misuse of taxpayer data. Specifically, the agency suspected that PII obtained outside the agency's tax system was used to access the agency's online federal student aid application in an attempt to secure tax information through the data retrieval tool. In April 2017, the agency began notifying taxpayers who could have been affected by the breach.
- In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate, but related, incident had compromised its systems and the

[16]The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. The agency's Cyber Division leads efforts to investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

files related to background investigations for 21.5 million individuals. In total, OPM estimated 22.1 million individuals had some form of PII stolen, with 3.6 million being a victim of both breaches.

Federal Information Security Included on GAO's High-Risk List Since 1997

Safeguarding federal IT systems and the systems that support critical infrastructures has been a long-standing concern of GAO. Due to increasing cyber-based threats and the persistent nature of information security vulnerabilities, we have designated information security as a government-wide high-risk area since 1997.[17] In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure.[18] At that time, we highlighted the need to manage critical infrastructure protection activities that enhance the security of the cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety.

We further expanded the information security high-risk area in 2015[19] to include protecting the privacy of PII. Since then, advances in technology have enhanced the ability of government and private sector entities to collect and process extensive amounts of PII, which has posed challenges to ensuring the privacy of such information. In addition, high-profile PII breaches at commercial entities, such as Equifax, heightened concerns that personal privacy is not being adequately protected.

Our experience has shown that the key elements needed to make progress toward being removed from the High-Risk List are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action. The five criteria for removal that we identified in November 2000 are as follows:[20]

- **Leadership Commitment.** Demonstrated strong commitment and top leadership support.

[17]GAO-HR-97-1.

[18]See GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

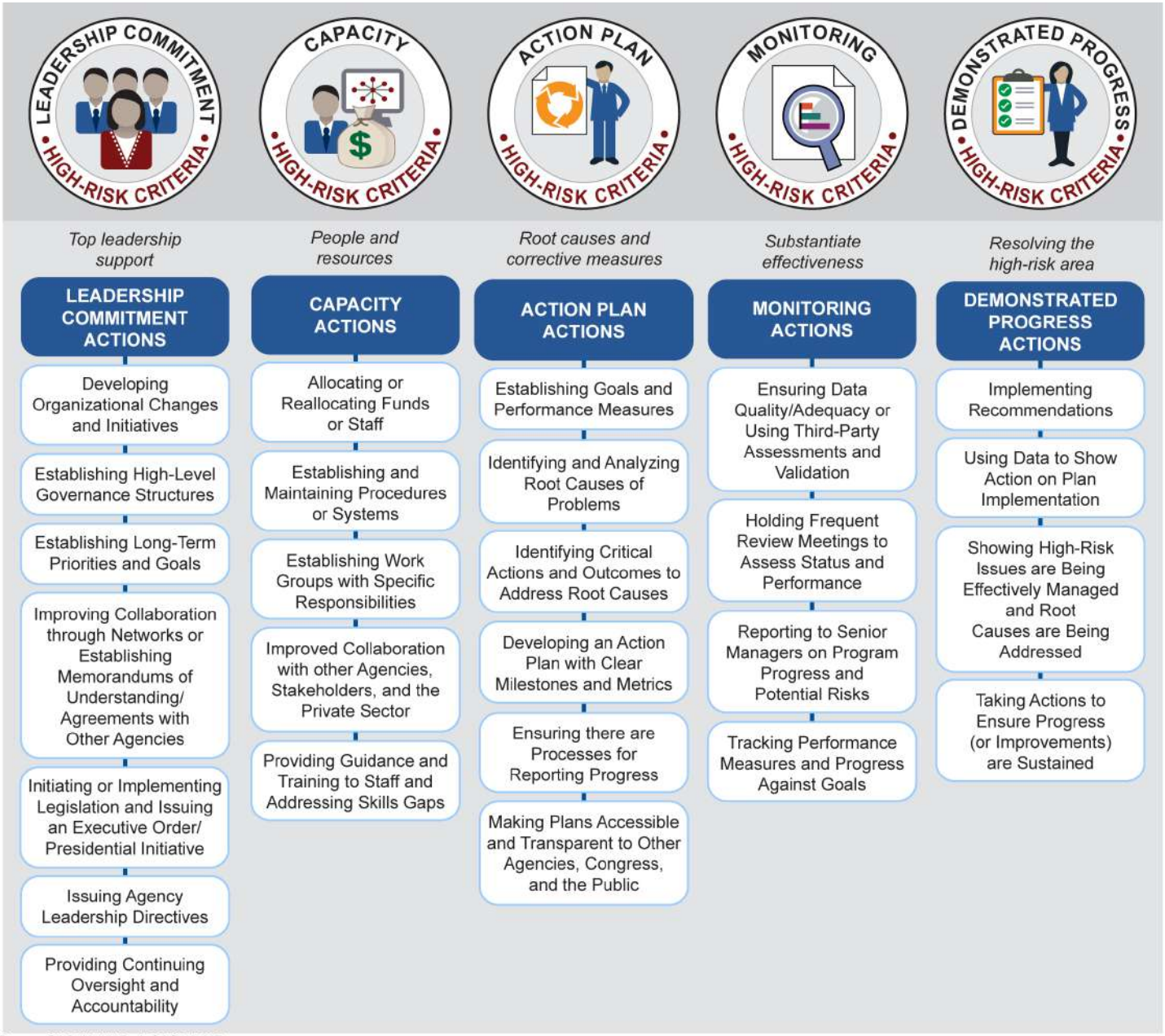
[19]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

[20]GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

- **Capacity**. The agency has the capacity (i.e., people and resources) to resolve the risk(s).
- **Action Plan**. A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.
- **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.
- **Demonstrated Progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

These five criteria form a road map for efforts to improve and ultimately address high-risk issues. Addressing some of the criteria leads to progress, while satisfying all of the criteria is central to removal from the list. Figure 2 shows the five criteria and illustrative actions taken by agencies to address the criteria. Importantly, the actions listed are not "stand alone" efforts taken in isolation from other actions to address high-risk issues. That is, actions taken under one criterion may be important to meeting other criteria as well. For example, top leadership can demonstrate its commitment by establishing a corrective action plan including long-term priorities and goals to address the high-risk issue and using data to gauge progress—actions which are also vital to monitoring criteria.

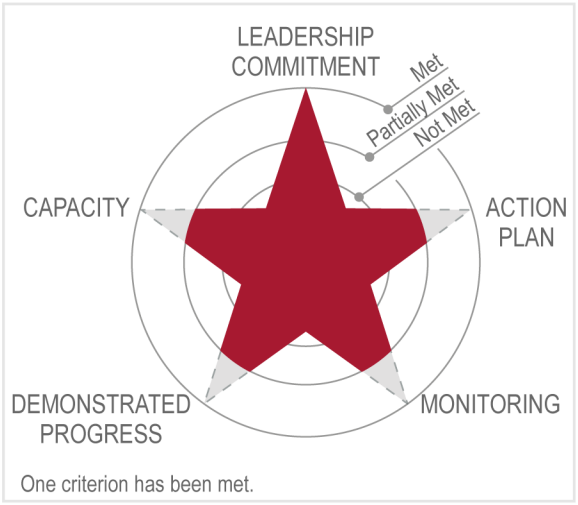
Figure 2: Criteria for Removal from the High-Risk List and Examples of Actions Leading to Progress



Source: GAO-16-480R. | GAO-18-622

As we reported in the February 2017 high-risk report,[21] the federal government's efforts to address information security deficiencies had fully met one of the five criteria for removal from the High-Risk List—leadership commitment—and partially met the other four, as shown in figure 3. We plan to update our assessment of this high-risk area against the five criteria in February 2019.

Figure 3: Status of High-Risk Area for Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information, as of February 2017



Source: GAO analysis. | GAO-18-622

Note: Each point of the star represents one of the five criteria for removal from the High-Risk List and each ring represents one of the three designations: not met, partially met, or met. An unshaded point at the innermost ring means that the criterion has not been met, a partially shaded point at the middle ring means that the criterion has been partially met, and a fully shaded point at the outermost ring means that the criterion has been met.

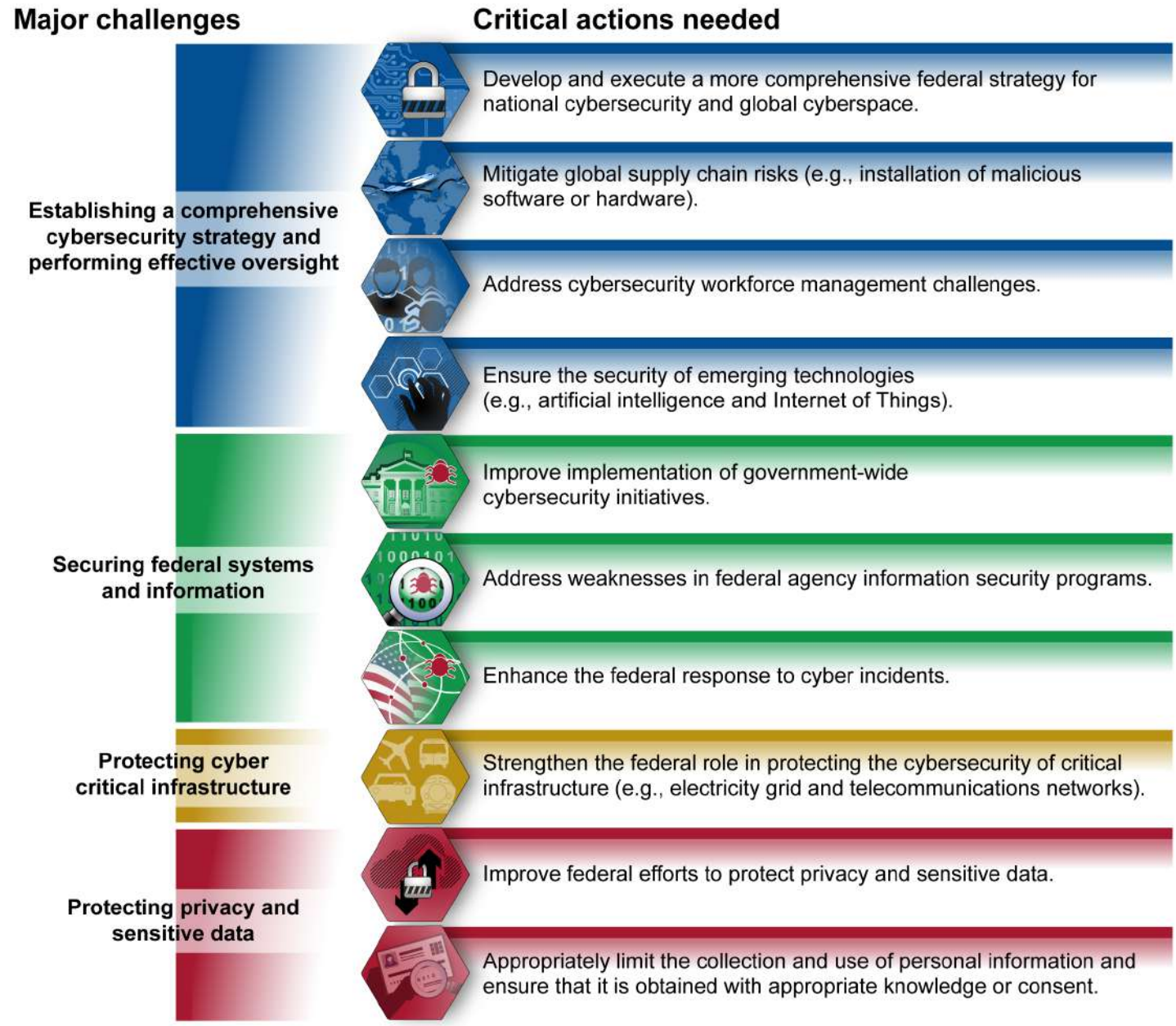
Ten Critical Actions Needed to Address Major Cybersecurity Challenges

Based on our prior work, we have identified four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address these challenges, we have identified 10 critical actions that the federal government and other entities need to take (see figure 4). The four challenges and the 10 actions

[21]GAO-17-317.

needed to address them are summarized following the table. In addition, we also discuss in more detail each of the 10 actions in appendices II through XI.

Figure 4: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Source: GAO analysis. | GAO-18-622

Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government has been challenged in establishing a comprehensive cybersecurity strategy and in performing effective oversight as called for by federal law and policy.[22] Specifically, we have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.[23] We have also reported on challenges in performing oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies. The federal government can take four key actions to improve the nation's strategic approach to, and oversight of, cybersecurity.

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.** In February 2013 we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[24]

  In October 2015, in response to our recommendation to develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy,[25] the Director of OMB and the Federal Chief Information Officer issued a *Cybersecurity Strategy and Implementation Plan for the Federal*

[22]This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget's Circular No. A-130, "*Managing Information as a Strategic Resource*" and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

[23]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).

[24]GAO-13-187.

[25]In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004)).

Civilian Government.[26] The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy's milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. For example, a May 2017 presidential executive order required federal agencies to take a variety of actions, including better manage their cybersecurity risks and coordinate to meet reporting requirements related to cybersecurity of federal networks, critical infrastructure, and the nation.[27] Additionally, the December 2017 National Security Strategy[28] cites cybersecurity as a national priority and identifies related needed actions, such as including identifying and prioritizing risk, and building defensible government networks.

Further, DHS issued a cybersecurity strategy in May 2018,[29] which articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. The strategy is intended to provide DHS with a framework to execute its cybersecurity responsibilities during the next 5 years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

[26]OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

[27]Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, *Executive Order 13800* (Washington, D.C.: May 11, 2017).

[28]The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: December 2017).

[29]DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018).

These efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we have previously recommended. The recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically, the documents generally did not include milestones and performance measures to gauge results, nor did they describe the resources needed to carry out the goals and objective. Further, most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, such as DHS, the Department of Defense (DOD), and OMB, who contribute substantially to the nation's cybersecurity programs.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses. For more information on this action area, see appendix II.

- **Mitigate global supply chain risks.** The global, geographically disperse nature of the producers and suppliers of IT products is a growing concern. We have previously reported on potential issues associated with IT supply chain and risks originating from foreign-manufactured equipment. For example, in July 2017, we reported that the Department of State had relied on certain device manufacturers, software developers, and contractor support which had suppliers that were reported to be headquartered in a cyber-threat nation (e.g., China and Russia).[30] We further pointed out that the reliance on complex, global IT supply chains introduces multiple risks to federal agencies, including insertion of counterfeits, tampering, or installation of malicious software or hardware.

  In July 2018, we testified that if such global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[31] Thus, the potential exists

[30]GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO-17-688R (Washington, D.C.: July 27, 2017).

[31]GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies,* GAO-18-667T (Washington, D.C.: July 12, 2018).

for serious adverse impact on an agency's operations, assets, and employees. These factors highlight the importance and urgency of federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agency-wide information security programs. For more information on this action area, see appendix III.

- **Address cybersecurity workforce management challenges.** The federal government faces challenges in ensuring that the nation's cybersecurity workforce has the appropriate skills. For example, in June 2018, we reported on federal efforts to implement the requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015*.[32] We determined that most of the Chief Financial Officers (CFO) Act[33] agencies had not fully implemented all statutory requirements, such as developing procedures for assigning codes to cybersecurity positions. Further, we have previously reported that DHS and DOD had not addressed cybersecurity workforce management requirements set forth in federal laws.[34] In addition, we have reported in the last 2 years that federal agencies (1) had not identified and closed cybersecurity skills gaps,[35] (2) had been

[32]GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466 (Washington, D.C.: June 14, 2018). The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (Dec. 18, 2015).

[33]There are 24 agencies identified in the Chief Financial Officers Act: the 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; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[34]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); and *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements,* GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

[35]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

challenged with recruiting and retaining qualified staff,[36] and (3) had difficulty navigating the federal hiring process.[37]

A recent executive branch report also discussed challenges associated with the cybersecurity workforce. Specifically, in response to Executive Order 13800, the Department of Commerce and DHS led an interagency working group exploring how to support the growth and sustainment of future cybersecurity employees in the public and private sectors. In May 2018, the departments issued a report[38] that identified key findings, including:

- the U.S. cybersecurity workforce needs immediate and sustained improvements;
- the pool of cybersecurity candidates needs to be expanded through retraining and by increasing the participation of women, minorities, and veterans;
- a shortage exists of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors; and
- comprehensive and reliable data about cybersecurity workforce position needs and education and training programs are lacking.

The report also included recommendations and proposed actions to address the findings, including that private and public sectors should (1) align education and training with employers' cybersecurity workforce needs by applying the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework; (2) develop cybersecurity career model paths; and (3) establish a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives.

In addition, in June 2018, the executive branch issued a government reform plan and reorganization recommendations that included,

[36]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).

[37]GAO, *Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities,* GAO-16-521 (Washington, D.C.: Aug. 2, 2016).

[38]The Secretaries of Commerce and Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, (Washington, D.C.: May 2018).

among other things, proposals for solving the federal cybersecurity workforce shortage.[39] In particular, the plan notes that the administration intends to prioritize and accelerate ongoing efforts to reform the way that the federal government recruits, evaluates, selects, pays, and places cyber talent across the enterprise. The plan further states that, by the end of the first quarter of fiscal year 2019, all CFO Act agencies, in coordination with DHS and OMB, are to develop a critical list of vacancies across their organizations. Subsequently, OMB and DHS are to analyze these lists and work with OPM to develop a government-wide approach to identifying or recruiting new employees or reskilling existing employees. Regarding cybersecurity training, the plan notes that OMB is to consult with DHS to standardize training for cybersecurity employees, and should work to develop an enterprise-wide training process for government cybersecurity employees. For more information on this action area, see appendix IV.

- **Ensure the security of emerging technologies.** As the devices used in daily life become increasingly integrated with technology, the risk to sensitive data and PII also grows. Over the last several years, we have reported on weaknesses in addressing vulnerabilities associated with emerging technologies, including:
  - IoT devices, such as fitness trackers, cameras, and thermostats, that continuously collect and process information are potentially vulnerable to cyber-attacks;[40]
  - IoT devices, such as those acquired and used by DOD employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department;[41]
  - vehicles that are potentially susceptible to cyber-attack through technology, such as Bluetooth;[42]

[39]Executive Office of the President of the United States, *Delivering Government Solutions in the 21st Century: Reform Plan and Reorganization Recommendations* (Washington, D.C.: June 2018).

[40]GAO, *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[41]GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

- the unknown impact of artificial intelligence cybersecurity; and[43]
- advances in cryptocurrencies and blockchain technologies.[44]

Executive branch agencies have also highlighted the challenges associated with ensuring the security of emerging technologies. Specifically, in a May 2018 report issued in response to Executive Order 13800, the Department of Commerce and DHS issued a report on the opportunities and challenges in reducing the botnet threat.[45] The opportunities and challenges are centered on six principal themes, including the global nature of automated, distributed attacks; effective tools; and awareness and education. The report also provides recommended actions, including that federal agencies should increase their understanding of what software components have been incorporated into acquired products and establish a public campaign to support awareness of IoT security. For more information on this action area, see appendix V.

In our previously discussed reports related to this cybersecurity challenge, we made a total of 50 recommendations to federal agencies to address the weaknesses identified. As of August 2018, 48 recommendations had not been implemented. These outstanding recommendations include 8 priority recommendations, meaning that we believe that they warrant priority attention from heads of key departments and agencies. These priority recommendations include addressing weaknesses associated with, among other things, agency-specific cybersecurity workforce challenges and agency responsibilities for supporting mitigation of vehicle network attacks. Until our recommendations are fully implemented, federal agencies may be limited in their ability to provide effective oversight of critical government-wide

[42]GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Apr. 25, 2016).

[43]GAO, *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).

[44]GAO, *GAO Strategic Plan 2018-2023: Trends Affecting Government and Society*, GAO-18-396SP (Washington, D.C.: Feb. 22, 2018).

[45]The Secretaries of Commerce and Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, (Washington, D.C.: May 22, 2018).

initiatives, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies.

In addition to our prior work related to the federal government's efforts to establish key strategy documents and implement effective oversight, we also have several ongoing reviews related to this challenge. These include reviews of:

- the CFO Act agencies' efforts to submit complete and reliable baseline assessment reports of their cybersecurity workforces;
- the extent to which DOD has established training standards for cyber mission force personnel, and efforts the department has made to achieve its goal of a trained cyber mission force; and
- selected agencies' ability to implement cloud service technologies and notable benefits this might have on agencies.

Securing Federal Systems and Information

The federal government has been challenged in securing federal systems and information. Specifically, we have reported that federal agencies have experienced challenges in implementing government-wide cybersecurity initiatives, addressing weaknesses in their information systems and responding to cyber incidents on their systems. This is particularly concerning given that the emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. As such, it is important that federal agencies take appropriate steps to better ensure they have effectively implemented programs to protect their information and systems. We have identified three actions that the agencies can take.

- **Improve implementation of government-wide cybersecurity initiatives.** Specifically, in January 2016, we reported that DHS had not ensured that the National Cybersecurity Protection System (NCPS) had fully satisfied all intended system objectives related to intrusion detection and prevention, information sharing, and analytics.[46] In addition, in February 2017, we reported[47] that the DHS

[46]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). NCPS 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.

National Cybersecurity and Communications Integration Center's (NCCIC)[48] functions were not being performed in adherence with the principles set forth in federal laws.[49] We noted that, although NCCIC was sharing information about cyber threats in the way it should, the center did not have metrics to measure that the information was timely, relevant and actionable, as prescribed by law. For more information on this action area, see appendix VI.

- **Address weaknesses in federal information security programs.** We have previously identified a number of weaknesses in agencies' protection of their information and information systems. For example, over the past 2 years, we have reported that:
  - most of the 24 agencies covered by the CFO Act had weaknesses in each of the five major categories of information system controls (i.e., access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management);[50]
  - three agencies—the Securities Exchange Commission, the Federal Deposit Insurance Corporation, and the Food and Drug Administration—had not effectively implemented aspects of their

[47]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).

[48]DHS established the NCCIC as to serve as the 24/7 cyber monitoring, incident response, and management center. The center provides a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats.

[49]*The National Cybersecurity Protection Act of 2014* and *Cybersecurity Act of 2015* require NCCIC to carry out 11 cybersecurity functions, to the extent practicable, in accordance with nine principles. Pub. L. No. 113-282, Dec. 18, 2014. The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

[50]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).

information security programs, which resulted in weaknesses in these agencies' security controls;[51]

- information security weaknesses in selected high-impact systems at four agencies—the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, OPM, and the Department of Veterans Affairs—were cited as a key reason that the agencies had not effectively implemented elements of their information security programs;[52]
- DOD's process for monitoring the implementation of cybersecurity guidance had weaknesses and resulted in the closure of certain tasks (such as completing cyber risk assessments) before they were fully implemented;[53] and
- agencies had not fully defined the role of their Chief Information Security Officers, as required by FISMA.[54]

We also recently testified that, although the government had acted to protect federal information systems, additional work was needed to improve agency security programs and cyber capabilities.[55] In particular, we noted that further efforts were needed by agencies to implement our prior recommendations in order to strengthen their information security programs and technical controls over their computer networks and systems. For more information on this action area, see appendix VII.

[51]GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions,* GAO-17-469 (Washington, D.C.: July 27, 2017); *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information,* GAO-17-436 (Washington, D.C.: May 31, 2017); and *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk,* GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

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

[53]GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened,* GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

[54]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).

[55]GAO, *Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity*, GAO-18-566T (Washington, D.C.: May 23, 2018).

- **Enhance the federal response to cyber incidents.** We have reported that certain agencies have had weaknesses in responding to cyber incidents. For example,
  - as of August 2017, OPM had not fully implemented controls to address deficiencies identified as a result of its 2015 cyber incidents;[56]
  - DOD had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises;[57]
  - as of April 2016, DOD had not identified, clarified, or implemented all components of its support of civil authorities during cyber incidents;[58] and
  - as of January 2016, DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.

  For more information on this action area, see appendix VIII.

In the public versions of the reports previously discussed for this challenge area, we made a total of 101 recommendations to federal agencies to address the weaknesses identified.[59] As of August 2018, 61 recommendations had not been implemented. These outstanding recommendations include 14 priority recommendations to address weaknesses associated with, among other things, the information security programs at the National Aeronautics and Space Administration, OPM, and the Security Exchange Commission. Until these recommendations are implemented, these federal agencies will be limited in their ability to

[56]GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed,* GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[57]GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises,* GAO-16-574 (Washington, D.C.: Sept. 6, 2016).

[58]GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents,* GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

[59]GAO often issues two versions of its audit reports on the security of federal systems and information. One version is publicly available, and one version is not available to the public because of the sensitive security information it contains. GAO has made hundreds of recommendations to agencies to rectify technical security control deficiencies identified in these non-publicly available reports.

ensure the effectiveness of their programs for protecting information and systems.

In addition to our prior work, we also have several ongoing reviews related to the federal government's efforts to protect its information and systems. These include reviews of:

- Federal Risk and Authorization Management Program (FedRAMP)[60] implementation, including an assessment of the implementation of the program's authorization process for protecting federal data in cloud environments;
- the Equifax data breach, including an assessment of federal oversight of credit reporting agencies' collection, use, and protection of consumer PII;
- the Federal Communication Commission's Electronic Comment Filing System security, to include a review of the agency's detection of and response to a May 2017 incident that reportedly impacted the system;
- DOD's efforts to improve the cybersecurity of its major weapon systems;
- DOD's whistleblower program, including an assessment of the policies, procedures, and controls related to the access and storage of sensitive and classified information needed for the program;
- IRS's efforts to (1) implement security controls and the agency's information security program, (2) authenticate taxpayers, and (3) secure tax information; and
- the federal approach and strategy to securing agency information systems, to include federal intrusion detection and prevention capabilities and the intrusion assessment plan.

Protecting Cyber Critical Infrastructure

The federal government has been challenged in working with the private sector to protect critical infrastructure. This infrastructure includes both public and private systems vital to national security and other efforts, such as providing the essential services that underpin American society. As the cybersecurity threat to these systems continues to grow, federal agencies have millions of sensitive records that must be protected. Specifically, this

[60]In December 2011, OMB established FEDRAMP—a government-wide program intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services.

critical infrastructure threat could have national security implications and more efforts should be made to ensure that it is not breached.

To help address this issue, the National Institute of Standards and Technology (NIST) developed the cybersecurity framework—a voluntary set of cybersecurity standards and procedures for industry to adopt as a means of taking a risk-based approach to managing cybersecurity.[61]

However, additional action is needed to strengthen the federal role in protecting the critical infrastructure. Specifically, we have reported on other critical infrastructure protection issues that need to be addressed. For example:

- DHS did not track vulnerability reduction from the implementation and verification of planned security measures at the high-risk chemical facilities that engage with the department, as a basis for assessing performance.[62]
- Entities within the 16 critical infrastructure sectors reported encountering four challenges to adopting the cybersecurity framework, such as being limited in their ability to commit necessary resources towards framework adoption and not having the necessary knowledge and skills to effectively implement the framework.[63]
- DOD and the Federal Aviation Administration identified a variety of operations and physical security risks that could adversely affect DOD missions.[64]
- Major challenges existed to securing the electricity grid against cyber threats.[65] These challenges included monitoring implementation of

[61]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The cybersecurity framework was updated on April 16, 2018.

[62]GAO, *Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders*, GAO-18-538 (Washington, D.C.: Aug. 8, 2018).

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

[64]GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[65]GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

cybersecurity standards, ensuring security features are built into smart grid systems, and establishing metrics for cybersecurity.

- DHS and other agencies needed to enhance cybersecurity in the maritime environment. Specifically, DHS did not include cyber risks in its risk assessments that were already in place nor did it address cyber risks in guidance for port security plans.[66]
- Sector-specific agencies[67] were not properly addressing progress or metrics to measure their progress in cybersecurity.[68]

For more information on this action area, see appendix IX.

We made a total of 21 recommendations to federal agencies to address these weaknesses and others. These recommendations include, for example, a total of 9 recommendations to 9 sector-specific agencies to develop methods to determine the level and type of cybersecurity framework adoption across their respective sectors.[69] As of August 2018, all 21 recommendations had not been implemented. Until these recommendations are implemented, the federal government will continue to be challenged in fulfilling its role in protecting the nation's critical infrastructure.

In addition to our prior work related to the federal government's efforts to protect critical infrastructure, we also have several ongoing reviews focusing on:

- the physical and cybersecurity risks to pipelines across the country responsible for transmitting oil, natural gas, and other hazardous liquids;
- the cybersecurity risks to the electric grid; and

[66]GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*, GAO-16-116T (Washington, D.C.: Oct. 8, 2015).

[67]Sector-specific agencies are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise. They accomplish this by leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the environment.

[68]GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015). The government facilities sector was excluded from the scope of this review due to its uniquely governmental focus.

[69]GAO-18-211.

- the privatization of utilities at DOD installations.

Protecting Privacy and Sensitive Data

The federal government has been challenged in protecting privacy and sensitive data. Advances in technology, including powerful search technology and data analytics software, have made it easy to correlate information about individuals across large and numerous databases, which have become very inexpensive to maintain. In addition, ubiquitous Internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices such as smartphones and fitness trackers.

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of PII maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

Federal agencies should take two types of actions to address this challenge area. In addition, we have previously proposed two matters for congressional consideration aimed toward better protecting PII.

- **Improve federal efforts to protect privacy and sensitive data.** We have issued several reports noting that agencies had deficiencies in protecting privacy and sensitive data that needed to be addressed. For example:
  - The Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS) and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.[70]

[70]GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, GAO-18-210 (Washington, D.C.: March 6, 2018).

- The Department of Education's Office of Federal Student Aid had not properly overseen its school partners' records or information security programs.[71]
- HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.[72]
- CMS had not fully protected the privacy of users' data on state-based marketplaces.[73]
- Poor planning and ineffective monitoring had resulted in the unsuccessful implementation of government initiatives aimed at eliminating the unnecessary collection, use, and display of SSNs.[74]

For more information on this action area, see appendix X.

- **Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.** We have issued a series of reports that highlight a number of the key concerns in this area. For example:
  - The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent;[75]
  - Federal laws for smartphone tracking applications have not generally been well enforced;[76]
  - The FBI has not fully ensured privacy and accuracy related to the use of face recognition technology.[77]

[71]GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information,* GAO-18-121 (Washington, D.C.: Dec. 15, 2017).

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

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

[74]GAO, *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display,* GAO-17-553 (Washington, D.C.: July 25, 2017).

[75]GAO-17-75.

[76]GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking*, GAO-16-317 (Washington, D.C.: Apr. 21, 2016).

For more information on this action area, see appendix XI.

We have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974[78] and the E-Government Act of 2002,[79] because they may not consistently protect PII.[80] Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. However, revisions to the Privacy Act and the E-Government Act have not yet been enacted.

Further, we also suggested that Congress consider strengthening the consumer privacy framework[81] and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices.[82] However, these suggested changes have not yet been enacted.

We also made a total of 29 recommendations to federal agencies to address the weaknesses identified. As of August 2018, 28 recommendations had not been implemented. These outstanding recommendations include 6 priority recommendations to address weaknesses associated with, among other things, publishing privacy impact assessments[83] and improving the accuracy of the FBI's face recognition services. Until these recommendations are implemented,

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

[78]Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

[79]Pub. L. No. 107-347, 116 Stat. 2899.

[80]GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

[81]This framework presents a consumer privacy bill of rights, describes a stakeholder process to specify how the principles in that bill of rights would apply, and encourages Congress to provide the Federal Trade Commission with enforcement authorities for the bill of rights.

[82]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[83]Privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

federal agencies will be challenged in their ability to protect privacy and sensitive data and ensure that its collection and use is appropriately limited.

In addition to our prior work, we have several ongoing reviews related to protecting privacy and sensitive data. These include reviews of:

- IRS's taxpayer authentication efforts, including what steps the agency is taking to monitor and improve its authentication methods;
- the extent to which the Department of Education's Office of Federal Student Aid's policies and procedures for overseeing non-school partners' protection of federal student aid data align with federal requirements and guidance;
- data security issues related to credit reporting agencies, including a review of the causes and impacts of the August 2017 Equifax data breach;
- the extent to which Equifax assessed, responded to, and recovered from its August 2017 data breach;
- federal agencies' efforts to remove PII from shared cyber threat indicators; and
- how the federal government has overseen Internet privacy, including the roles of the Federal Communications Commission and the Federal Trade Commission, and strengths and weaknesses of the current oversight authorities.

Continued Implementation of Our Recommendations Is Needed to Address Cybersecurity Weaknesses

In conclusion, since 2010, we have made over 3,000 recommendations to agencies aimed at addressing the four cybersecurity challenges. 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. Of the roughly 3,000 recommendations made since 2010, nearly 1,000 had not been implemented as of August 2018. We have also designated 35 as priority recommendations, and as of August 2018, 31 had not been implemented.

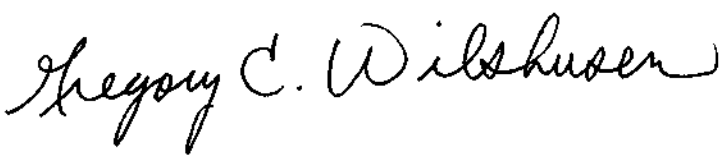
The federal government and the nation's critical infrastructure are dependent on IT systems and electronic data, which make them highly vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's security, prosperity, and well-being. Nevertheless, the security over these systems and data is inconsistent and urgent actions are needed to address ongoing

cybersecurity and privacy challenges. Specifically, the federal government needs to implement a more comprehensive cybersecurity strategy and improve its oversight, including maintaining a qualified cybersecurity workforce; address security weaknesses in federal systems and information and enhance cyber incident response efforts; bolster the protection of cyber critical infrastructure; and prioritize efforts to protect individual's privacy and PII. Until our recommendations are addressed and actions are taken to address the four challenges we identified, the federal government, the national critical infrastructure, and the personal information of U.S. citizens will be increasingly susceptible to the multitude of cyber-related threats that exist.

We are sending copies of this report to the appropriate congressional committees. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or 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 report. GAO staff who made key contributions to this report are listed in appendix XII.

Nick Marinos
Director, Cybersecurity and Data Protection Issues



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Related GAO Reports

Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders. GAO-18-538. Washington, D.C.: August 8, 2018.

High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation. GAO-18-645T. Washington, D.C.: July 25, 2018.

Information Security: Supply Chain Risks Affecting Federal Agencies. GAO-18-667T. Washington, D.C.: July 12, 2018.

Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity. GAO-18-566T. Washington, D.C.: May 23, 2018.

Cybersecurity: DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks, GAO-18-520T. Washington, D.C.: April 24, 2018.

Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement. GAO-18-210. Washington, D.C.: March 6, 2018.

Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications. GAO-18-142SP. Washington, D.C.: March 28, 2018.

GAO Strategic Plan 2018-2023: Trends Affecting Government and Society. GAO-18-396SP. Washington, D.C.: February 22, 2018.

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

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

Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. GAO-18-177. Washington, D.C.: January 18, 2018.

Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information. GAO-18-121. Washington, D.C.: December 15, 2017.

Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements. GAO-18-47. Washington, D.C.: November 30, 2017.

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

Information Security: OPM Has Improved Controls, but Further Efforts Are Needed. GAO-17-614. Washington, D.C.: August 3, 2017.

Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened. GAO-17-512. Washington, D.C.: August 1, 2017.

State Department Telecommunications: Information on Vendors and Cyber-Threat Nations. GAO-17-688R. Washington, D.C.: July 27, 2017.

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD. GAO-17-668. Washington, D.C.: July 27, 2017.

Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions. GAO-17-469. Washington, D.C.: July 27, 2017.

Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data. GAO-17-395. Washington, D.C.: July 26, 2017.

Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display. GAO-17-553. Washington, D.C.: July 25, 2017.

Information Security: FDIC Needs to Improve Controls over Financial Systems and Information. GAO-17-436. Washington, D.C.: May 31, 2017.

Technology Assessment: Internet of Things: Status and implications of an increasingly connected world. GAO-17-75. Washington, D.C.: May 15, 2017.

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

High-Risk Series: An Update. GAO-17-317. Washington, D.C.: February 2017.

IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps. GAO-17-8. Washington, D.C.: November 30, 2016.

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

Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises. GAO-16-574. Washington, D.C.: September 6, 2016.

Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk. GAO-16-513. Washington, D.C.: August 30, 2016.

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

Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities. GAO-16-521. Washington, D.C.: August 2, 2016.

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

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

Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking. GAO-16-317. Washington, D.C.: May 9, 2016.

Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. GAO-16-350. Washington, D.C.: April 25, 2016.

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. GAO-16-332. Washington, D.C.: April 4, 2016.

Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls. GAO-16-265. Washington, D.C.: March 23, 2016.

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.: January 28, 2016.

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

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention. GAO-16-174T. Washington, D.C.: October 21, 2015.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity. GAO-16-116T. Washington, D.C.: October 8, 2015.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2014.

Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace. GAO-13-663. Washington, D.C.: September 25, 2013.

Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. GAO-08-536. Washington, D.C.: May 19, 2008.

Appendix II: Action 1—Develop and Execute a More Comprehensive Federal Strategy for National Cybersecurity and Global Cyberspace

Federal law and policy call for a risk-based approach to managing cybersecurity within the government, as well as globally.[1] We have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.

More specifically, in February 2013, we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[2] Accordingly, we recommended that the White House Cybersecurity Coordinator[3] in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy[4] including, among other things, milestones and performance measures for major activities to address stated priorities; cost and resources needed to accomplish stated priorities; and specific roles and responsibilities of federal organizations related to the strategy's stated priorities.

In response to our recommendation, in October 2015, the Director of OMB and the Federal Chief Information Officer, issued a *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*.[5]

[1]This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget's Circular No. A-130, "*Managing Information as a Strategic Resource*" and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

[2]GAO-13-187.

[3]In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Cyberspace Policy Review, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation's digital infrastructure.

[4]In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004)).

[5]OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy's milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. Table 1 identifies these recent efforts and a description of their related contents.

Table 1: Recent Executive Branch Initiatives That Identify Cybersecurity Priorities for the Federal Government

Executive branch initiative	Date of issuance	Description
Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	May 2017	The Presidential executive order required federal agencies to take a variety of actions, including better manage their cybersecurity risks and coordinate to meet reporting requirements related to cybersecurity of federal networks, critical infrastructure, and the nation.[a] As of August 2018, the executive branch had publicly released several reports, including a high-level assessment by the Office of Management and Budget (OMB) of the cybersecurity risk management capabilities of the federal government.[b] The assessment stated that OMB and the Department of Homeland Security (DHS) examined the capabilities of 96 civilian agencies across 76 cybersecurity metrics and found that 71 agencies had cybersecurity programs that were either at risk or high risk.[c] The report also stated agencies were not equipped to determine how malicious actors seek to gain access to their information systems and data. The report identified core actions to address cybersecurity risks across the federal enterprise.
National Security Strategy	December 2017	The National Security Strategy[d] identified four vital national interests: protecting the homeland, the American people, and American way of life; promoting American prosperity; preserving peace through strength; and advance American influence. The strategy also cites cybersecurity as a national priority and identifies related needed actions, including identifying and prioritizing risk, building defensible government networks, determining and disrupting malicious cyber actors, improving information sharing and deploying layered defenses.
DHS Cybersecurity Strategy	May 2018	The DHS cybersecurity strategy[e] articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. The goals were spread across five pillars that correspond to DHS-wide risk management, including risk identification, vulnerability reduction, threat reduction, consequence mitigation, and enabling cybersecurity outcomes. The strategy is intended to provide DHS with a framework to execute its cybersecurity responsibilities during the next 5 years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

Source: GAO analysis of agency documents. | GAO-18-622

[a]Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order 13800 (Washington, D.C.: May 11, 2017).

[b]OMB, *Federal Cybersecurity Risk Determination Report and Action Plan*, (Washington, D.C.: May 2018).

[c]OMB and DHS designated agencies as "at risk" if agencies had some essential policies, processes, and tools in place to mitigate overall cybersecurity risks. OMB and DHS designated agencies as "high risk" if agencies did not have essential policies, processes, and tools in place to mitigate overall cybersecurity risks.

[d]The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: Dec. 2017).

[e]DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018).

These efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we recommended. The recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically:

- Milestones and performance measures to gauge results were generally not included in strategy documents. For example, although the DHS Cybersecurity Strategy stated that its implementation would be assessed on an annual basis, it did not describe the milestones and performance measures for tracking the effectiveness of the activities intended to meet the stated goals (e.g., protecting critical infrastructure and responding effectively to cyber incidents). Without such performance measures, DHS will lack a means to ensure that the goals and objectives discussed in the document are accomplished and that responsible parties are held accountable.

  According to officials from DHS's Office of Cybersecurity and Communications, the department is developing a plan for implementing the DHS Cybersecurity Strategy and expects to issue the plan by the end of calendar year 2018. The officials stated that the plan is expected to identify milestones, roles, and responsibilities across DHS to inform the prioritization of future efforts.

- The strategy documents generally did not include information regarding the resources needed to carry out the goals and objectives. For example, although the DHS Cybersecurity Strategy identified a variety of actions the agency planned to take to perform their cybersecurity mission, it did not articulate the resources needed to carry out these actions and requirements. Without information on the specific resources needed, federal agencies may not be positioned to allocate such resources and investments and, therefore, may be hindered in their ability meet national priorities.

- Most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, such as DHS, DOD, and OMB. These agencies contribute substantially to the nation's cybersecurity programs. For example, although the National Security Strategy discusses multiple priority actions needed to address the nation's cybersecurity challenges (e.g., building defensible government networks, and deterring and disrupting malicious cyber actors), it does not describe the roles, responsibilities, or the expected coordination of any specific federal agencies, including DHS, DOD, or OMB, or other non-federal entities needed to carry out those actions. Without this information, the federal government may not be able foster effective coordination, particularly where there is overlap in responsibilities, or hold agencies accountable for carrying out planned activities.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

Appendix III: Action 2—Mitigate Global Supply Chain Risks

The exploitation of information technology (IT) products and services through the supply chain is an emerging threat. IT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's IT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

Federal regulation and guidance issued by the National Institute of Standards and Technology (NIST) set requirements and best practices for mitigating supply chain risks. The Federal Acquisition Regulation established codification and publication of uniform policies and procedures for acquisition by all executive branch agencies. Agencies are required by the Federal Acquisition Regulation to ensure that contracts include quality requirements that are determined necessary to protect the government's interest. In addition, the NIST guidance on supply chain risk management practices for federal information systems and organizations intends to assist federal agencies with identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations.

We have previously reported on risks to the IT supply chain and risks originating from foreign-manufactured equipment. For example:

- In July 2018, we testified that if global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[1] Thus, the potential exists for serious adverse impact on an agency's operations, assets, and employees. We further stated that in 2012 we determined that four national security-related agencies—the Departments of Defense, Justice, Energy, Homeland Security (DHS)—varied in the extent to which they had addressed supply chain risks.[2] We recommended that three agencies take eight actions, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. The agencies generally concurred with

[1]GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies,* GAO-18-667T (Washington, D.C.: July 12, 2018).

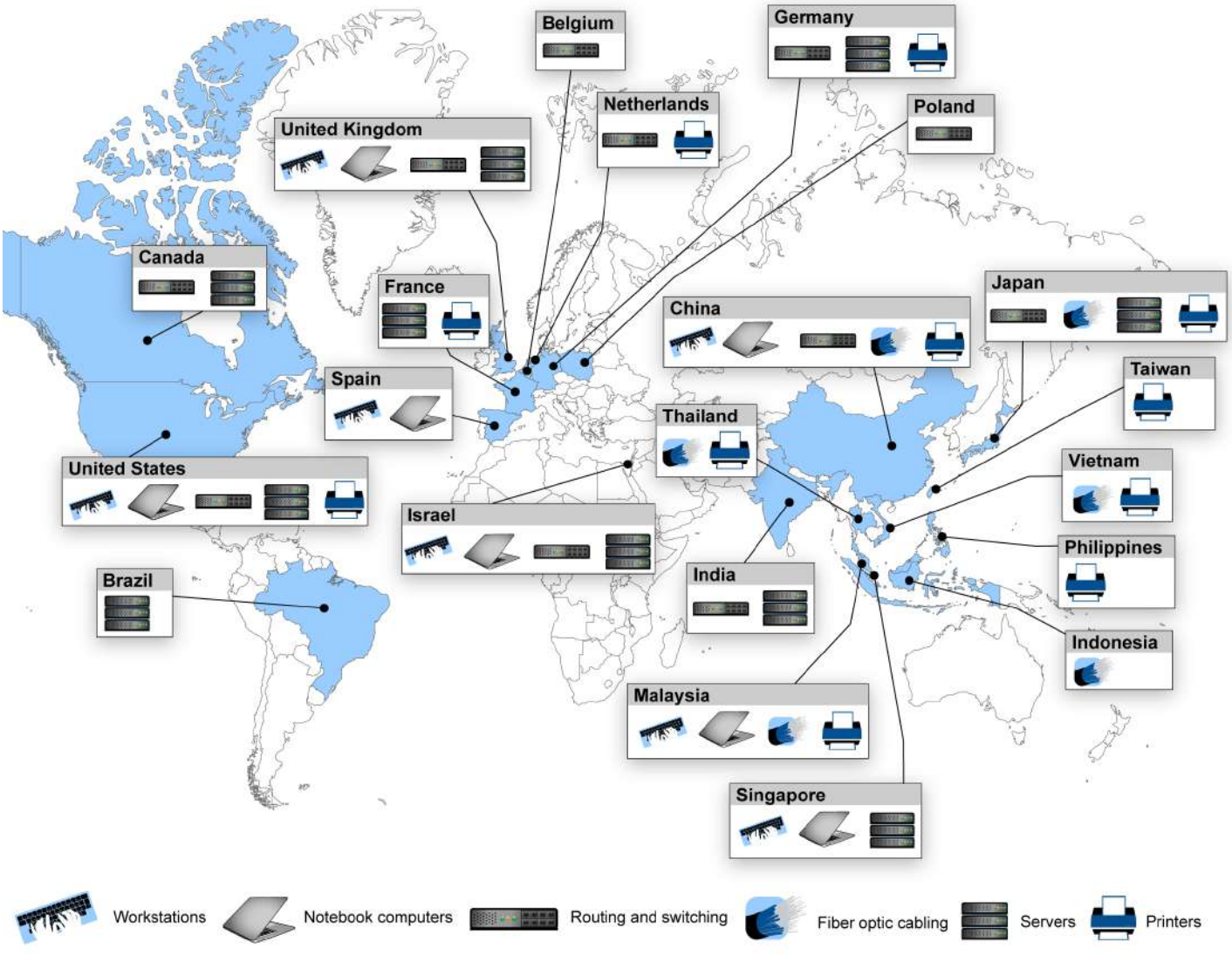
[2]GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

the recommendations and subsequently implemented seven recommendations and partially implemented the eighth recommendation.

- In July 2017, we reported that, based on a review of a sample of organizations within the Department of State's telecommunications supply chain, we were able to identify instances in which device manufacturers, software developers and contractor support were reported to be headquartered in a leading cyber-threat nation.[3] For example, of the 52 telecommunications device manufacturers and software developers in our sample, we were able to identify 12 that had 1 or more suppliers that were reported to be headquartered in a leading cyber-threat nation. We noted that the reliance on complex, global IT supply chains introduces multiple risks to federal agencies, including insertion of counterfeits, tampering, or installation of malicious software or hardware. Figure 5 illustrates possible manufacturing locations of typical network components.

[3]GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO-17-688R (Washington, D.C.: July 27, 2017).

Figure 5: Possible Manufacturing Locations of Typical Network Components



Source: GAO analysis of public information. | GAO-18-622

Although federal agencies have taken steps to address IT supply chain deficiencies that we previously identified, this area continues to be a potential threat vector for malicious actors to target the federal government. For example, in September 2017, DHS issued a binding operating directive which calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems and to develop detailed plans to remove and discontinue present and

future use of the products. DHS expressed concern about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks.

Appendix IV: Action 3—Address Cybersecurity Workforce Management Challenges

On May 11, 2017, the President issued an executive order on strengthening the cybersecurity of federal networks and critical infrastructure.[1] The order makes it the policy of the United States to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace. It directed the Secretaries of Commerce and Homeland Security (DHS), in consultation with other federal agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.

Nevertheless, the federal government continues to face challenges in addressing the nation's cybersecurity workforce.

- **Agencies had not effectively conducted baseline assessments of their cybersecurity workforce or fully developed procedures for coding positions.** In June 2018, we reported[2] that 21 of the 24 agencies covered by the Chief Financial Officer's Act[3] had conducted and submitted to Congress a baseline assessment identifying the extent to which their cybersecurity employees held professional certifications, as required by the *Federal Cybersecurity Workforce Assessment Act of 2015*.[4] However, we found that the results of these assessments may not have been reliable because agencies did not address all of the reportable information and agencies were limited in their ability to obtain complete and consistent information about their cybersecurity employees and the certifications they held. We

[1]*Presidential Executive Order on Strengthening the* Cybersecurity *of Federal Networks and Critical Infrastructure*. Executive Order 13800 (Washington, D.C.: May 11, 2017).

[2]GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions,* GAO-18-466 (Washington, D.C.: June 14, 2018)

[3]There are 24 agencies identified in the Chief Financial Officers Act: the 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; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[4]The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, sec. 303 (Dec. 18, 2015); 129 Stat. 2242, 2975-77.

determined that this was because agencies had not yet fully identified all members of their cybersecurity workforces or did not have a consistent list of appropriate certifications for cybersecurity positions.

Further, 23 of the agencies reviewed had established procedures for identifying and assigning the appropriate employment codes to their civilian cybersecurity positions, as called for by the act. However, 6 of the 23 did not address one or more of 7 activities required by OPM in their procedures, such as reviewing all filled and vacant positions and annotating reviewed position descriptions with the appropriate employment code. Accordingly, we made 30 recommendations to 13 agencies to fully implement two of the act's requirements on baseline assessments and coding procedures. The extent to which these agencies agreed with the recommendations varied.

- **DHS and the Department of Defense (DOD) had not addressed cybersecurity workforce management requirements set forth in federal laws.** In February 2018, we reported[5] that, while DHS had taken actions to identify, categorize, and assign employment codes to its cybersecurity positions,[6] as required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*,[7] its actions were not timely and complete. For example, DHS did not establish timely and complete procedures to identify, categorize, and code its cybersecurity position vacancies and responsibilities. Further, DHS had not yet completed its efforts to identify all of its cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. Table 2 shows DHS's progress in implementing the requirements of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017.

[5]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).

[6]These employment codes define work roles and tasks for cybersecurity specialty areas such as program management and system administration.

[7]*The Homeland Security Workforce Assessment Act of 2014*, enacted a part of the *Border Patrol Agent Pay Reform Act of 2014*, was passed by Congress in December 2014. This law requires DHS to identify all cybersecurity workforce positions within the department, determine the cybersecurity work category and specialty area of such positions, and assign the corresponding data element employment code to each cybersecurity position. After completing these activities, DHS was to identify its cybersecurity work categories and specialty areas of critical need within a year of identifying and assigning employment codes, and report these needs annually to OPM. Pub. L. No. 113-277, § 3,128 Stat. 2995, 3008-3010 (Dec. 18, 2014), 6 U.S.C. § 146.

Table 2: The Department of Homeland Security's Progress in Implementing Requirements of the Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017

Required activity		Due date	Completion date
1.	Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015	Apr. 2016
2.	Identify all positions with cybersecurity functions and determine work category and specialty areas of each position.	Sept. 2015	Ongoing
3.	Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing
4.	Identify and report critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
5.	Report critical needs annually to the Office of Personnel Management.	Sept. 2016	Not addressed

Source: GAO analysis of Department of Homeland Security documentation and the Homeland Security Cybersecurity Workforce Assessment Act of 2014. | GAO-18-622

Accordingly, 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 agreed with our six recommendations, but had not implemented them as of August 2018.

Regarding DOD, in November 2017, we reported[8] that instead of developing a comprehensive plan for U.S. Cyber Command, the department submitted a report consisting of a collection of documents that did not fully address the required six elements set forth in Section 1648 of the *National Defense Authorization Act for Fiscal Year 2016*.[9] More specifically, DOD's 1648 report did not address an element related to cyber incident training. In addition to not addressing the training element in the report, DOD had not ensured that staff were trained as required by the *Presidential Policy Directive on United*

[8]GAO, *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements,* GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

[9]Section 1648 of the *National Defense Authorization Act for Fiscal Year 2016* included a provision that DOD develop a comprehensive plan for U.S. Cyber Command to support civil authorities in responding to cyberattacks by foreign powers against the United States. Among the elements required in the plan is a description of internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments. Pub. L. No. 114-92, § 1648(a) (2015).

States Cyber Incident Coordination[10] or DOD's Significant Cyber Incident Coordination Procedures.

Accordingly, we made two recommendations to DOD to address these issues. DOD agreed with one of the recommendations and partially agreed with the other, citing ongoing activities related to cyber incident coordination training it believed were sufficient. However, we continued to believe the recommendation was warranted. As of August 2018, both recommendations had not yet been implemented.

- **Agencies had not identified and closed cybersecurity skills gaps.** In November 2016, we reported that five selected agencies[11] had made mixed progress in assessing their information technology (IT) skill gaps.[12] These agencies had started focusing on identifying cybersecurity staffing gaps, but more work remained in assessing competency gaps and in broadening the focus to include the entire IT community. Accordingly, we made a total of five recommendations to the agencies to address these issues. Four agencies agreed and one, DOD, partially agreed with our recommendations citing progress made in improving its IT workforce planning. However, we continued to believe our recommendation was warranted. As of August 2018, all five of the recommendations had not been implemented.
- **Agencies had been challenged with recruiting and retaining qualified staff.** In August 2016, we reported on the current authorities chief information security officers (CISO) at 24 agencies.[13] Among other things, CISOs identified key challenges they faced in fulfilling

[10]*Presidential Policy Directive – United States Cyber Incident Coordination/PPD-41* (July 26, 2016). PPD-41 requires federal agencies, including DOD, to update cyber incident coordination training to incorporate the tenets of PPD-41 by December 2016 and to identify and maintain a cadre of personnel qualified and trained in the National Incident Management System and unified coordination to manage and respond to a significant cyber incident.

[11]The five selected agencies reviewed were the Department of Commerce, the Department of Defense, the Department of Health and Human Services, the Department of Transportation, and the Department of the Treasury.

[12]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[13]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).

their responsibilities. Several of these challenges were related to the cybersecurity workforce, such as not having enough personnel to oversee the implementation of the number and scope of security requirements. In addition, CISOs stated that they were not able to offer salaries that were competitive with the private sector for candidates with high-demand technical skills. Furthermore, CISOs stated that certain security personnel lacked the skill sets needed or were not sufficiently trained. To assist CISOs in carrying out their responsibilities and better define their roles, we made a total of 34 recommendations to the Office of Management and Budget (OMB) and 13 agencies in our review. Agency responses to the recommendations varied; as of August 2018, 18 of the 34 recommendations had not been implemented.

- **Agencies have had difficulty navigating the federal hiring process.** In August 2016, we reported on the extent to which federal hiring authorities were meeting agency needs.[14] Although competitive hiring has been the traditional method of hiring, agencies can use additional hiring authorities to expedite the hiring process or achieve certain public policy goals. Among other things, we noted that agencies rely on a relatively small number of hiring authorities (as established by law, executive order, or regulation) to fill the vast majority of hires into the federal civil service.

  Further, while OPM collects a variety of data to assess the federal hiring process, neither it nor agencies used this information to assess the effectiveness of hiring authorities. Conducting such assessments would be a critical first step in making more strategic use of the available hiring authorities to more effectively meet their hiring needs. Accordingly, we made three recommendations to OPM to work with agencies to strengthen hiring efforts. OPM generally agreed with the recommendations; however, as of August 2018, two of them had not been implemented.

[14]GAO, *Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities,* GAO-16-521 (Washington, D.C.: Aug. 2, 2016).

Appendix V: Action 4—Ensure the Security of Emerging Technologies

The emergence of new technologies can potentially introduce security vulnerabilities for those technologies which were previous unknown. As we have previously reported, additional processes and controls will need to be developed to potentially address these new vulnerabilities. While some progress has been made to address the security and privacy issues associated with these technologies, such as the Internet of Things (IoT)[1] and vehicle networks, there is still much work to be done. For example:

- **IoT devices that continuously collect and process information are potentially vulnerable to cyber-attacks.** In May 2017, we reported that the IoT has become increasingly used to communicate and process vast amounts of information using “smart” devices (such as fitness trackers, cameras, and thermostats).[2] However, we noted that this emerging technology also presents new issues in areas such as information security, privacy, and safety. For example, IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. Table 3 provides examples of cyber-attacks that could affect IoT devices and networks.

[1]IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

[2]GAO, *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world*, GAO-17-75 (Washington, D.C.: May 15, 2017).

Table 3: Types of Attacks Possible with Internet of Things Devices

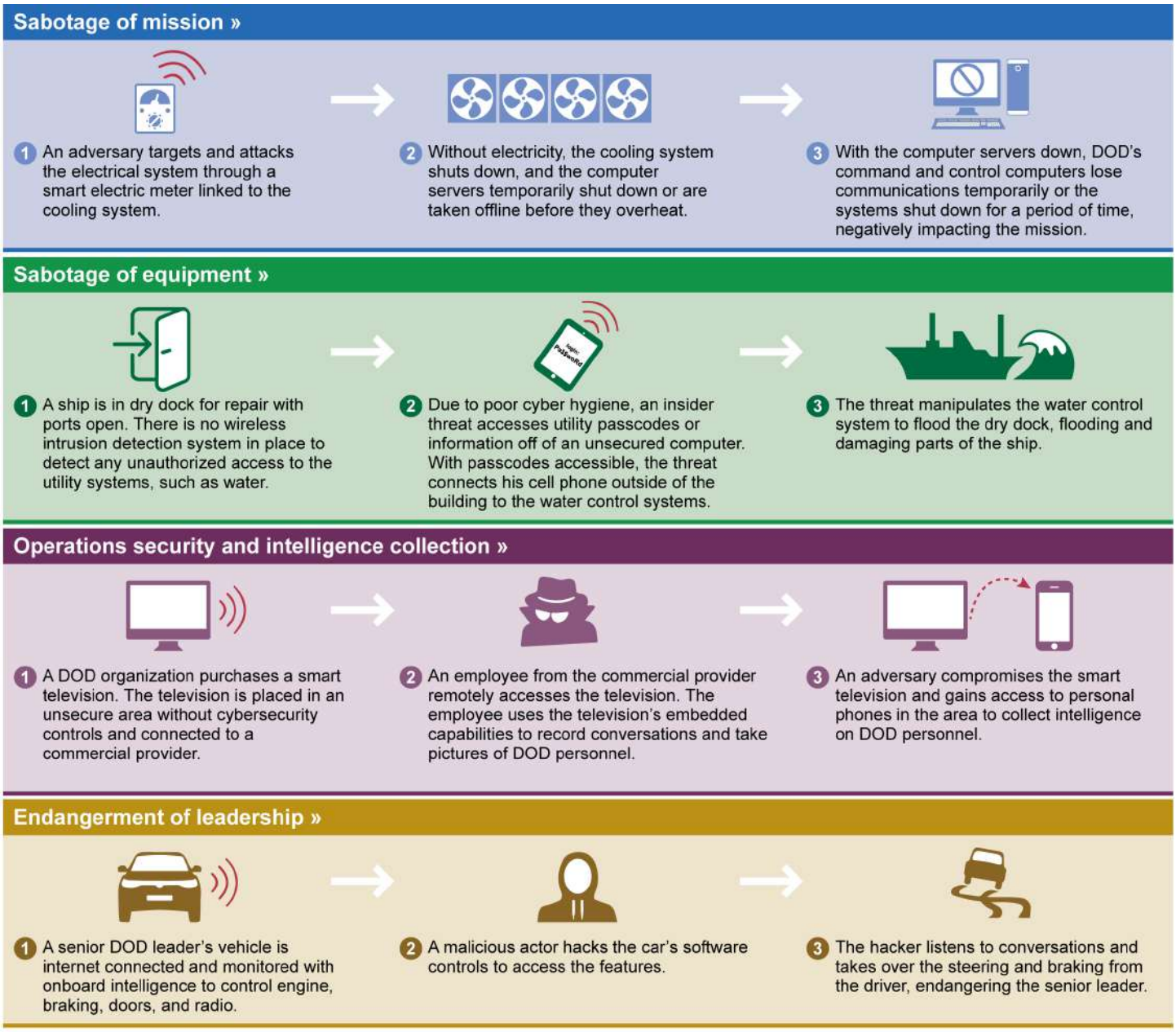
Type of attack	Description
Denial-of-Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples include logic bombs, Trojan horses, ransomware, viruses, and worms.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured query language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and Industry Reports. | GAO-18-622

- **IoT devices may increase the security risks to federal agencies.** In July 2017, we reported that IoT devices, such as those acquired and used by Department of Defense (DOD) employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department.[3] We noted that these risks can be divided into two categories, risks with the devices themselves, such as limited encryption, and risks with how they are used, such as unauthorized communication of information. The department has also identified notional threat scenarios, based on input from multiple DOD entities, which exemplify how these security risks could adversely impact DOD operations, equipment, or personnel. Figure 6 highlights a few examples of these scenarios.

[3]GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

Figure 6: Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)



Source: GAO analysis of Department of Defense (DOD) information. | GAO-18-622

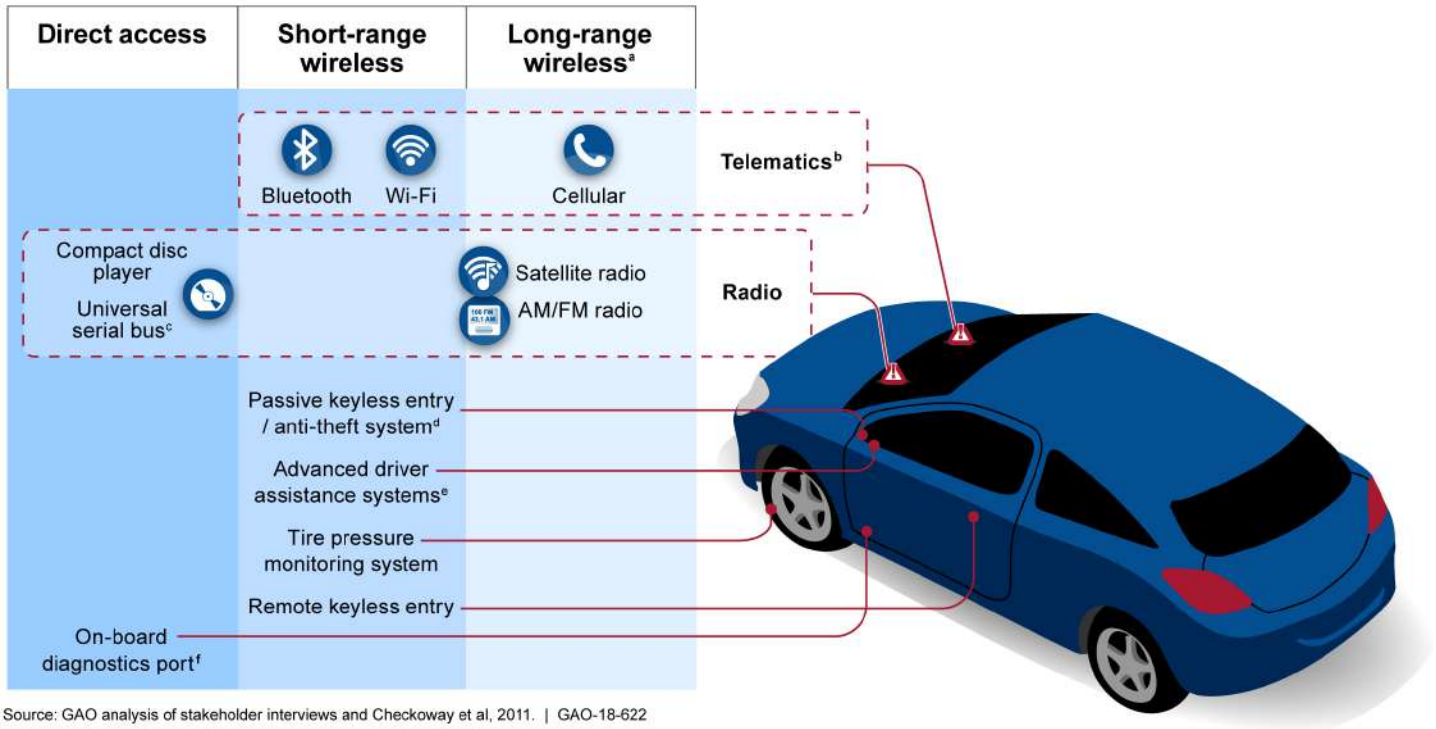
In addition, we reported that DOD had started to examine the security risks of IoT devices, but that the department had not conducted required assessments related to the security of its operations. Further,

DOD had issued policies and guidance for these devices, but these did not clearly address all of the risks relating to these devices. To address these issues, we made two recommendations to DOD. The department agreed with our recommendations; however, as of August 2018, they had not yet been implemented.

- **Vehicles are potentially susceptible to cyber-attack through networks, such as Bluetooth.** In March 2016, we reported that many stakeholders in the automotive industry acknowledge that in-vehicle networks pose a threat to the safety of the driver, as an external attacker could gain control to critical systems in the car.[4] Further, these industry stakeholders agreed that critical systems and other vehicle systems, such as a Bluetooth connection, should be separate in-vehicle networks so they could not communicate or interfere with one another. Figure 7 identifies the key interfaces that could be exploited in a vehicle cyber-attack.

[4]GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Apr. 25, 2016).

Figure 7: Key Interfaces That Could Be Exploited in a Vehicle Cyberattack



Source: GAO analysis of stakeholder interviews and Checkoway et al, 2011. | GAO-18-622

[a]In this context, long-range refers to access at distances over 1 kilometer.

[b]Universal serial bus storage devices are used to store text, video, audio, and image information. By inserting such devices into the vehicle's universal serial bus port, users can access stored information through the vehicle's radio or other media systems.

[c]These systems can prevent the car from operating unless the correct key is present, as verified by the presence of the correct radio-frequency identification tag.

[d]This port is mandated in vehicles by regulation for emission-testing purposes and to facilitate diagnostic assessments of vehicles, such as by repair shops.

[e]These systems use on-board sensors and other cameras to assist the driver in undertaking certain functions, such as changing lanes or braking suddenly.

[f]Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

To enhance the Department of Transportation's ability to effectively respond in the event of a real-world vehicle cyberattack, we made one recommendation to the department to better define its roles and responsibilities. The department agreed with the recommendation but, as of August 2018, had not yet taken action to implement it.

- **Artificial intelligence holds substantial promise for improving cybersecurity, but also posed new risks.** In March 2018, we reported on the results of a forum we convened to discuss emerging opportunities, challenges, and implications associated with artificial intelligence.[5] At the forum, participants from industry, government, academia, and nonprofit organizations discussed the potential implications of this emerging technology, including assisting with cybersecurity by helping to identify and patch vulnerabilities and defending against attacks; creating safer automated vehicles; improving the criminal justice system's allocation of resources; and improving how financial services govern investments.

  However, forum participants also highlighted a number of challenges and risks related to artificial intelligence. For example, if the data used by artificial intelligence are biased or become corrupted by hackers, the results could be biased or cause harm. Moreover, the collection and sharing of data needed to train artificial intelligence systems, a lack of access to computing resources, and adequate human capital were also challenges facing the development of artificial intelligence. Finally, forum participants noted that the widespread adoption raises questions about the adequacy of current laws and regulations.

- **Cryptocurrencies provide an alternative to traditional government-issued currencies, but have security implications.** In February 2018, we reported on trends affecting government and society, including the increased use of cryptocurrencies—digital representations of value that are not government-issued—that operate online and verify transactions using a public ledger called blockchain.[6] We highlighted the potential benefits of this technology, such as anonymity and lower transaction costs, as well as drawbacks, including making it harder to detect money laundering and other financial crimes. Because of these capabilities and others, we noted the potential for virtual currencies and blockchain technology to reshape financial services and affect the security of critical financial infrastructures. Lastly, we pointed out that the use of blockchain technology could have more security vulnerabilities as computing power increases as a result of new advancements in quantum computing, an area of quantum information science.

[5]GAO, *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).

[6]GAO, *Strategic Plan 2018-2023; Trends Affecting Government and Society*, GAO-18-396SP (Washington, D.C.: Feb 28, 2018).

Appendix VI: Action 5—Improve Implementation of Government-wide Cybersecurity Initiatives

In January 2008, the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. The directive established the Comprehensive National Cybersecurity Initiative, a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats against the federal government's networks. Under the initiative, the Department of Homeland Security (DHS) was to lead several projects to better secure civilian federal government networks. Specifically, the agency established the National Cybersecurity and Communications Integration Center (NCCIC), which functions as the 24/7 cyber monitoring, incident response, and management center. Figure 8 depicts the Watch Floor, which functions as a national focal point of cyber and communications incident integration.

Figure 8: The National Cybersecurity and Communications Integration Center Watch Floor

Source: Department of Homeland Security, National Cybersecurity and Communications Integration Center. | GAO-18-622

The United States Computer Emergency Readiness Team (US-CERT), one of several subcomponents of the NCCIC, is responsible for operating the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to entities across the federal government.

Although DHS is fulfilling its statutorily required mission by establishing the NCCIC and managing the operation of NCPS,[1] we have identified challenges in the agency's efforts to manage these programs:

- **DHS had not ensured that NCPS has fully satisfied all intended system objectives.** In January 2016, we reported that NCPS had a limited ability to detect intrusions across all types of network types.[2] In addition, we reported that the system's intrusion prevention capability was limited and its information-sharing capability was not fully developed. Furthermore, we reported that DHS's current metrics did not comprehensively measure the effectiveness of NCPS. Accordingly, we made nine recommendations to DHS to address these issues and others. The department agreed with our recommendations and has taken action to address one of them. However, as of August 2018, eight of these recommendations had not been implemented.
- **DHS had been challenged in measuring how the NCCIC was performing its functions in accordance with mandated implementing principles.** In February 2017, we reported[3] instances where, with certain products and services, NCCIC had implemented its functions in adherence with one or more of its principles, as required by the National Cybersecurity Protection Act of 2014 and Cybersecurity Act of 2015.[4] For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts.

[1]NCPS 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.

[2]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).

[3]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).

[4]*The National Cybersecurity Protection Act of 2014* and *Cybersecurity Act of 2015* require NCCIC to carry out 11 cybersecurity functions, to the extent practicable, in accordance with nine principles. Pub. L. No. 113-282, Dec. 18, 2014. The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

However, we also identified instances where the cybersecurity functions were not performed in adherence with the principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities, but it had not established measures or other procedures for ensuring the timeliness of these assessments. Further, we reported that NCCIC faces impediments to performing its cybersecurity functions more efficiently, such as tracking security incidents and working across multiple network platforms. Accordingly, we made nine recommendations to DHS related to implementing the requirements identified in the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015. The department agreed with our recommendations and has taken action to address two of them. However, as of August 2018, the remaining seven recommendations had not been implemented.

Appendix VII: Action 6—Address Weaknesses in Federal Agency Information Security Programs

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program and evaluate it for effectiveness.[1] The act retains many of the requirements for federal agencies' information security programs previously set by the Federal Information Security Management Act of 2002.[2] These agency programs should include periodic risk assessments; information security policies and procedures; plans for protecting the security of networks, facilities, and systems; security awareness training; security control assessments; incident response procedures; a remedial action process, and continuity plans and procedures.

In addition, Executive Order 13800[3] states that the President will hold agency heads accountable for managing cybersecurity risk to their enterprises. In addition, according to the order, it is the policy of the United States to manage cybersecurity risk as an executive branch enterprise because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security.

Over the past several years, we have performed numerous security control audits to determine how well agencies are managing information security risk to federal information systems and data through the implementation of effective security controls. These audits have resulted in the identification of hundreds of deficiencies related to agencies' implementation of effective security controls. Accordingly, we provided agencies with limited official use only reports identifying technical security control deficiencies for their respective agency. In these reports, we made hundreds of recommendations related to improving agencies' implementation of those security control deficiencies.

In addition to systems and networks maintained by federal agencies, it is also important that agencies ensure the security of federal information systems operated by third party providers, including cloud service

[1]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.

[2]The *Federal information Security Management Act of 2002* was enacted as Pub.L. No. 107-347, Title III, 116 Stat.2899, 2946 (Dec. 17, 2002).

[3]Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order 13800 (Washington, D.C.: May 11, 2017).

providers. Cloud computing is a means for delivering computing services via information technology networks. Since 2009, the government has encouraged agencies to use cloud-based services to store and process data as a cost-savings measure. In this regard, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is intended to ensure that cloud computing services have adequate information security, eliminate duplicative efforts, and reduce costs.

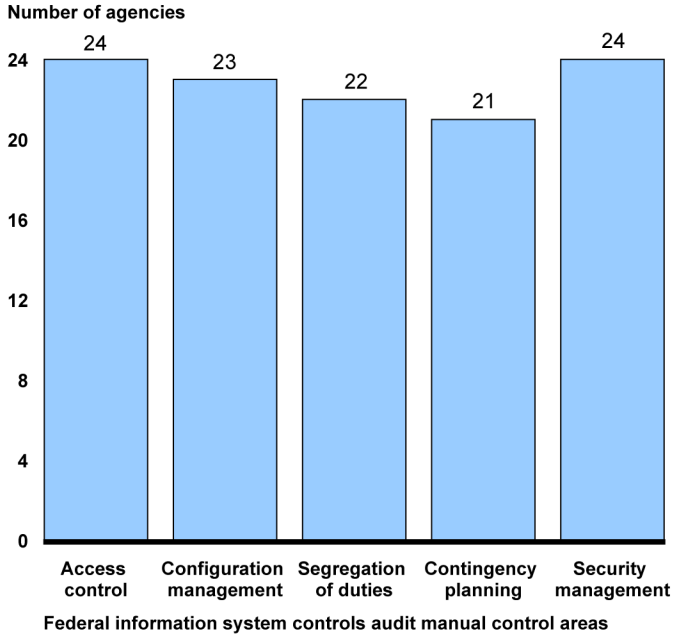
Although there are requirements and government-wide programs to assist with ensuring the security of federal information systems maintained by federal agencies and third party providers, we have identified weaknesses in agencies' implementation of information security programs.

- **Federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices.** In September 2017, we reported that most of the 24 agencies covered by the Chief Financial Officers (CFO) Act[4] had weaknesses in each of the five major categories of information system controls (i.e., access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management).[5] Weaknesses in these security controls indicate that agencies did not adequately or effectively implement information security policies and practices during fiscal year 2016. Figure 9 identifies the number of agencies with information security weaknesses in each of the five categories.

[4]There are 24 agencies identified in the Chief Financial Officers Act: the 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; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[5]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).

Figure 9: The 24 Chief Financial Officers Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 *Chief Financial Officers Act* agencies' information security practices and policies for fiscal year 2016. | GAO-18-622

Note: The 24 agencies identified in the Chief Financial Officers Act: the 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; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

In addition, we found that several agencies had not effectively implemented some aspects of its information security program, which resulted in weaknesses in these agencies' security controls.

- In July 2017, we reported that the Security Exchange Commission did not always keep system security plans complete and accurate or fully implement continuous monitoring, as required by agency policy.[6] We made two recommendations to the Security Exchange Commission to effectively manage its information security program. The agency

[6]GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions,* GAO-17-469 (Washington, D.C.: July 27, 2017).

agreed with our recommendations; however, as of August 2018, they had not been implemented.

- In another July 2017 report, we noted that the Internal Revenue Service (IRS) did not effectively support a risk-based decision to accept system deficiencies; fully develop, document, or update information security policies and procedures; update system security plans to reflect changes to the operating environment; perform effective tests and evaluations of policies, procedures, and controls; or address shortcomings in the agency's remedial process.[7] Accordingly, we made 10 recommendations to IRS to more effectively implement security-related policies and plans. The agency neither agreed nor disagreed with the recommendations; as of August 2018, all 10 recommendations had not been implemented.
- In May 2017, we reported that the Federal Deposit Insurance Corporation did not include all necessary information in procedures for granting access to a key financial application; fully address its Inspector General findings that security control assessments of outsourced service providers had not been completed in a timely manner; fully address key previously identified weaknesses related to establishing agency-wide configuration baselines and monitoring changes to critical server files; or complete actions to address the Inspector General's finding that the Federal Deposit Insurance Corporation had not ensured that major security incidents are identified and reported in a timely manner.[8] We made one recommendation to the agency to more fully implement its information security program. The agency agreed with our recommendation and has taken steps to implement it.
- In August 2016, we reported that the Food and Drug Administration did not fully implement certain security practices involved with assessing risks to systems; complete or review security policies and procedures in a timely manner; complete and review system security plans annually; always track and fully train users with significant security responsibilities; fully test controls or monitor them; remediate identified security weaknesses in a timely fashion based on risk; or

[7]GAO, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data,* GAO-17-395 (Washington, D.C.: July 26, 2017).

[8]GAO, *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information,* GAO-17-436 (Washington, D.C.: May 31, 2017).

fully implement elements of its incident response program.[9] Accordingly, we issued 15 recommendations to the Food and Drug Administration to fully implement its agency-wide information security program. The agency agreed with our recommendations. As of August 2018, all 15 recommendations had been implemented.

- In May 2016, we reported that a key reason for the information security weaknesses in selected high-impact systems at four agencies—National Aeronautics and Space Administration, Nuclear Regulatory Commission, the Office of Personnel Management, and Department of Veterans Affairs—was that they had not effectively implemented elements of their information security programs.[10] For example, most of the selected agencies had conducted information security control assessments for systems, but not all assessments were comprehensive. We also reported that remedial action plans developed by the agencies did not include all the required elements, and not all agencies had developed a continuous monitoring strategy. Table 4 identifies the extent to which the selected agencies implemented key aspects of their information security programs.

Table 4: Agency Implementation of Key Information Security Program Elements for Selected Systems

	National Aeronautics and Space Administration	Nuclear Regulatory Commission	Office of Personnel Management	Department of Veterans Affairs
Risk assessments	●	●	●	●
Security plans	●	◐	◐	◐
Controls assessments	◐	◐	◐	○
Remedial action plans	◐	◐	◐	◐

Note: ● – Met ◐ – Partially Met ○ – Did not meet

Source: GAO analysis of agency documentation. | GAO-18-622

Accordingly, we made 19 recommendations to the four selected agencies to correct these weaknesses. Agency responses to the recommendations varied. Further, as of August 2018, 16 of the 19 recommendations had not been implemented.

[9]GAO, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk,* GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

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

- **DOD's monitoring of progress in implementing cyber strategies varied.** In August 2017, we reported[11] that the DOD's progress in implementing key strategic cybersecurity guidance—the *DOD Cloud Computing Strategy*, *DOD Cyber Strategy*, and *DOD Cybersecurity Campaign*—has varied.[12] More specifically, we determined that the department had implemented the cybersecurity objectives identified in the *DOD Cloud Computing Strategy* and had made progress in implementing the *DOD Cyber Strategy* and *DOD Cybersecurity Campaign*. However, the department's process for monitoring implementation of the *DOD Cyber Strategy* had resulted in the closure of tasks as implemented before the tasks were fully implemented. In addition, the *DOD Cybersecurity Campaign* lacked time frames for completion and a process to monitor progress, which together provide accountability to ensure implementation.

  We made two recommendations to improve DOD's process of ensuring its cyber strategies are effectively implemented. The department partially concurred with these recommendations and identified actions it planned to take to address them. We noted that, if implemented, the actions would satisfy the intent of our recommendations. However, as of August 2018, DOD had not yet implemented our recommendations.

- **Agencies had not fully defined the role of their Chief Information Security Officers (CISO), as required by FISMA.** In August 2016, we reported[13] that 13 of 24 agencies covered by the CFO Act had not fully defined the role of their CISO.[14] For example, these agencies did not always identify a role for the CISO in ensuring that security controls are periodically tested; procedures are in place for detecting, reporting, and responding to security incidents; or contingency plans and procedures for agency information systems are in place. Thus,

[11]GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened,* GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

[12]Department of Defense Chief Information Officer, *Cloud Computing Strategy* (July 2012); Department of Defense. *DOD Cybersecurity Campaign* (June 2015) (For official use only); and Department of Defense, *The Department of Defense Cyber Strategy* (April 2015) (hereinafter cited as *The DOD Cyber Strategy*).

[13]GAO-16-686.

[14]Under the *Federal Information Security Modernization Act of 2014*, the agency CISO has the responsibility to ensure that the agency is meeting the requirements of the law, including developing, documenting, and implementing the agency-wide information security program.

we determined that the CISOs' ability to effectively oversee these agencies' information security activities can be limited.

To assist CISOs in carrying out their responsibilities and better define their roles, we made a total of 34 recommendations to OMB and 13 agencies in our review. Agency responses to the recommendations varied; as of August 2018, 18 of the 34 recommendations had not been implemented.

Appendix VIII: Action 7—Enhance the Federal Response to Cyber Incidents

Presidential Policy Directive-41[1] sets forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities. According to the directive, federal agencies shall undertake three concurrent lines of effort when responding to any cyber incident: threat response;[2] asset response;[3] and intelligence support and related activities.[4] In addition, when a federal agency is an affected entity, it shall undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

We have reviewed federal agencies' preparation and response to cyber incidents and have identified the following weaknesses:

- **The Office of Personnel Management (OPM) had not fully implemented controls to address deficiencies identified as a result of a cyber incident**. In August 2017, we reported that OPM did not fully implement the 19 recommendations made by the Department of Homeland Security's (DHS) United States Computer Emergency

[1]The White House, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, D.C.: July 2016).

[2]Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing an operational coordination with asset response.

[3]Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk of the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

[4]Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

Readiness Team (US-CERT)[5] after the data breaches in 2015.[6] Specifically, we noted that, after breaches of personnel and background investigation information were reported, US-CERT worked with the agency to resolve issues and develop a comprehensive mitigation strategy. In doing so, US-CERT made 19 recommendations[7] to OPM to help the agency improve its overall security posture and, thus, improve its ability to protect its systems and information from security breaches.

In our August 2017 report, we determined that OPM had fully implemented 11 of the 19 recommendations. For the remaining 8 recommendations, actions for 4 were still in progress. For the other 4 recommendations, OPM indicated that it had completed actions to address them, but we noted further improvements were needed. Further, OPM had not validated actions taken to address the recommendations in a timely manner.

As a result of our review, we made five other recommendations to OPM to improve its response to cyber incidents. The agency agreed with four of these and partially concurred with the one related to validating its corrective action. The agency did not cite a reason for its partial concurrence and we continued to believe that the recommendation was warranted. As of August 2018, three of the five recommendations had not been implemented.

- **The Department of Defense (DOD) had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises.** In September 2016, we reported that DOD had not identified the National Guard's cyber capabilities or addressed challenges in its exercises.[8]

[5]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.

[6]GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed,* GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[7]Due to the sensitive nature of the recommendations, we did not provide specific recommendations or specific examples associated with them in the related report. Generally, the recommendations pertained to strengthening activities and controls related to passwords, access permissions, patches, audit and monitoring, among other things.

[8]GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises,* GAO-16-574 (Washington, D.C.: Sept. 6, 2016).

Specifically, DOD had not identified and did not have full visibility into National Guard cyber capabilities that could support civil authorities during a cyber incident because the department has not maintained a database that identifies National Guard cyber capabilities, as required by the *National Defense Authorization Act for Fiscal Year 2007*. In addition, we identified three types of challenges with DOD's cyber exercises that could limit the extent to which DOD is prepared to support civilian authorities in a cyber incident:

- limited access because of classified exercise environments;
- limited inclusion of other federal agencies and critical infrastructure owners; and
- inadequate incorporation of joint physical-cyber scenarios.

In our September 2016 report, we noted that DOD had not addressed these challenges. Furthermore, we stated that DOD had not addressed its goals by conducting a "tier 1" exercise (i.e., an exercise involving national-level organizations and combatant commanders and staff in highly complex environments), as stated in the *DOD Cyber Strategy*.[9]

Accordingly, we recommended that DOD (1) maintain a database that identifies National Guard cyber capabilities and (2) conduct a tier 1 exercise to prepare its forces in the event of a disaster with cyber effects. The department partially agreed with our recommendations, stating that its current mechanisms and exercises are sufficient to address the issues highlighted in our report. However, we continued to believe the recommendations were valid. As of August 2018, our two recommendations had not been implemented.

- **DOD had not identified, clarified, or implemented all components of its incident response program.** In April 2016, we also reported that DOD had not clarified its roles and responsibilities for defense support of civil authorities during cyber incidents.[10] Specifically, we

[9]DOD is to conduct tier 1 exercises that are designed to prepare national-level organizations and combatant commanders and staffs at the strategic and operational level to integrate interagency, non-governmental, and multinational partners in highly complex environments. The goal of these exercises is to integrate a diverse audience in a joint training environment and identify core competencies, procedural disconnects, and common ground to achieve U.S. unity of effort.

[10]GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents,* GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

found that DOD's overarching guidance about how it is to support civil authorities as part of its Defense Support of Civil Authorities mission did not clearly define the roles and responsibilities of key DOD entities, such as DOD components, the supported command, or the dual-status commander, if they are requested to support civil authorities in a cyber incident. Further, we found that, in some cases, DOD guidance provides specific details on other types of Defense Support of Civil Authorities-related responses, such as assigning roles and responsibilities for fire or emergency services support and medical support, but does not provide the same level of detail or assign roles and responsibilities for cyber support.

Accordingly, we recommended that DOD issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with the recommendation and stated that the department will issue or update guidance. However, as of August 2018, the department had not implemented our recommendation.

- **DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.** In January 2016, we reported that NCPS had a limited ability to detect intrusions across all types of network types.[11] In addition, we reported that the system's intrusion prevention capability was limited and its information-sharing capability was not fully developed. Furthermore, we reported that DHS's current metrics did not comprehensively measure the effectiveness of NCPS. Accordingly, we made nine recommendations to DHS to address these issues and others. The department agreed with our recommendations and has taken action to address one of them. However, as of August 2018, eight of these recommendations had not been implemented.

[11]GAO-16-294.

Appendix IX: Action 8—Strengthen the Federal Role in Protecting the Cybersecurity of Critical Infrastructure

The nation's critical infrastructure include both public and private systems vital to national security and other efforts including providing the essential services, such as banking, water, and electricity—that underpin American society. The cyber threat to critical infrastructure continues to grow and represents a national security challenge. To address this cyber risk, the President issued Executive Order 13636[1] in February 2013 to enhance the security and resilience of the nation's critical infrastructure and maintain a cyber environment that promotes safety, security, and privacy.

In accordance with requirements in the executive order which were enacted into law in 2014, the National Institute of Standards and Technology (NIST) facilitated the development of a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure. This process, which involved stakeholders from the public and private sectors, resulted in NIST's *Framework for Improving Critical Infrastructure Cybersecurity.*[2] The framework is to provide a flexible and risk-based approach for entities within the nation's 16 critical infrastructure sectors to protect their vital assets from cyber-based threats. Since then, progress has been made to protect the critical infrastructure of the nation but we have reported that challenges to ensure the safety and security of our infrastructure exist.

- **The Department of Homeland Security (DHS) had not measured the impact of its efforts to support cyber risk reduction for high-risk chemical sector entities.** In August 2018, we reported that DHS had strengthened its processes for identifying high-risk chemical facilities and assigning them to tiers under its Chemical Facility Anti-Terrorism Standards program.[3] However, we found that DHS's new performance measure methodology did not measure reduction in vulnerability at a facility resulting from the implementation and verification of planned security measures during the compliance inspection process. We concluded that doing so would provide DHS an opportunity to begin assessing how vulnerability is reduced—and by extension, risk lowered—not only for individual high-risk facilities

[1]Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[2]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

[3]GAO, *Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders*, GAO-18-538 (Washington, D.C.: Aug. 8, 2018).

but for the Chemical Facility Anti-Terrorism Standards program as a whole.

We also determined that, although DHS shares some Chemical Facility Anti-Terrorism Standards program information, first responders and emergency planners may not have all of the information they need to minimize the risk of injury or death when responding to incidents at high-risk facilities. This was due to first responders at the local level not having access or widely using a secure interface that DHS developed (known as the Infrastructure Protection Gateway) to obtain information about high-risk facilities and the specific chemicals they process.

To address the weaknesses we identified, we recommended that DHS take actions to (1) measure reduction in vulnerability of high-risk facilities and use that data to assess program performance, and (2) encourage access to and wider use of the Infrastructure Protection Gateway among first responders and emergency planners. DHS concurred with both recommendations and outlined efforts underway or planned to address them.

- **The federal government had identified major challenges to the adoption of the cybersecurity framework.** In February 2018, we reported that there were four different challenges to adopting the cybersecurity framework, including limited resources and competing priorities, reported by entities within their sectors.[4] We further reported that none of the 16 sector-specific agencies[5] were measuring the implementation by these entities, nor did they have qualitative or quantitative measures of framework adoption. While research had been done to determine the use of the framework in the sectors, these efforts had yielded no real results for sector wide adoption. We concluded that, until sector-specific agencies understand the use of the framework by the implementing entities, their ability to understand

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

[5]Sector-specific agencies are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise. They accomplish this by leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the environment.

implementation efforts would be limited.[6] Accordingly, we made a total of nine recommendations to nine sector-specific agencies to address these issues. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed; as of August 2018, all five recommendations had not been implemented.

- **Agencies had not addressed risks to their systems and the information they maintain.** In January 2018, we reported that the Department of Defense (DOD) and Federal Aviation Administration (FAA) identified a variety of operations and physical security risks related to Automatic Dependent Surveillance-Broadcast Out technology that could adversely affect DOD missions.[7] These risks came from information broadcast by the system itself,[8] as well as from potential vulnerabilities to electronic warfare- and cyber-attacks, and from the potential divestment of secondary-surveillance radars.[9] However, DOD and FAA had not approved any solutions to address the risks they identified to the system. Accordingly, we recommended that DOD and FAA, among other things, take action to approve one or more solutions to address Automatic Dependent Surveillance-Broadcast Out-related security risks. DOD and FAA generally agreed with our recommendations; however, as of August 2018, they had not been implemented.
- **Major challenges existed to securing the electricity grid against cyber threats.** In October 2015, we testified on the status of the electricity grid's cybersecurity, reporting that entities associated with the grid have encountered several challenges.[10] We noted that these

[6]The previous report, GAO-16-152, highlighted actions taken by agencies to develop and promote the framework. However, we identified deficiencies in agencies' ability to measure progress of their programs for promoting the adoption of the framework.

[7]GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[8]In 2010, the FAA issued a final rule that requires all aircraft, including military aircraft, flying in specified airspace within the national airspace system as of January 1, 2020, to be equipped with technology that would transmit flight information to an enabled receiver. See 14 C.F.R §§ 91.225 and 91.227.

[9]DOD defines an electronic attack as a division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

[10]GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

challenges included implementation monitoring, built-in security features in smart grid systems, and establishing metrics for cybersecurity. We concluded that continued attention to these issues and cyber threats in general was required to help mitigate these risks to the electricity grid.

- **DHS and other agencies needed to enhance cybersecurity in the maritime environment.** In October 2015, we testified on the status of the cybersecurity of our nation's ports, concluding that steps needed to be taken to enhance their security.[11] Specifically, we noted that DHS needed to include cyber risks in its risk assessments that are already in place as well as addressing cyber risks in guidance for port security plans. We concluded that, until DHS and the other stakeholders take steps to address cybersecurity in the ports, risk of a cyber-attack with serious consequences are increased.
- **Sector-specific agencies were not properly addressing progress or metrics to measure their progress in cybersecurity.** In November 2015, we reported that sector-specific agencies were not comprehensively addressing the cyber risk to the infrastructure, as 11 of the 15 sectors had significant cyber risk.[12] Specifically, we noted that these entities had taken actions to mitigate their cyber risk; however, most had not identified incentives to promote cybersecurity in their sectors. We concluded that while the sector-specific agencies have successfully disseminated the information they possess, there was still work to be done to properly measure cybersecurity implementation progress. Accordingly, we made seven recommendations to six agencies to address these issues. Four of these agencies agreed with our recommendation, while two agencies did not comment on the recommendations. As of August 2018, all seven recommendations had not been implemented.

[11]GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*, GAO-16-116T (Washington, D.C.: Oct. 8, 2015).

[12]GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015). The government facilities sector was excluded from the scope of this review due to its uniquely governmental focus.

Appendix X: Action 9—Improve Federal Efforts to Protect Privacy and Sensitive Data

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.

Certain agencies, such as the Department of Education's Office of Federal Student Aid and the Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS), hold millions of sensitive records for people all over the country. The focus on personally identifiable information (PII) is to protect this information as much as feasibly possible using federal standards and procedures to mitigate the risk that is always present with this type of information. We have issued several reports noting that agencies can take steps to improve their protection of privacy and sensitive data. For example:

- **CMS and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.** In March 2018, we reported that CMS shares Medicare beneficiary data with three external entities—Medicare Administrative Contractors, researchers, and other qualified public and private entities.[1] However, we identified weakness in their oversight of these entities. Specifically, we found that researchers were not given guidance for how to implement proper security controls nor was there a program to oversee security implementation for these researchers or for qualified entities. As such, we made three recommendations to CMS to improve its oversight of the external entities it works with. The agency agreed with our recommendations, but had not implemented them as of August 2018.
- **The Department of Education's Office of Federal Student Aid did not properly oversee its school partners' records or information security programs.** In December 2017, we reported that the agency had established policies and procedures for managing and protecting the student information, but there were shortcomings that hindered

[1]GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, GAO-18-210 (Washington, D.C.: March 6, 2018).

the effectiveness of these procedures.[2] Based on a survey of the schools, the majority of the schools had policies in place for records retention but the way these policies were implemented was highly varied for paper and electronic records. We also found that the oversight of the school's programs was lacking, as Federal Student Aid conducts reviews but does not consider information security as a factor for selecting schools.

Accordingly, we made seven recommendations to the Department of Education. The department agreed with five of the recommendations, partially agreed with one, and did not agree with one recommendation. However, we continued to believe that all the recommendations were warranted. As of August 2018, all of our recommendations had not been implemented.

- **HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.** In August 2016, we reported that HHS's guidance for securing electronic health information issued by the department did not address all key controls called for by other federal cybersecurity guidance.[3] In addition, the 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 to address these issues; however, as of August 2018, the five recommendations had not been implemented.
- **CMS had not fully protected the privacy of users' data on state-based marketplaces**. In March 2016, we reported on weaknesses in technical controls for the "data hub" that CMS uses to exchange information between its health insurance marketplace and external partners.[4] We also identified significant weaknesses in the controls in place at three selected state-based marketplaces established to carry

[2]GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information,* GAO-18-121 (Washington, D.C.: Dec. 15, 2017).

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

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

out provisions of the Patient Protection and Affordable Care Act.[5] We made three recommendations to CMS related to defining procedures for overseeing the security of state-based marketplaces and requiring continuous monitoring of state marketplace controls. HHS concurred with our recommendations. As of August 2018, two of the recommendations had not yet been implemented.

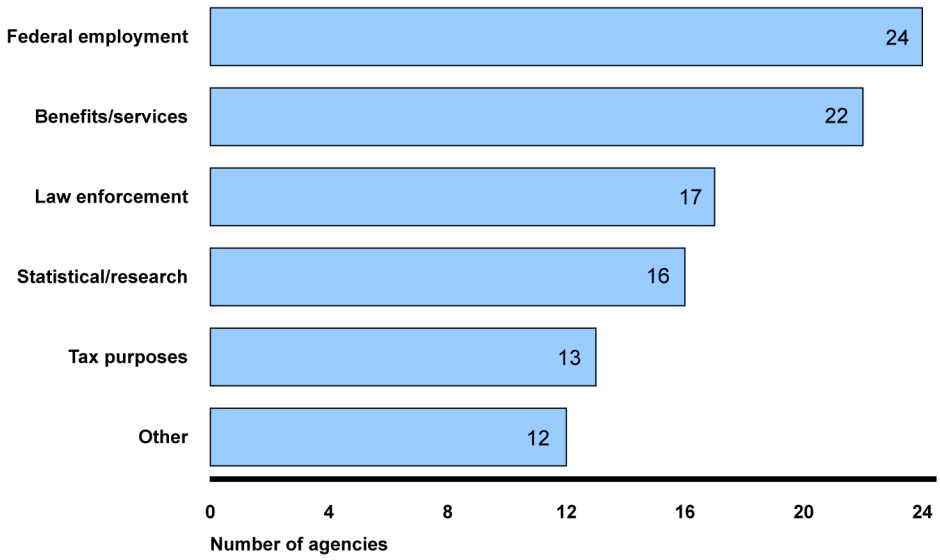
- **Poor planning and ineffective monitoring had resulted in the unsuccessful implementation of government initiatives designed to protect federal data**. In July 2017, we reported that government initiatives aimed at eliminating the unnecessary collection, use, and display of Social Security numbers (SSN) have had limited success.[6] Specifically, in agencies' response to our questionnaire on SSN reduction efforts, the 24 agencies covered by the Chief Financial Officers Act[7] reported successfully curtailing the collection, use, and display of SSNs. Nevertheless, all of the agencies continued to rely on SSNs for important government programs and systems, as seen in figure 10.

[5]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).

[6]GAO, *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display,* GAO-17-553 (Washington, D.C.: July 25, 2017).

[7]There are 24 agencies identified in the Chief Financial Officers Act: the 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; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

Figure 10: Agency Reported Use of Social Security Numbers



Source: Agency-reported data. | GAO-18-622

We also determined that poor planning by agencies and ineffective monitoring by the Office of Management and Budget (OMB) had also limited efforts to reduce SSN use. For example, lacking direction from OMB, many agencies' SSN reduction plans did not include key elements, such as time frames and performance indicators, calling into question their utility. Moreover, OMB had not required agencies to maintain up-to-date inventories of their SSN holdings or provided criteria for determining "unnecessary use and display," limiting agencies' ability to gauge progress. Finally, OMB had not ensured that agencies update their progress in annual reports or established performance metrics to monitor agency efforts. Accordingly, we made five recommendations to the Director of OMB to address these issues. As of August 2018, all five recommendations had not been implemented.

Appendix XI: Action 10—Appropriately Limit the Collection and Use of Personal Information and Ensure That It Is Obtained with Appropriate Knowledge or Consent

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of personally identifiable information (PII) maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

- **The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent.**[1] In May 2017, we reported that the IoT has become increasingly used to communicate and process vast amounts of information using "smart" devices (such as a fitness tracker connected to a smartphone). However, we noted that this emerging technology also presents new issues in areas such as information security, privacy, and safety.
- **Smartphone tracking apps can present serious safety and privacy risks.** In April 2016, we reported on smartphone applications that facilitated the surreptitious tracking of a smartphone's location and other data.[2] Specifically, we noted that some applications could be used to intercept communications and text messages, essentially facilitating the stalking of others. While it is illegal to use these applications for these purposes, stakeholders differed over whether current federal laws needed to be strengthened to combat stalking. We also noted that stakeholders expressed concerns over what they perceived to be limited enforcement of laws related to tracking apps and stalking. In particular, domestic violence groups stated that additional education of law enforcement officials and consumers about how to protect against, detect, and remove tracking apps is needed.

[1]GAO-17-75.

[2]GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking*, GAO-16-317 (Washington, D.C.: May 9, 2016).

- **The Federal Bureau of Investigation (FBI) has not ensured privacy and accuracy related to the use of face recognition technology.** In May 2016, we reported[3] that the Department of Justice had not been timely in publishing and updating privacy documentation for the FBI's use of face recognition technology.[4] 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. We continued to believe all the recommendations made were valid. As of August 2018, the six recommendations had not been implemented.

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

[4]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.

Appendix XII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342 or marinosn@gao.gov
Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Jon Ticehurst, Assistant Director; Kush K. Malhotra, Analyst-In-Charge; Chris Businsky; Alan Daigle; Rebecca Eyler; Chaz Hubbard; David Plocher; Bradley Roach; Sukhjoot Singh; Di'Mond Spencer; and Umesh Thakkar made key contributions to this report.