United States Government Accountability Office

Testimony

Before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, July 25, 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Accessible Version

Statement of Gene L. Dodaro,
Comptroller General of the United States

GAO Highlights

Highlights of GAO-18-645T, a testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

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.

GAO was asked to update its 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 July 2018, about 1,000 still needed to be implemented.

View GAO-18-645T. 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.

July 2018

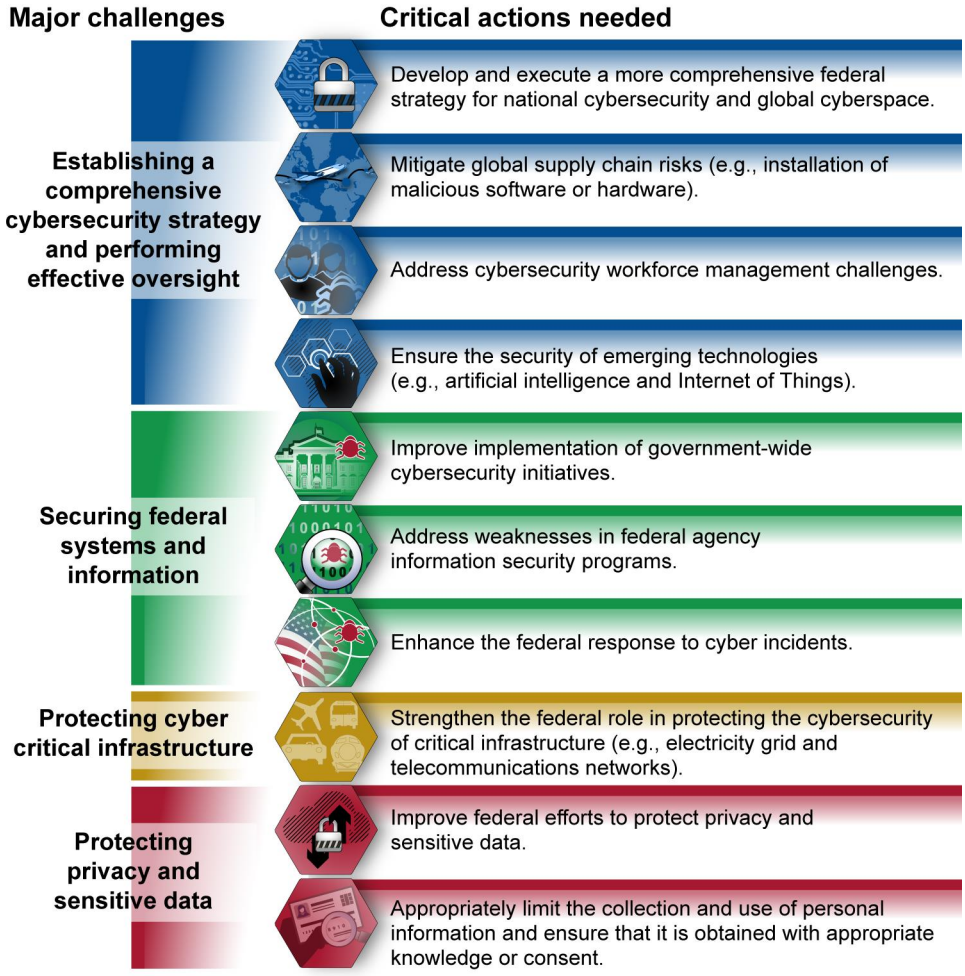
HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

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-18-645T

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.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees:

I appreciate the opportunity to be here today to participate in your hearing on cybersecurity challenges. 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 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]

[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 (USA PATRIOT Act) 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.

[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.

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.

At your request, my testimony updates 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. This statement 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.

[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.

[5]GAO-17-317.

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 experience challenges.

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.

[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).

We conducted the work on which this testimony is based 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.

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

[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.

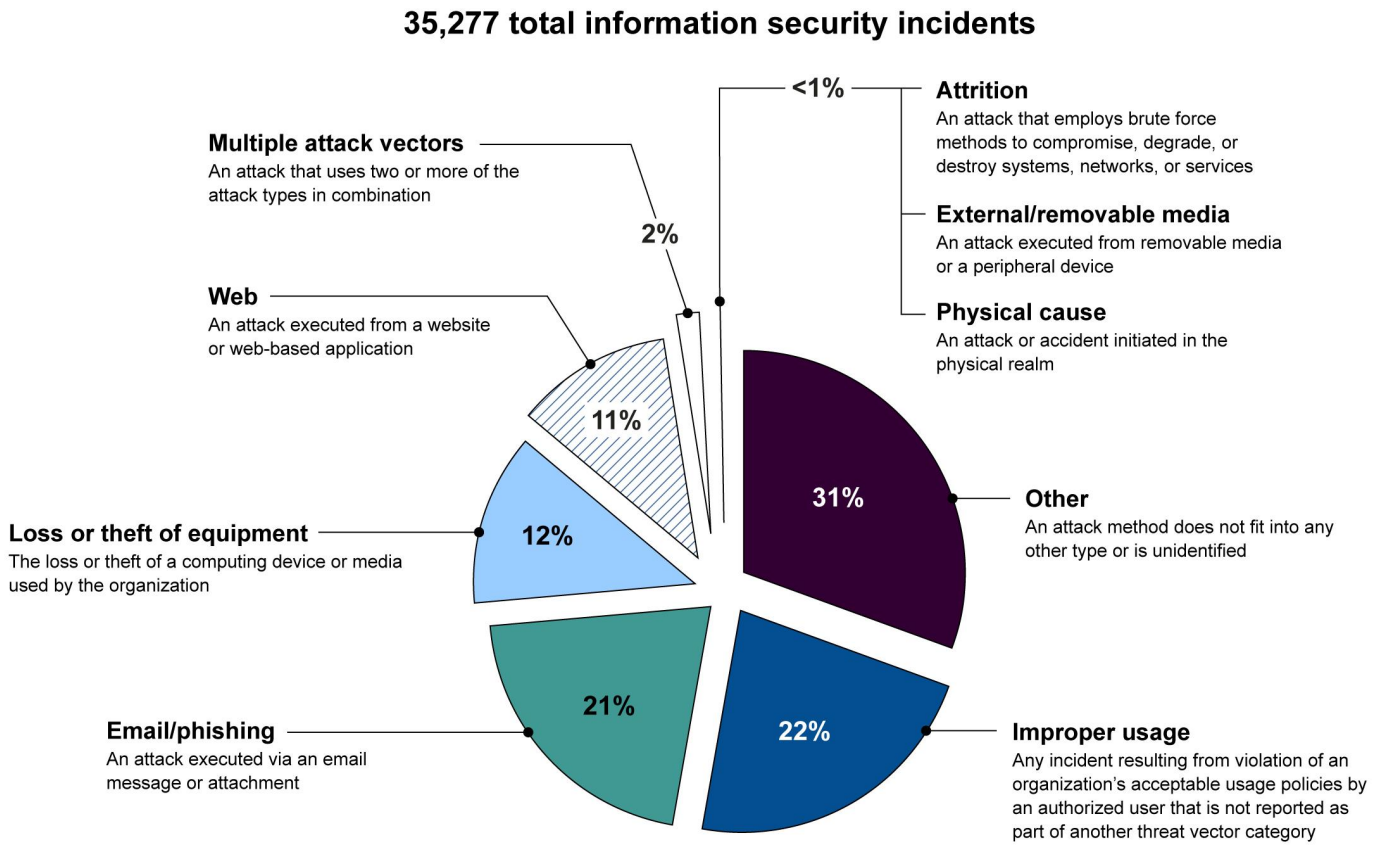
[12]The Federal Information Security Modernization Act of 2014 was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code.

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

[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.

the nine threat vector categories for fiscal year 2017, as reported by OMB.

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-18-645T

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

Other	Improper Usage	E-mail/ Phishing	Loss or Theft of Equipment	Web	Multiple Attack Vectors	Attrition	External/ Removable Media	Physical cause
10818	7856	7328	4395	4049	601	151	72	7

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 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

[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.

[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.

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 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.

[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).

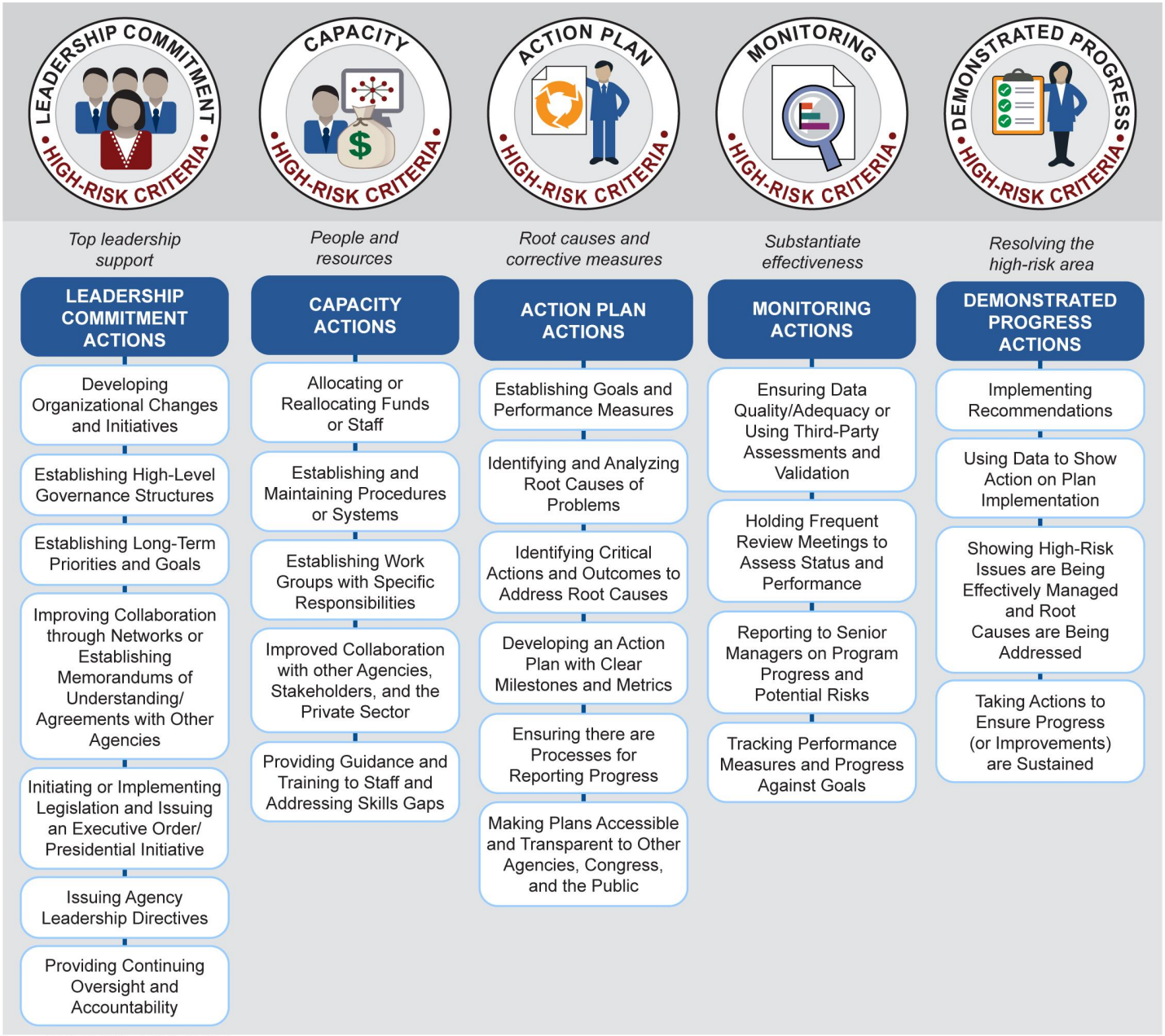
Our experience has shown that the key elements needed to make progress toward being removed from the High-Risk List are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action. The five criteria for removal that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

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

- **Leadership Commitment.** Demonstrated strong commitment and top leadership support.
- **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-18-645T

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-18-645T

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.

[21]GAO-17-317.

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 needed to address them are summarized following the table.

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

Source: GAO analysis. | GAO-18-645T

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 timeframes for their completion.[24] Accordingly, we recommended that the White House Cybersecurity Coordinator[25] in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a

[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 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.

national strategy[26] 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*.[27] 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.

[26]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).

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

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 Executive Order required federal agencies to take a variety of actions, including to better manage their cybersecurity risks and coordinate to meet reporting requirements related to the cybersecurity of federal networks, critical infrastructure, and the nation.[a] As of July 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-18-645T

[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 mid-August 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 to 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 to 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.

- **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).[28] 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.

  Earlier this month, we testified that if such global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[29] Thus, the potential exists 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 agencywide information security programs.

- **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*

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

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

of 2015.[30] We determined that most of the Chief Financial Officers (CFO) Act[31] 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.[32] In addition, we have reported in the last 2 years that federal agencies (1) had not identified and closed cybersecurity skills gaps,[33] (2) had been challenged with recruiting and retaining qualified staff,[34] and (3) had difficulty navigating the federal hiring process.[35]

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

[30]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).

[31]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.

[32]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).

[33]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).

[34]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).

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

private sectors. In May 2018, the departments issued a report[36] 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, among other things, proposals for solving the federal cybersecurity workforce shortage.[37] 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

[36]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).

[37]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).

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.

- **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;[38]
  - 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;[39]
  - vehicles that are potentially susceptible to cyber-attack through technology, such as Bluetooth;[40]
  - the unknown impact of artificial intelligence cybersecurity; and[41]
  - advances in cryptocurrencies and blockchain technologies.[42]

  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

[38]GAO, *Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[39]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).

[40]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).

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

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

on the opportunities and challenges in reducing the botnet threat.[43] 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.

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 July 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 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;
- selected agencies' ability to implement cloud service technologies and notable benefits this might have on agencies; and

[43]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).

- the federal approach and strategy to securing agency information systems, to include federal intrusion detection and prevention capabilities and the intrusion assessment plan.

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.[44] In addition, in February 2017, we reported[45] that the DHS National Cybersecurity and Communications Integration Center's (NCCIC)[46] functions were not being performed in adherence with the

[44]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.

[45]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).

[46]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.

principles set forth in federal laws.[47] 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.

- **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);[48]
  - three agencies—the Securities Exchange Commission, the Federal Deposit Insurance Corporation, and the Food and Drug Administration—had not effectively implemented aspects of their information security programs, which resulted in weaknesses in these agencies' security controls;[49]
  - 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;[50]

[47] *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.

[48] 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).

[49] 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).

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

- 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;[51] and
- agencies had not fully defined the role of their Chief Information Security Officers, as required by FISMA.[52]

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. [53]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.

- **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;[54]
  - DOD had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises.[55]
  - as of April 2016, DOD had not identified, clarified, or implemented all components of its support of civil authorities during cyber incidents;[56] and

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

[52]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).

[53]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).

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

[55]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).

- as of January 2016, DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.[57]

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.[58] As of July 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 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)[59] 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;

[56]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).

[57]GAO-16-294.

[58]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.

[59]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.

- 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
- federal intrusion detection and prevention capabilities.

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 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, 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.[60]

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:

- Entities within the 16 critical infrastructure sectors reported encountering four challenges to adopting the cybersecurity

[60] 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.

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.[61]

- Major challenges existed to securing the electricity grid against cyber threats.[62] These challenges included monitoring implementation of 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.[63]
- Sector-specific agencies[64] were not properly addressing progress or metrics to measure their progress in cybersecurity.[65]
- DOD and the Federal Aviation Administration identified a variety of operations and physical security risks that could adversely affect DOD missions.[66]

We made a total of 19 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.[67] As of July 2018, all

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

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

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

[64]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.

[65]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.

[66]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).

[67]GAO-18-211.

19 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
- 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.[68]
  - The Department of Education's Office of Federal Student Aid had not properly overseen its school partners' records or information security programs.[69]
  - HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.[70]
  - CMS had not fully protected the privacy of users' data on state-based marketplaces.[71]
  - 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.[72]
- **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:

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

[69]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).

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

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

[72]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).

- The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent;[73]
- Federal laws for smartphone tracking applications have not generally been well enforced.[74]
- The FBI has not fully ensured privacy and accuracy related to the use of face recognition technology.[75]

We have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974[76] and the E-Government Act of 2002,[77] because they may not consistently protect PII.[78] 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[79] 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.[80] However, these suggested changes have not yet been enacted.

[73]GAO-17-75.

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

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

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

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

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

[79]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.

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

We also made a total of 29 recommendations to federal agencies to address the weaknesses identified. As of July 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[81] and improving the accuracy of the FBI's face recognition services. Until these recommendations are implemented, 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.

In summary, 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

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

implemented as of July 2018. We have also designated 35 as priority recommendations, and as of July 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.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contacts and Staff Acknowledgments

Questions about this testimony can be directed to Nick Marinos, Director, Cybersecurity and Data Protection Issues, at (202) 512-9342 or marinosn@gao.gov; and Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are 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.

Related GAO Reports

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.

Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement. GAO-18-210. Washington, D.C.: April 5, 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.

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

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

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548