![GAO]

United States Government Accountability Office

Report to Congressional Addressees

March 2021

HIGH-RISK SERIES

Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

![GAO@100]

A Century of Non-Partisan Fact-Based Work

GAO@100

Highlights

HIGH-RISK SERIES

Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

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.

GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting (1) cyber critical infrastructure in 2003 and (2) the privacy of personally identifiable information in 2015.

In 2018, GAO reported that the federal government needed to address 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. Within these four challenges are 10 actions critical to successfully dealing with the serious cybersecurity threats facing the nation (see the figure at right identifying the four challenges and 10 actions).

This report provides an update on the progress that the federal government has made in addressing GAO's recommendations for the four major cybersecurity challenges, as of December 2020.

What GAO Found

GAO reiterates the importance of addressing the four major cybersecurity challenges and the 10 associated critical actions listed below.

Four Major Cybersecurity Challenges and 10 Associated Critical Actions

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis. | GAO-21-288

As described below, although the federal government has made selected improvements, it needs to move with a greater sense of urgency commensurate with the rapidly evolving and grave threats to the country.

- **Establishing a comprehensive cybersecurity strategy and performing effective oversight**. The prior administration's September 2018 national cybersecurity strategy and the June 2019 implementation plan detail the executive branch's approach to managing the nation's cybersecurity. In September 2020 GAO reported that the national strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed. The new administration needs to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics.

  GAO also highlighted the urgent need to clearly define a central role for leading the implementation of the national strategy. Accordingly, it recommended that the Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, the Congress did so by establishing the Office of the National Cyber Director within the Executive Office of the President. Once the position is filled, the federal government will be better situated to direct activities to overcome the nation's cyber threats and challenges, and to perform effective oversight.

United States Government Accountability Office

In performing its work, GAO generally reviewed the cybersecurity-related products it had issued since September 2018. It also assessed actions taken on prior GAO recommendations, and determined which recommendations had not yet been implemented. Further, GAO identified its relevant ongoing cybersecurity work. Finally, GAO reviewed cybersecurity findings from agency inspector general reports, and analyzed the recommendations of the U.S. Cyberspace Solarium Commission.

What GAO Recommends

Since 2010, GAO has made about 3,300 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of December 2020, more than 750 of those recommendations are not yet implemented.

GAO requested comments on a draft of this report from the Department of Homeland Security (DHS), National Security Council (NSC), and Office of Management and Budget (OMB). DHS provided technical comments, which were incorporated as appropriate. NSC staff and OMB's liaison to GAO both provided comments via email.

NSC staff stated that, as the administration charts a course for cyber policy issues, the draft offered a comprehensive review of the cybersecurity challenges facing the nation and the opportunities available to make concrete improvements. Further, NSC staff described the administration's preliminary views about the four major cybersecurity challenges identified in the report.

In its comments, OMB highlighted ongoing and planned efforts that the office is taking for two major challenges—securing federal systems and information and protecting privacy and sensitive data.

Although establishing the Cyber Director position is an essential step forward, critical risks remain on supply chains, workforce management, and emerging technologies. For example, in December 2020, GAO reported that none of the 23 agencies in its review had fully implemented key foundational practices for managing information and communications technology supply chains. It made a total of 145 recommendations to the agencies to implement such practices in their approaches to supply chain management.

- **Securing federal systems and information**. The federal government has made some progress in securing systems. Nevertheless, federal agencies continue to have numerous cybersecurity weaknesses due in large part to ineffective information security programs. Further, cyber incidents are increasingly posing a threat to government and private sector entities. The seriousness of the threat was reinforced by the December 2020 discovery of a cyberattack that has had widespread impact on government agencies, critical infrastructures, and the private sector. In 2019 GAO reported that most of the 16 agencies reviewed had incident response processes with key shortcomings thereby limiting the ability to minimize damage from attacks.

- **Protecting cyber critical infrastructure**. The nation's critical infrastructure includes both public and private systems vital to national security and other efforts including providing the essential services that underpin American society. Since 2010, GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity; for example, GAO recommended that agencies better measure the adoption of the National Institute of Standards and Technology framework of voluntary cyber standards and correct sector-specific weaknesses. However, most of these recommendations (nearly 50) have not been implemented. As a result, the risks of unprotected infrastructures being harmed are heightened.

- **Protecting privacy and sensitive data**. The federal government and private sector have struggled to protect privacy and sensitive data. Advances in technology have made it easy to correlate information about individuals and ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities. The vast number of individuals affected by various data breaches has underscored concerns that personally identifiable information is not adequately being protected. GAO's reviews of agency practices to protect sensitive data have identified weaknesses and made numerous recommendations at agencies such as the Department of Housing and Urban Development, Department of Education, and Internal Revenue Service.

In January 2019, GAO reported that the United States did not have a comprehensive internet privacy law governing the collection, use, and sale or other disclosure of consumers' personal information. Accordingly, GAO recommended that the Congress consider developing legislation on internet privacy that, among other things, would enhance consumer protections.

Contents

Figures

AI	artificial intelligence
BASE	Baseline Assessment for Security Enhancement
Bureau	Census Bureau
CBP	U.S. Customs and Border Protection
CDM	Continuous Diagnostics and Mitigation
CFATS	Chemical Facility Anti-Terrorism Standards
CFO	Chief Financial Officer
CFPB	Consumer Financial Protection Bureau
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Centers for Medicare & Medicaid Services
Commerce	Department of Commerce
COVID-19	Coronavirus Disease 2019
CRA	consumer reporting agencies
CSET	Bureau of Cyberspace Security and Emerging Technologies
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FedRAMP	Federal Risk and Authorization Management Program
FERC	Federal Energy Regulatory Commission

FISMA	Federal Information Security Modernization Act of 2014
FRT	facial recognition technology
FSA	Federal Student Aid
GLBA	Gramm-Leach-Bliley Act
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
HVA	high value asset
ICT	information and communications technology
IoT	Internet of Things
IT	information technology
IRS	Internal Revenue Service
NCPS	National Cybersecurity Protection System
NERC	North American Electric Reliability Corporation
NFR	notice of findings and recommendations
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of actions and milestones
PPD-41	Presidential Policy Directive-41
SCRM	supply chain risk management
SSA	sector-specific agency
State	Department of State
Treasury	Department of the Treasury
TSA	Transportation Security Administration
UCG	Cyber Unified Coordination Group
US-CERT	United States Computer Emergency Readiness Team

March 24, 2021

Congressional Addressees

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. In addition, 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 on the federal government's efforts to address information security deficiencies—a designation we have made in each report since 1997.[3] In 2003, we expanded the information security

---

[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, whether physical or virtual, 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: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021) 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.

high-risk area to include the protection of critical cyber infrastructure.[4] 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 to include protecting the privacy of PII.[5] 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.

In September 2018, we reported that the federal government needed to take 10 specific actions[6] to address the four major cybersecurity challenges that the federal government and other entities face: (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.[7] Since September 2018, we and others have made numerous recommendations to federal agencies and the Congress related to the 10 specific actions needed to address the four major cybersecurity challenges. For example, in March 2020, the Cyberspace

---

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

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

[6]The 10 actions are (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace; (2) mitigate global supply chain risks; (3) address cybersecurity workforce management challenges; (4) ensure the security of emerging technologies; (5) improve implementation of government-wide cybersecurity initiatives; (6) address weaknesses in federal agency information security programs; (7) enhance the federal response to cyber incidents targeting federal systems; (8) strengthen the federal role in protecting the cybersecurity of critical infrastructure; (9) improve federal efforts to protect privacy and sensitive data; and (10) appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

[7]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

Solarium Commission[8] issued its *U.S. Cyberspace Solarium Commission Final Report*, which contained 82 recommendations to Congress and federal agencies.[9] These recommendations were aimed at addressing the strategic approach needed to defend the nation against cyberattacks and the policies and legislation needed to implement that strategy. In addition, agency inspectors general have made numerous recommendations to agencies to address deficiencies in their cybersecurity programs and improve their implementation of critical infrastructure protection responsibilities.[10]

This report provides an update on the progress that agencies have made in addressing the major cybersecurity challenges. To do so, we primarily reviewed work that we have conducted since our September 2018 update (see appendix I for a list of our previously issued products).[11] Specifically, we first reviewed and summarized the findings of our prior work specific to each challenge. We then reviewed the status of our prior recommendations as of December 2020, including priority recommendations,[12] to the Executive Office of the President and federal agencies, and any actions taken by these entities to address our recommendations. Finally, we reviewed relevant findings from agency inspectors general reports,[13] and recommendations made by the

---

[8]The John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018) established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees, as well as officials from the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Federal Bureau of Investigation.

[9]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[10]See, e.g., Section III of the White House's *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2019*, which identifies many cybersecurity-related recommendations that the agency inspectors general have made.

[11]See GAO-18-622. We also highlighted products that were issued prior to our September 2018 report in select cases, such as reports that contain open recommendations.

[12]Priority recommendations are those that we believe warrant priority attention from heads of key departments or agencies. They are highlighted because, upon implementation, they may significantly improve government operation—for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue.

[13]We identified relevant findings and recommendations from inspectors general reports for the second and third challenges.

Cyberspace Solarium Commission.[14] In reviewing the status of our 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 implement them. We then summarized the actions needed and the status of our prior recommendations. We also identified our ongoing work related to each action (see appendix II for a list of our ongoing work).

We performed our work at the initiative of the U.S. Comptroller General. We conducted this performance audit from October 2020 to March 2021 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, systems and networks used by federal agencies and our nation's critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet.

With this greater connectivity, threat actors are increasingly willing and capable of conducting a cyberattack on our nation's critical infrastructure that could be disruptive and destructive. The *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* and *the 2020 Homeland Threat Assessment* noted that criminal groups and nations pose the greatest cyberattack threats to our nation.[15] According to the more recent assessment, both criminal groups and nation cyber actors—motivated by profit, espionage, or disruption—will exploit the Coronavirus Disease (COVID-19) pandemic by targeting the U.S. health care and public health

---

[14]We identified relevant findings and recommendations from the Cyberspace Solarium Commission for the first, second, and third challenges.

[15]The *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* noted the cyber risk of terrorists, in addition to nations and criminal groups. However, the more recent *2020 Homeland Threat Assessment* did not identify terrorists as one of the top cyber threats facing the nation's critical infrastructure.

sector, government response entities, and the broader emergency services sector. In addition to these threats, risks to cyber-based assets can originate from hackers, insiders, and terrorists. Table 1 describes common cyber adversaries.

Table 1: Common Cyber Adversaries

Threat actor	Description
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. According to the *2020 Homeland Threat Assessment*, criminal groups increasingly target U.S. critical infrastructure to generate profit, whether through ransomware, email impersonation fraud, social engineering, or malware. The assessment also states that ransomware attacks—which have at least doubled since 2017—often are directed against critical infrastructure entities at the state and local level by exploiting gaps in cybersecurity.
Hackers and hacktivists	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. By contrast, hacktivists are ideologically motivated actors who use cyber exploits to further political goals. Hackers and hacktivists no longer need a great amount of skill to compromise information technology systems because they can download commonly available cyberattack tools.
Insiders	Insiders are individuals (e.g., employees, contractors, or vendors) with authorized access to an information system or enterprise who have the potential to cause harm, wittingly or unwittingly, through destruction, disclosure, or modification of data, or through denial of service. Insiders could include knowledgeable employees with privileged access to critical systems or contractors with limited system knowledge.
Nations	Nations, including groups or programs sponsored or sanctioned by nation-states, use cyber tools as part of their information gathering and espionage activities. According to the *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment*, China and Russia pose the greatest cyberattack threats because they have the ability to launch cyberattacks that could disrupt or damage critical infrastructure. While China and Russia are the most capable nation-state cyber adversaries, Iranian and North Korean cyber actors also pose a threat to U.S. systems, networks, and information, according to both assessments.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. However, while terrorists are highly motivated, they do not currently have the sophisticated tools or skill necessary to execute a cyberattack that could cause a widespread outage or significantly damage the power system, according to the *2019 Worldwide Threat Assessment*. Nonetheless, terrorists could create disruptions, such as by executing denial-of-service attacks against poorly protected networks.

Source: GAO and GAO analysis of the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community and the 2020 Homeland Threat Assessment. | GAO-21-288

To facilitate their efforts, cyber adversaries use a variety of tactics, techniques. For example, according to MITRE's ATT&CK® Framework— a cybersecurity knowledgebase of adversary tactics and techniques— attackers often begin by performing reconnaissance (e.g., scanning for vulnerabilities in target hosts or applications) and establishing resources that can be used to support their operations (e.g., develop malicious

software).[16] Subsequently, attackers will seek to gain initial access to a target network by, for example, using targeted spear phishing[17] emails or exploiting weaknesses on public-facing webservers. After gaining an initial foothold, attackers will often use a variety of tactics and techniques to achieve their objectives, such as trying to run malicious code, attempting to steal account names and passwords and gain higher-level permissions, and moving throughout a network to find and gain access to their target.

These tactics and techniques can facilitate cybersecurity incidents and cyberattacks that have a range of consequences, such as disruption of critical operations; inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. According to the Federal Bureau of Investigation (FBI), some of the most common and damaging types of cybersecurity incidents include those involving business email compromise, data breaches, denial-of-service, malware, and ransomware. Table 2 describes each of these types of cybersecurity incidents as well as recent examples of them.

---

[16]"MITRE ATT&CK®," Main Page, MITRE Corporation, last accessed on February 11, 2021, https://attack.mitre.org/. The MITRE ATT&CK® Framework is an overview of the tactics and techniques that could be used to attack IT systems. The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. MITRE has done extensive research under contract for the federal government on cybersecurity issues.

[17]Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack. A phishing attack is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Table 2: Examples of the Most Common and Damaging Types of Cybersecurity Incidents

Types of cybersecurity incidents	Examples
Business email compromise are sophisticated scams carried out by threat actors compromising email accounts through social engineering (e.g., spoofing of a legitimate known email address) or computer intrusion techniques (e.g., malicious software that can gain access to legitimate email threads about billing/invoices) to conduct unauthorized transfer of funds.	• In April 2020, the Federal Bureau of Investigation (FBI) warned the federal government and the health care industry of incidents related to procurement of personal protective equipment, medical equipment, and other equipment in short supply during the COVID-19 pandemic. In particular, the FBI stated that there were multiple incidents in which state government agencies, attempting to procure such equipment, transferred funds to fraudulent brokers and sellers in advance of receiving the items. • Also in April 2020, the FBI issued a public service announcement noting that between January 2014 and October 2019, the agency received complaints totaling more than $2.1 billion in losses from business email compromise scams using two popular email services.
A **data breach** is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information. This information can include personally identifiable information (PII), such as Social Security numbers, or financial information, such as credit card numbers.	• In February 2020, the Department of Justice (DOJ) announced that four members of the Chinese People's Liberation Army were indicted for allegedly hacking into the information technology (IT) systems at Equifax. The indictment stemmed from a July 2017 breach at Equifax that resulted in attackers accessing the personal information of at least 145.5 million individuals. • In December 2018, DOJ announced that two members of the Chinese Ministry of State Security were indicted for global computer intrusion campaigns targeting intellectual property and confidential business information from over 45 technology companies and U.S. government agencies.
A **denial-of-service** attack is one that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A **distributed denial-of-service attack** is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.	• In September 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency warned of denial-of-service and distributed denial-of-service attacks against finance and business organizations worldwide. • In October 2016, a company that facilitates internet traffic was targeted by a massive denial-of-service attack, leaving major websites unavailable to people across the United States. The attack was carried out by the Mirai botnet (i.e., a network of devices infected with malicious software and controlled as a group without the owners' knowledge) that used a short list of common default usernames and passwords to scan the internet for vulnerable devices to infect. As a result, the botnet accessed over 380,000 devices.
Malware, scareware, and viruses are software or code intended to damage or disable computers and computer systems.	• In October 2020, DOJ announced that six officers of the Russian Main Intelligence Directorate (also known as the GRU) were indicted for engaging in computer intrusions and attacks intended to support Russian government efforts. According to the department, these computer attacks used some of the world's most destructive malware to date, including: • Killdisk and Industroyer, which each caused blackouts in Ukraine; • NotPetya, which damaged computers supporting businesses and critical infrastructure worldwide; and • Olympic Destroyer, which disrupted computers supporting the 2018 Olympics.
Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.	• In February 2021, DOJ announced that three North Korean individuals were indicted for, among other things, the creation of the destructive WannaCry ransomware and the extortion and attempted extortion of victim companies from 2017 through 2020. • In May 2019, the Mayor of Baltimore, Maryland, reported that the city was the victim of a ransomware attack. As a result, city employees were not able to access their emails and the attack delayed real estate sales and water billing for months. • In November 2018, DOJ announced that two Iranian individuals were indicted for deploying ransomware to extort hospitals, municipalities, and public institutions, causing more than $30 million in losses to more than 200 victims.

Source: GAO and GAO analysis of documentation from NIST, DHS and DOJ. | GAO-21-288

Recent events highlight the significant cyber threats facing the nation and the range of consequences that these attacks pose.

- In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive and alert explaining that an advanced persistent threat actor had compromised the supply chain of a network management software suite and inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product. The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.[18]

- In February 2021, CISA issued an alert explaining that cyber threat actors obtained unauthorized access to a U.S. water treatment facility's industrial controls systems and attempted to increase the amount of a caustic chemical that is used as part of the water treatment process.[19] According to CISA, threat actors likely accessed systems by exploiting cybersecurity weakness, including poor password security and an outdated operating system.

- In March 2021, CISA issued an emergency directive and alert explaining that CISA's partners had observed active exploitation of vulnerabilities in Microsoft Exchange Server—a product for email inboxes, calendars, and collaboration tools.[20]

GAO Has Previously Identified Four Major Cybersecurity Challenges Facing the Nation

In our September 2018 update to our high-risk series, we identified four major cybersecurity challenges that the federal government and other entities face: (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.[21] To address these challenges, we identified

---

[18]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020); and *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, Alert AA20-352A (Dec. 17, 2020).

[19]CISA, *Compromise of U.S. Water Treatment Facility*, Alert AA21-042A (Feb. 11, 2021).

[20]CISA, *Mitigate Microsoft Exchange Server Vulnerabilities*, Alert AA21-062A (Mar. 3, 2021); and *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021).

[21]GAO-18-622.

10 critical actions that the federal government and other entities need to take (see figure 1).

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-288

Agencies Have Made Progress, but More Work Remains to Fully Address Major Cybersecurity Challenges

Federal agencies have made progress in improving the security of federal and critical infrastructure IT systems, but more work remains to fully address the four cybersecurity challenges facing the nation. For example, since 2010, agencies have implemented more than 2,700 of about 3,300 recommendations that we have made related to the four cybersecurity challenges. Nevertheless, many agencies and critical infrastructure entities continue to face challenges in safeguarding their information systems and information, in part because many of these recommendations had not been implemented. In particular, more than 750 of our recommendations had not been implemented, as of December 2020. We have also designated 103 as priority recommendations, and as of December 2020, 67 had not been implemented. Until our recommendations are implemented and actions are taken to address the four challenges we identified, the federal government's IT systems, the nation's critical infrastructure, and the personal information of U.S. citizens will be increasingly susceptible to the multitude of cyber-related threats that exist.

Agencies Need to Address Four Actions Related to Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government needs to take additional actions to fully establish a comprehensive cybersecurity strategy and perform effective oversight as called for by federal law and policy.[22] To address this challenge, federal agencies need to take the following four actions: (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace, (2) mitigate global supply chain risks, (3) address cybersecurity workforce management challenges, and (4) ensure the security of emerging technologies.

Federal agencies have not implemented many of our recommendations related to establishing a comprehensive cybersecurity strategy and performing effective oversight. Of the roughly 170 recommendations made in our public reports since 2010, about 70 had not been implemented as of December 2020. We have also designated 18 as priority recommendations, and as of December 2020, 14 had not been implemented.

Until our recommendations are implemented, federal agencies may be limited in their ability to provide effective oversight of critical government-wide initiatives, mitigate global supply chain risks, address challenges

---

[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.

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

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.[23] We and the Cyberspace Solarium Commission 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. For example:

- **The federal government needs to address missing elements and lack of clear leadership in the *National Cyber Strategy and Implementation Plan*.** The White House's September 2018 *National Cyber Strategy* and the National Security Council's (NSC) accompanying June 2019 *Implementation Plan* detail the executive branch's approach to managing the nation's cybersecurity. However, in September 2020 we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies.[24] In particular, the *National Cyber Strategy*, when combined with the *Implementation Plan*, addressed three of the six desirable characteristics of national strategies, but lacked certain elements for three other characteristics. Specifically, the documents fully addressed the three desirable characteristics of a national strategy related to defining purpose, specifying organizational roles, and integration and implementation with other documents. However, the documents did not fully address the three desirable characteristics of a national strategy related to problem definition and risk assessment, performance measures, and resources (see table 3).

---

[23]For example, 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.

[24]GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).

Table 3: The Extent to Which the National Cyber Strategy and Implementation Plan Addressed the Desirable Characteristics of a National Strategy

Characteristic	Extent to which the cyber strategy and plan addressed the characteristic
Purpose, scope, and methodology	Addressed
Organizational roles, responsibilities, and coordination	Addressed
Integration and implementation	Addressed
Problem definition and risk assessment	Did not fully address
Goals, subordinate objectives, activities, and performance measures	Did not fully address
Resources, investments, and risk management	Did not fully address

Source: GAO analysis of 2018 National Cyber Strategy and 2019 Implementation Plan. | GAO-21-288

We also reported that the White House identified NSC as the organization responsible for coordinating the implementation of the *National Cyber Strategy*. However, in light of the elimination of the White House Cybersecurity Coordinator position in May 2018, it has remained unclear what official within the executive branch ultimately maintains responsibility for coordinating the execution of the *Implementation Plan* and holding federal agencies accountable for the plan's nearly 200 activities moving forward. NSC staff stated responsibility for duties previously attributed to the White House Cyber Coordinator were passed to the senior director of NSC's Cyber directorate; however, the staff did not provide a description of what those responsibilities include.

We recommended that NSC work with relevant federal entities to update cybersecurity strategy documents to include goals, performance measures, and resource information, among other things. NSC staff neither agreed nor disagreed with our recommendation and has yet to address it. Moving forward, the new administration needs to either update the existing strategy and plan or develop a new comprehensive strategy that addresses those characteristics. In March 2021, the White House released the *Interim National Security Strategic Guidance* to convey the administration's vision for how the nation will interact with the world.[25] The interim guidance highlights cybersecurity as a top priority, noting that the administration aims to strengthen the nation's capability, readiness,

---

[25]The White House, *Interim National Security Strategic Guidance*, (Washington, D.C.: March 2021).

GAO-21-288 High-Risk Series

and resilience in cyberspace. In addition, the interim guidance directs departments and agencies to align their actions with the guidance as work begins on a National Security Strategy.

We also suggested that Congress consider legislation to designate a leadership position in the White House with the commensurate authority to encourage action in support of the nation's cyber critical infrastructure, including the implementation of the *National Cyber Strategy*. In January 2021, Congress enacted a law that established the Office of the National Cyber Director within the Executive Office of the President. The office is to be headed by a Senate-confirmed National Cyber Director and is to be responsible for, among other things, the coordination of cybersecurity policy and operations across the executive branch. Once this position is filled, the White House will be better positioned to (1) ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and (2) coordinate the government's efforts to overcome the nation's cyber-related threats and challenges.[26]

- **The Department of State (State) needs to use data and evidence to justify its proposal to establish the Bureau of Cyberspace Security and Emerging Technologies (CSET) and involve federal agencies as it creates the bureau**. It is also important for the United States to have sufficient leadership in building consensus among international organizations regarding internet standards and cultivating norms for acceptable state behavior in cyberspace. In June 2019, State notified Congress of its intent to establish the CSET that would focus on cyberspace security and the security aspects of emerging technologies. On January 7, 2021, State announced that the Secretary had approved the creation of CSET and directed the department to move forward with establishing the bureau. As of late January 2021, State had not created CSET.

We had reported in September 2020 that State did not involve federal agency partners in its plans to establish this bureau. Officials from six agencies that work with State on cyber diplomacy issues stated that (1) they were unaware of State's plan and (2) if they were informed of State's plan it would be helpful for maintaining and improving

---

[26]Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021), established, within the Executive Office of the President, the Office of the National Cyber Director. The office is to be headed by a National Cyber Director, a presidentially appointed, Senate-confirmed position.

communications with the department.[27] In addition, in January 2021 we reported that State did not demonstrate that it used data and evidence to develop its proposal for establishing CSET.[28]

We recommended that State (1) involve federal agencies that contribute to cyber diplomacy to obtain their views and identify any risks, as it implements its plan to establish CSET, and (2) use data and evidence to justify its proposal to establish CSET.[29] State did not concur with our recommendation to involve other federal agencies, citing that other agencies are not stakeholders in an internal State reform, and that it was unaware that these agencies had consulted with the department before reorganizing their own cyberspace security organizations. We believed our recommendation was warranted and maintained that State's agency partners are key stakeholders, as they work closely with the department on a range of cyber diplomacy efforts.

In addition, while State disagreed with our characterization of its use of data and evidence to develop its proposal for CSET, it agreed that reviewing such information to evaluate program effectiveness can be useful. State commented that it had provided us with appropriate material on its decision to establish CSET and had not experienced challenges in coordinating cyberspace security policy across the department while the CSET proposal had been in discussion. The documents State provided in response to our requests, including a set of briefing slides and an action memo to the Secretary, did not sufficiently demonstrate that it used data and evidence in developing its proposal. In addition, State's comment that it had not experienced

---

[27]GAO, *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau*, GAO-20-607R (Washington, D.C.: Sept. 22, 2020).

[28]GAO, *Cyber Diplomacy: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies*, GAO-21-266R (Washington, D.C.: Jan. 28, 2021).

[29]The Cyberspace Solarium Commission also recommended that the CSET should lead the U.S. government in the following activities to strengthen norms of behavior in cyberspace: (1) prioritize norms against malicious cyber activity targeting elements of critical infrastructure that underpin shared global stability (e.g., the financial services sector); (2) seek to address, where practical, cyberspace policy in venues in which heads of states participate; and (3) expand engagement in international forums in order to reinforce rules that support the U.S. vision for an open, interoperable, reliable, and secure internet. See U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

coordination challenges in recent years was not sufficient evidence that the potential for such challenges did not exist.

- **DHS needs to take actions to ensure organizational changes result in more effective cybersecurity for our nation**. To implement the requirements of the CISA Act of 2018,[30] CISA leadership within DHS launched an organizational transformation initiative. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency.[31] In March 2021, we reported that while CISA had completed the first two of three phases of its organizational transformation initiative, it had not fully implemented its phase three transformation that was intended to completed by December 2020.[32]

We also reported that of 10 selected key practices[33] for effective agency reforms we previously identified, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. Finally, we reported on a number of challenges that selected government and private-sector stakeholders reported on when coordinating with CISA, including a lack of clarity surrounding its organizational changes. Although CISA had activities under way to mitigate some of these challenges, it had not developed strategies to, among other things, clarify changes to its organizational structure.

To address these weaknesses, we made 11 recommendations to DHS. DHS concurred with our recommendations. As of March 2021, DHS had not implemented our recommendations.

Action 2—Mitigate Global Supply Chain Risks

The exploitation of information and communications technology (ICT) products and services through the supply chain is an emerging threat. ICT 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

---

[30]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018).

[31]Pub. L. No. 115-278, § 2(a), 132 Stat. at 4169-74 (codified at 6 U.S.C. § 652).

[32]GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236 (Washington, D.C.: Mar. 10, 2021).

[33]GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C.: June 13, 2018).

disposes of an information system. As a result, the compromise of an agency's ICT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

As previously mentioned, according to CISA, risks related to the compromise of ICT supply chains were realized. Specifically, CISA issued an emergency directive and alert in December 2020 related to a cyberattack campaign that exploited software supply chain weaknesses. According to CISA, an advanced persistent threat actor had been observed leveraging, among other techniques, a software supply chain compromise to conduct a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

Congress and federal agencies have taken several steps aimed at mitigating certain aspects of ICT supply chain risks. For example:

- In December 2018, the Federal Acquisition Supply Chain Security Act of 2018 established the Federal Acquisition Security Council, a cross-agency council responsible for providing direction and guidance to executive agencies to reduce their supply chain risks.[34] As of June 2020, the council had taken steps to address federal requirements related to the management of ICT supply chain risks. For example, according to officials in the Office of Management and Budget's (OMB) Office of the Chief Information Officer, in June 2020, the council finalized a strategic plan for addressing supply chain risks that is intended to, among other things, establish requirements for sharing relevant information about supply chain risks with all federal agencies.

- The John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits executive branch agencies and government contractors from, among other things, obtaining telecommunications

---

[34]Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act)—Title II, Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, Title II, § 202(a), 132 Stat. 5173, 5178 (2018) (codified at 41 U.S.C. § 1322). The law also establishes requirements specifically for the heads of executive agencies. 41 U.S.C. § 1326.

equipment produced by Huawei Technologies Company, ZTE Corporation, or any of their subsidiaries or affiliates.[35]

- In May 2019, the Department of Commerce (Commerce) added Huawei and certain non-U.S. affiliates to the Entity List[36] (with additional affiliates added in August 2019 and August 2020) as entities who may have engaged in activities that are contrary to U.S. national security or foreign policy interests.

- Also in May 2019, the President issued an executive order prohibiting transactions involving ICT and services provided by foreign adversaries or their agents, and which pose an undue risk to critical infrastructure or to U.S. national security.[37]

- In 2020, the Federal Communications Commission (FCC) published a final rule in response to ongoing concerns about the integrity of the communications supply chain.[38] The rule prohibits the use of money from the Universal Service Fund to purchase or obtain equipment or services from any communications equipment or service provider identified by the FCC's Public Safety and Homeland Security Bureau as posing a national security risk to communications networks or the communications supply chain, such as Huawei Technologies Company and ZTE Corporation.[39]

---

[35]The John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits executive branch agencies and government contractors from procuring, obtaining, extending, or renewing a contract to procure or obtain, any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. Pub. L. No. 115-232, § 889(a)(1)(A), 134 Stat. at 1917. The act defines "covered telecommunications equipment or services" to include telecommunications equipment produced by Huawei Technologies Company (Huawei), ZTE Corporation, or any of their subsidiaries or affiliates. Pub. L. No. 115-232, § 889(f)(3)(A), 134 Stat. at 1918.

[36]The Entity List can be found at Supplement No. 4 to Part 744 of the Export Administration Regulations.

[37]The White House, *Securing the Information and Communications Technology and Services Supply Chain*, Executive Order 13873 (Washington, D.C.: May 15, 2019).

[38]See 47 C.F.R. § 54.9 (2020).

[39]To support broadband deployment in unserved areas, FCC provided billions through the Universal Service Fund's high-cost program to telecommunications carriers that offer broadband and voice services in areas that are costly to serve. These areas are typically rural or remote and increase carriers' infrastructure costs due to challenges, such as difficult terrain and longer distances between consumers. These areas also often have fewer consumers overall, further limiting carriers' abilities to offset infrastructure costs with end-user revenue.

- The Secure and Trusted Communications Networks Act of 2019 was signed into law in March 2020 and prohibits the use of certain federal funds to obtain communications equipment or services from a company that poses a national security risk to U.S. communications networks.[40]

- In February 2021, the President issued an executive order requiring the Secretaries of Commerce and Homeland Security to submit a report by February 2022 on supply chains for critical sectors and subsectors of the ICT industrial base and for that report to review, among others, cyber risks that could compromise the supply chain.[41]

Nevertheless, we have previously reported that agencies have not effectively managed supply chain risks. In particular:

- **Agencies need to implement effective supply chain risk management practices.** In December 2020, we reported that few of the 23 civilian Chief Financial Officers (CFO) Act of 1990 agencies[42] implemented foundational practices for managing ICT supply chain risks.[43] In that report, we identified the seven practices from the National Institute of Standards and Technology's (NIST) guidance that are foundational for an organization-wide approach to ICT supply chain risk management (SCRM).[44] However, we found that none of the 23 agencies fully implemented all of the supply chain risk

---

[40]Pub. L. No. 116-124, § 3, 134 Stat. 158, 159 (2020).

[41]The White House, *America's Supply Chains*, Executive Order 14017 (Washington, D.C.: Feb. 24, 2021).
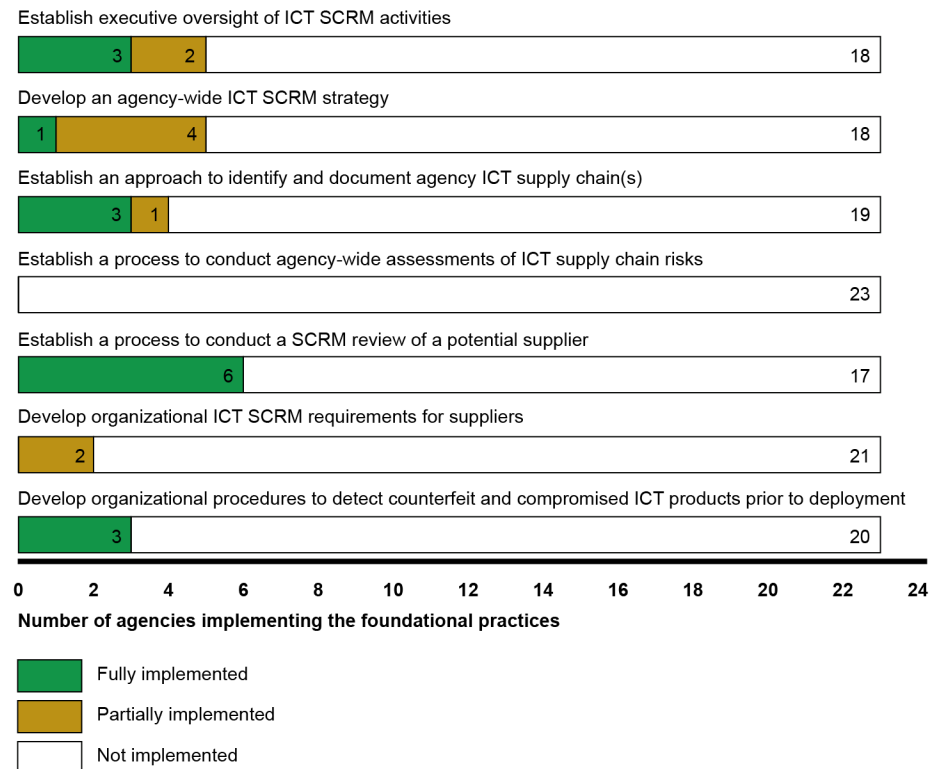
[42]The 23 civilian CFO Act agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; 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. There are 24 CFO Act agencies. We did not include the Department of Defense because our scope was the civilian agencies.

[43]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[44]See NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (Apr. 16, 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Gaithersburg, Md.: Apr. 2015); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018); and *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: Mar. 2011).

management practices and 14 of the 23 agencies had not implemented any of the practices (see figure 2).

Figure 2: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Practices

Establish executive oversight of ICT SCRM activities

| 3 | 2 | 18 |

Develop an agency-wide ICT SCRM strategy

| 1 | 4 | 18 |

Establish an approach to identify and document agency ICT supply chain(s)

| 3 | 1 | 19 |

Establish a process to conduct agency-wide assessments of ICT supply chain risks

| 23 |

Establish a process to conduct a SCRM review of a potential supplier

| 6 | 17 |

Develop organizational ICT SCRM requirements for suppliers

| 2 | 21 |

Develop organizational procedures to detect counterfeit and compromised ICT products prior to deployment

| 3 | 20 |

0 2 4 6 8 10 12 14 16 18 20 22 24

Number of agencies implementing the foundational practices

■ Fully implemented
■ Partially implemented
□ Not implemented

Source: GAO analysis of agency data. | GAO-21-288

In a sensitive report issued in October 2020, we made 145 recommendations to the 23 agencies to fully implement foundational practices in their organization-wide approaches to ICT SCRM.[45] Of the 23 agencies, 17 agreed with all of the recommendations made to them; two agencies agreed with most, but not all of the recommendations; one agency disagreed with all of the recommendations; two agencies neither agreed nor disagreed with the recommendations, but stated they would address them; and one agency had no comments. We believed that all of the

---

[45]GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: Oct. 27, 2020).

recommendations were warranted, as discussed in the sensitive report.

We have also previously reported on supply chain ICT risks to critical infrastructure sectors. For example:

- **Administration officials need to ensure that the national strategy to secure 5G networks fully addresses key characteristics needed for a national strategy.** As discussed in more detail later in this report, 5G wireless networks promise to provide significantly greater speeds and higher capacity to accommodate more devices. However, in November 2020, we reported that the global reach of the 5G supply chain, as well as the technological complexity of the components of 5G technologies, presented the risk that components from suppliers whose quality and security could not be fully guaranteed may be used in 5G networks.[46] According to an April 2019 Defense Innovation Board report, a compromised supply chain posed a serious threat to national security by introducing vulnerabilities into networks and systems.[47]

  In March 2020, the White House issued the *National Strategy to Secure 5G of the United States of America* (5G national strategy), as required by the Secure 5G and Beyond Act of 2020.[48] The strategy is intended to provide direction on how the U.S. government will secure 5G infrastructure domestically and abroad from risks, including supply chain risks. However, in October 2020, we reported that the strategy partially addressed five of the six characteristics that are desirable for a national strategy.[49] We made one recommendation to NSC to ensure that the plan to implement the 5G national strategy fully addresses all elements of our six desirable characteristics of a national strategy. NSC had no comments on our draft report.

- **The Federal Aviation Administration (FAA) needs to prioritize oversight of cybersecurity risks facing avionics, including supply chain risks.** Modern airplanes are equipped with networks and systems that share data with the pilots, passengers, maintenance

---

[46]GAO, *5G Wireless: Capabilities and Challenges for an Evolving Network,* GAO-21-26SP (Washington, D.C.: November 2020).
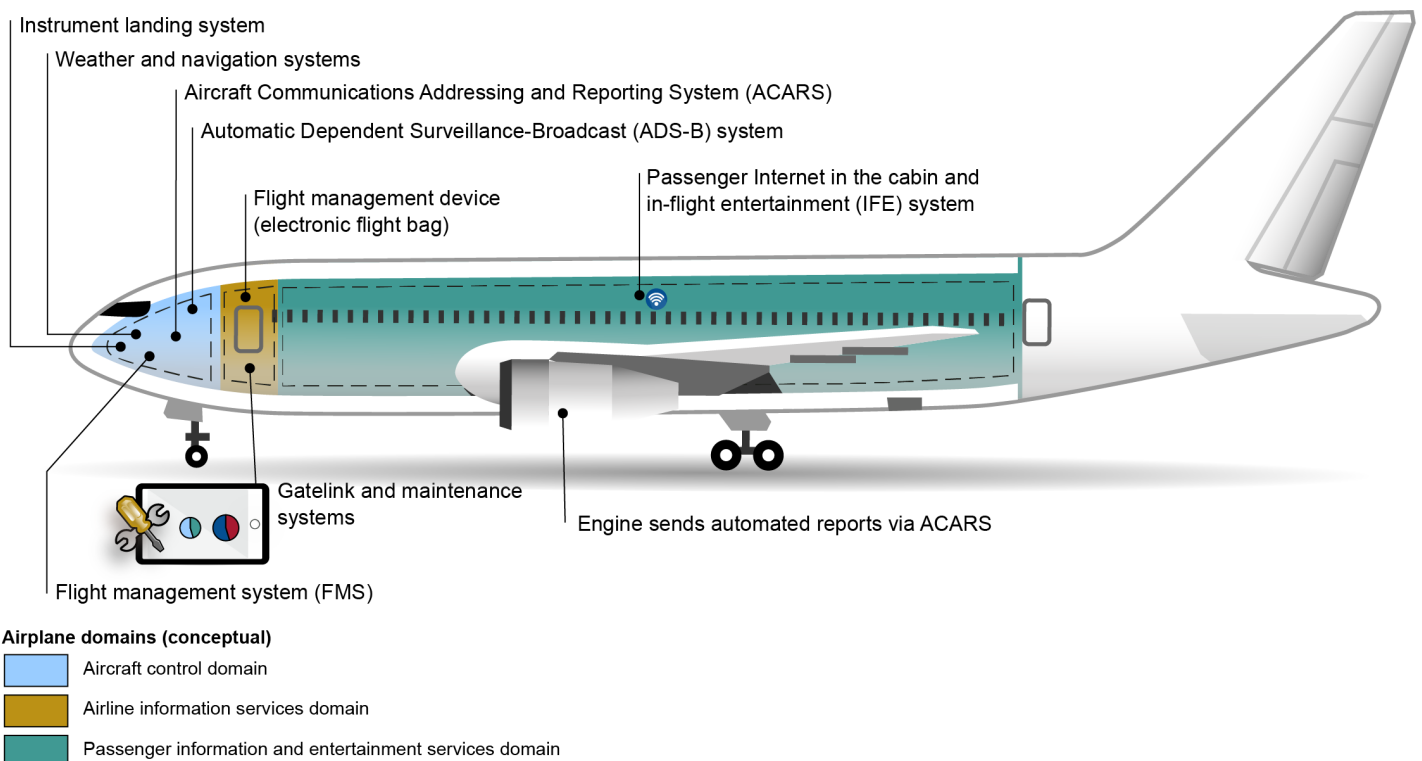
[47]Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities for DOD* (Washington, D.C.: April 2019).

[48]Pub. L. No. 116-129, § 3, 134 Stat. 223 (2020).

[49]GAO, *National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy,* GAO-21-155R (Washington, D.C.: Oct. 7, 2020).

GAO-21-288 High-Risk Series

crews, other aircraft, and air-traffic controllers in ways that were not previously feasible (see figure 3).

Figure 3: Key Systems Connections to Commercial Airplanes

Instrument landing system

Weather and navigation systems

Aircraft Communications Addressing and Reporting System (ACARS)

Automatic Dependent Surveillance-Broadcast (ADS-B) system

Flight management device (electronic flight bag)

Passenger Internet in the cabin and in-flight entertainment (IFE) system

Gatelink and maintenance systems

Engine sends automated reports via ACARS

Flight management system (FMS)

Airplane domains (conceptual)

Aircraft control domain

Airline information services domain

Passenger information and entertainment services domain

Source: GAO analysis of Federal Aviation Administration and industry documentation. | GAO-21-288

In October 2020, we reported that vulnerabilities can be introduced to avionics systems at multiple points within an insecure supply chain. To date, extensive cybersecurity controls have been implemented and there have not been any reports of successful cyberattacks on an airplane's avionics systems. However, the increasing connections between airplanes and other systems, combined with the evolving cyber threat landscape, could lead to increasing risks for future flight safety.[50] In particular, vulnerabilities in avionics systems could potentially result in a range of impacts, from allowing an adversary to take control of a system to decreasing the availability of materials

[50]GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks,* GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

needed to develop a system. For example, airplanes feature electronic hardware components known as line replaceable units,[51] which, if compromised, could adversely affect flight operations. As discussed in more detail later in this report, while FAA recognized avionics cybersecurity as a potential safety issue for modern commercial airplanes, it had not fully implemented key practices that are necessary to carry out a risk-based cybersecurity oversight program.

- **The Federal Energy Regulatory Commission (FERC) should fully address supply chain risks in its approved standards for electric grid entities.** In August 2019,[52] we reported that FERC[53] approved a new standard in October 2018 to bolster supply chain risk management protections for the nation's bulk power system.[54] However, we found that this and other FERC-approved cybersecurity standards partially addressed NIST's guidance for improving critical infrastructure cybersecurity. In particular, the standards fully addressed associated subcategories for establishing supply chain risk management processes, security measures in contracts with suppliers and third party partners, and evaluations of suppliers and third-party partners to ensure they meet their contractual obligations. However, the standards did not address subcategories for response and recovery planning and testing with suppliers and third-party providers, and for using the supply chain risk management process to identify, prioritize, and assess suppliers and third-party partners.

  We recommended, among other things, that FERC consider adopting changes to its approved cybersecurity standards to more fully address the NIST guidance. FERC agreed with, and has begun to take steps

---

[51]A line replaceable unit is a modular component of an airplane that is designed to be replaced quickly during maintenance activities to minimize downtime and restore a system to operational readiness.

[52]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid,* GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[53]FERC is the regulator for the interstate transmission of electricity with responsibility to review and approve standards for the reliable operation of the bulk power system.

[54]The term "bulk power system" refers to (1) facilities and control systems necessary for operating the interconnected electric transmission network and (2) the output from certain generation facilities needed for reliability. FERC oversees the North American Electric Reliability Corporation, the federally designated U.S. electric reliability organization responsible for conducting reliability assessments and developing and enforcing mandatory standards to provide for reliable operation of the bulk power system.

to implement, this recommendation. Specifically, in June 2020, FERC issued a Notice of Inquiry seeking comments on whether the North American Electric Reliability Corporation's cybersecurity standards adequately address NIST's guidance. However, as of December 2020, our recommendation had not been fully implemented.

The Cyberspace Solarium Commission has also made recommendations related to the challenge of mitigating supply chain risks.[55] For example:

- Congress should direct the U.S. government to develop and implement an ICT industrial base strategy to ensure more trusted supply chains.

- Congress should appropriate consistent funding and task the executive branch to develop and implement research and development priorities in emerging technologies

- Congress and the executive branch should identify and appropriate the funds necessary to achieve the goals of the Cyber Moonshot Initiative.[56]

- The Supply Chain and Counterintelligence Risk Management Task Force within the Office of the Director of National Intelligence (ODNI) should explore additional avenues to expand its support to critical infrastructure.

- The executive branch should strengthen the capacity of the Committee on Foreign Investment in the United States.

Action 3—Address Cybersecurity Workforce Management Challenges

Cybersecurity professionals can help to prevent or mitigate the vulnerabilities that could allow malicious individuals and groups access to federal IT systems. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that uses, implements, secures, and maintains these systems. As a result, a resilient, well-trained, and dedicated cybersecurity workforce is essential to protecting federal IT systems. Nevertheless, OMB and our prior reports

[55]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[56]In 2018, the President's National Security Telecommunications Advisory Committee called for a "moonshot" initiative to address the action needed to address the "progressively worsening cybersecurity threat environment" facing our public safety, economic prosperity, and national security. The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on a Cybersecurity Moonshot* (Nov. 14, 2018).

have pointed out that the federal government and private industry face a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats.

OMB and the Department of Homeland Security (DHS) have several initiatives under way that can assist agencies in meeting challenges related to hiring and retaining cybersecurity personnel. For example:

- In August 2017, the National Initiative for Cybersecurity Education (NICE),[57] led by NIST, created the NICE Cybersecurity Workforce Framework for defining cybersecurity workforce positions to help the federal government better identify cybersecurity workforce needs by enabling agencies to examine specific cybersecurity work roles and identify personnel skills gaps.

- The National Initiative for Cybersecurity Careers and Studies is an online resource for cybersecurity training managed by DHS that connects government employees, students, educators, and industry with cybersecurity training providers throughout the nation.[58] The initiative's Federal Virtual Training Environment, for example, is an on-demand cybersecurity training system that contains more than 800 hours of training on a variety of topics.

However, federal agencies continue to face challenges in addressing needs related to their cyber workforce. For example:

- **OMB and DHS need to take action to address the cybersecurity workforce shortage**. In June 2018, the prior administration released its government-wide reform plan, which included 32 proposals aimed at achieving improvements in, among other things, solving the cybersecurity workforce shortage. In April 2020, we reported that OMB and DHS partially addressed most of the leading practices associated with effective reforms through their efforts to address the cybersecurity workforce shortage, such as reskilling employees to fill

---

[57]NICE, led by NIST, is a partnership among government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals that are helping to keep our nation secure.

[58]https://niccs.us-cert.gov/about-niccs/niccs.

vacant cybersecurity positions and streamlining hiring processes.[59] However, we found that OMB and DHS had not established a dedicated implementation team or a government-wide implementation plan, among other practices.

We made seven recommendations to OMB, including to follow certain key practices to help solve the cybersecurity workforce shortage. OMB did not provide comments on the report. As of December 2020, all seven recommendations had not been implemented.

- **Agencies need to fully implement key workforce planning activities.** In October 2019, we reported that the 24 CFO Act agencies we reviewed varied widely in their efforts to implement key IT workforce planning activities that are critical to ensuring that agencies have the staff they need to support their missions.[60] For example, nearly all of the agencies had partially implemented, substantially implemented, or fully implemented three of the workforce planning activities (develop competency and staffing requirements, assess competency and staffing needs regularly, and assess gaps in competencies and staffing). However, most agencies had minimally implemented or did not implement the five other workforce planning activities (including efforts to establish a workforce planning process and address staffing gaps). Figure 4 shows the agencies' overall implementation of each of the eight key IT workforce planning activities, as of May 2019.
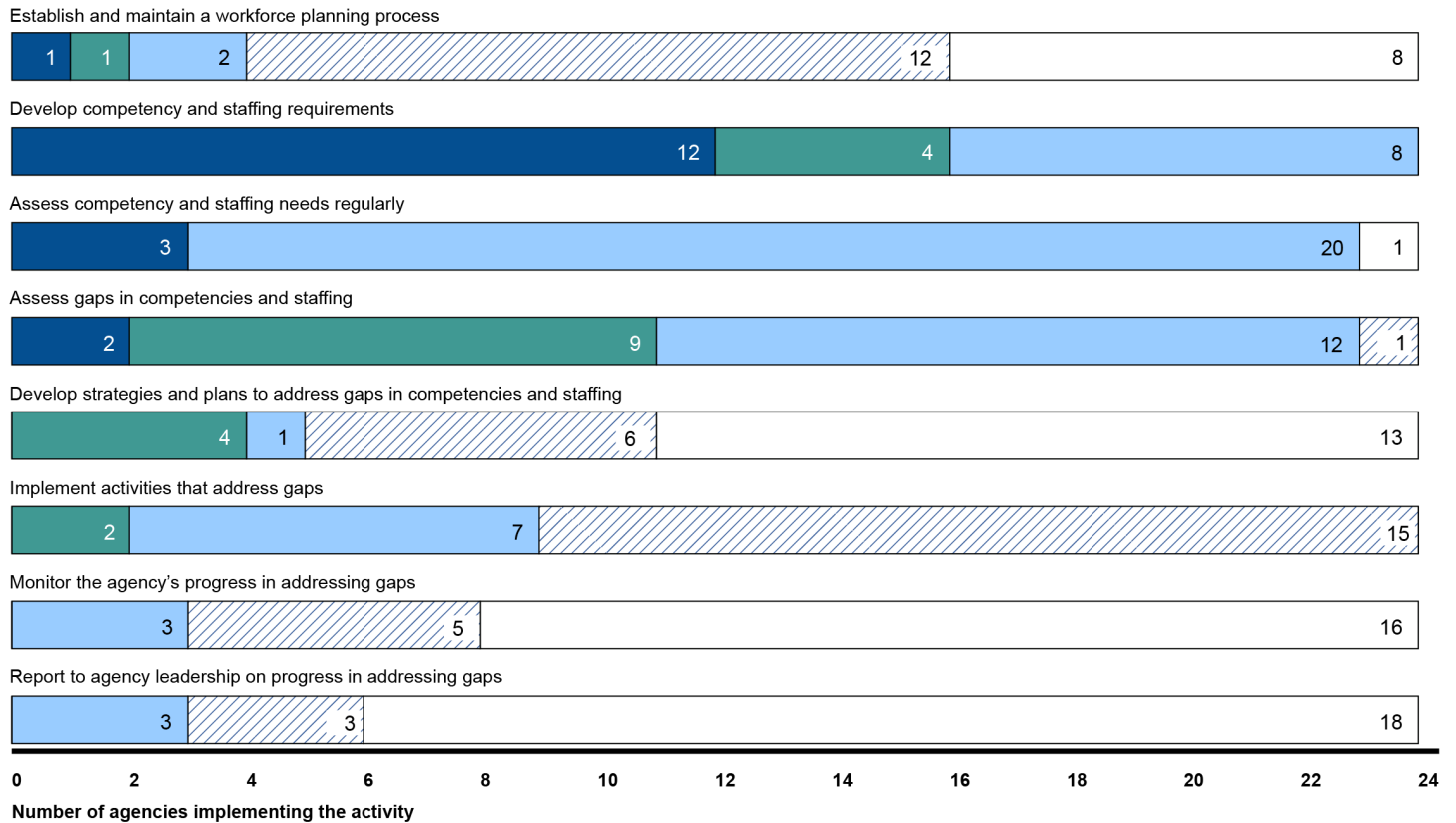
[59]GAO, *Federal Management: Selected Reforms Could Be Strengthened By Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: Apr. 23, 2020).

[60]GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities,* GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

Figure 4: The 24 Chief Financial Officers Act Agencies' Overall Implementation of Each of the Eight Key Information Technology Workforce Planning Activities

Establish and maintain a workforce planning process
| 1 | 1 | 2 | 12 | 8 |

Develop competency and staffing requirements
| 12 | 4 | 8 |

Assess competency and staffing needs regularly
| 3 | 20 | 1 |

Assess gaps in competencies and staffing
| 2 | 9 | 12 | 1 |

Develop strategies and plans to address gaps in competencies and staffing
| 4 | 1 | 6 | 13 |

Implement activities that address gaps
| 2 | 7 | 15 |

Monitor the agency's progress in addressing gaps
| 3 | 5 | 16 |

Report to agency leadership on progress in addressing gaps
| 3 | 3 | 18 |

0   2   4   6   8   10   12   14   16   18   20   22   24

Number of agencies implementing the activity

■ Fully implemented—the agency fully implemented both of an activity's evaluation criteria.

■ Substantially implemented—the agency fully implemented one of an activity's evaluation criteria and partially implemented the other evaluation criteria.

■ Partially implemented—the agency fully implemented one of an activity's evaluation criteria and did not implement the other criteria, or partially implemented both of an activity's evaluation criteria.

▨ Minimally implemented—the agency partially implemented one of an activity's evaluation criteria and did not implement the other evaluation criteria.

□ Not implemented—the agency did not implement either of an activity's evaluation criteria.

Source: GAO analysis of agency information technology workforce planning policies and documentation. | GAO-21-288

Accordingly, we made recommendations to 18 of the 24 federal agencies to fully implement the eight key IT workforce planning activities. Agency responses to the recommendations varied, and as of December 2020, the recommendations had not been implemented.

- **Federal agencies should review cybersecurity positions and categorize them appropriately to effectively identify critical staffing needs.** In March 2019, we reported that most of the 24 CFO

Act agencies had likely miscategorized the work roles of many IT and cybersecurity positions.[61] For example, at least 22 of the 24 agencies designated positions as not performing IT, cybersecurity, or cyber-related functions, when they did most likely perform these functions. In addition, the six agencies that we selected for additional review had assigned work role codes that were not consistent with the work roles and duties described in corresponding position descriptions for 63 of 120 positions in the IT occupational series (see figure 5).

Figure 5: Consistency of Assigned Work Role Codes with Position Descriptions for Random Sample of Information Technology Positions within the 2210 Occupational Series at Six Selected Agencies

Number of positions

Code **consistent** with position description

Code **inconsistent** with position description

Position description **incomplete or not provided**
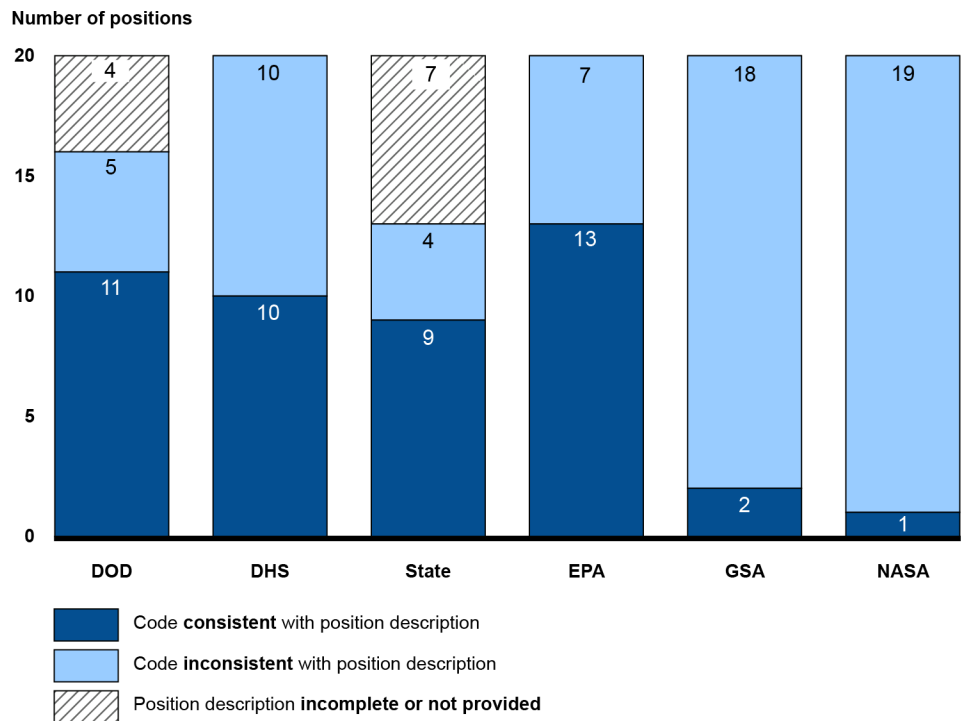
DOD (Department of Defense), DHS (Department of Homeland Security), State (Department of State), EPA (Environmental Protection Agency), GSA (General Services Administration), NASA (National Aeronautics and Space Administration)

Source: GAO analysis of DOD, DHS, State, NASA, EPA and GSA cybersecurity coding data. | GAO-21-288

We made 28 recommendations to 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related

---

[61]GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

positions. Twenty agencies agreed with the recommendations, one partially agreed, and one did not agree with one of two recommendations. We maintained our recommendations were warranted, and as of January 2021, 12 of our recommendations had not been implemented.

The Cyberspace Solarium Commission has also made recommendations related to cybersecurity workforce management challenges,[62] including the following:

- Congress and the executive branch should pass legislation and implement policies designed to better recruit, develop, and retain cyber talent while acting to deepen and diversify the pool of candidates for cyber work in the federal government.

- The U.S. government should take a number of actions to improve cyber-oriented education, such as further exploring ways to expand federal cyber training programs.

Action 4—Ensure the Security of Emerging Technologies

The emergence of new technologies can potentially introduce security vulnerabilities for those technologies which were previously unknown. As we and the Cyberspace Solarium Commission 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),[63] 5G networks, artificial intelligence (AI),[64] and quantum computing,[65] there is still much work to be done.

---

[62]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[63]IoT is generally defined as the concept of connecting and interacting through a network with a broad array of "smart" devices, such as building energy management systems, thermostats, or electric vehicle charging stations.

[64]The field of AI was founded on the idea that algorithms could be developed to simulate human intelligence. AI includes both narrow applications designed for task completion (like online "chatbots" or virtual assistants) and general systems that reason like a human across a range of contexts (such as self-driving cars).

[65]Quantum technologies build on the study of the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies. For example, Quantum computers could dramatically accelerate computation for some applications, such as decrypting information.

- **Additional action is needed to address IoT cybersecurity risks at federal agencies.** 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. IoT "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and respond automatically to improve industrial processes, public services, and the well-being of individual consumers.[66] However, this emerging technology also presents new issues in areas such as cybersecurity. The rapid and pervasive adoption of IoT devices, the lack of attention in designing them to be secure, and the predominant use of cloud computing to provide connectivity with these devices pose unique cybersecurity challenges that may limit broader adoption of the IoT.[67]

  Federal agencies have identified IoT cybersecurity challenges, but more needs to be done to address them. In August 2020, we reviewed federal agencies' responses to our survey on the federal government's experience with IoT and reported that agencies identified improvements in data collection, operational efficiency and productivity, and automated program and services as areas that benefited from IoT technologies.[68] However, some agencies told us that they chose not to adopt IoT technologies due to cybersecurity concerns. In particular, in our survey of federal agencies, cybersecurity was the most frequently cited challenge (43 of 74).[69] Selected agencies we spoke with identified specific cybersecurity challenges, including the National Aeronautics and Space Administration, which identified a series of challenges related to IoT

---

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

[67]As defined by NIST, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released.

[68]GAO, *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020).

[69]The levels of challenge survey that respondents had to choose from were "very challenging," "somewhat challenging," "slightly challenging," "not at all challenging," "do not know," and "not applicable." For the purpose of ranking challenges, we summed the number of responses for "very challenging" and "somewhat challenging."

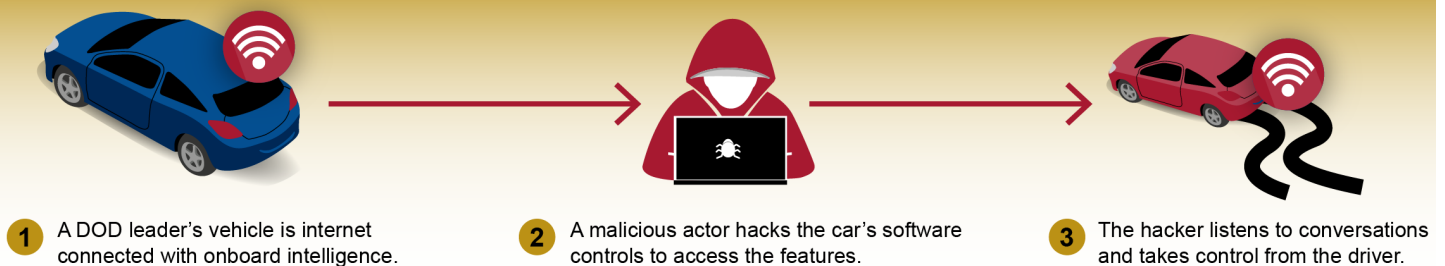and reported that cybersecurity was the most significant of these challenges.[70]

As another example, in July 2017 we reported that IoT devices, such as those acquired and used by the Department of Defense (DOD) employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department.[71] The department has also identified notional threat scenarios, based on input from multiple DOD entities, which exemplify how these security risks could adversely impact its operations, equipment, or personnel (see figure 6).

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

Operations security and intelligence collection

1. A smart television is in an unsecure area and connected to a provider.
2. An employee from the provider uses the television to record conversations and take pictures.
3. An adversary accesses personal phones through the television to collect intelligence.

Endangerment of leadership

1. A DOD leader's vehicle is internet connected with onboard intelligence.
2. A malicious actor hacks the car's software controls to access the features.
3. The hacker listens to conversations and takes control from the driver.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-288

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

---

[70]National Aeronautics and Space Administration, *IoT Phase III White Paper* (2018).

[71]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).

address these issues, we made two recommendations to DOD. The department agreed with our recommendations; however, the recommendations had not been implemented.

In response to these cybersecurity challenges related to IoT, in December 2020, the IoT Cybersecurity Improvement Act of 2020 was enacted to establish standards and guidelines for the appropriate use of federal government IoT devices, including minimum information security requirements for managing cybersecurity risks associated with such devices.[72] In particular, among other things, the law requires NIST to develop and publish the standards and guidelines while OMB is responsible for issuing policies and principles as necessary to ensure that agency policies and principles are consistent with the NIST standards.

The Cyberspace Solarium Commission has also highlighted the cybersecurity challenges related to IoT. In particular, the commission recommended that Congress direct and appropriate funds for federal agencies to create or designate critical technology security centers to provide the government with the capacity to test the security of critical technologies—including IoT.[73]

- **The federal government's 5G national strategy implementation plan needs to address all elements of our desirable characteristics of a national strategy.** 5G networks are expected to enable significantly higher data rates, massive increases in the number of connected devices, faster network response, and greater reliability, among other advancements than the existing fourth generation (4G)/"Long Term Evolution" (LTE) cellular networks. Figure 7 compares 4G and 5G performance goals across key performance measures.

---

[72]Pub. L. No. 116-207, § 4, 134 Stat. 1001, 1002 (2020).

[73]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

GAO-21-288 High-Risk Series

Figure 7: 5G Performance Goals Compared to 4G/LTE across Three Performance Measures

	100 Mbps	1 ms	1 million devices/km²
	User experienced data rate	Latency	Connection density
5G / 4G	10 Megabits per second (Mbps)	10 milliseconds (ms)	100,000 devices/km2 (square kilometer)
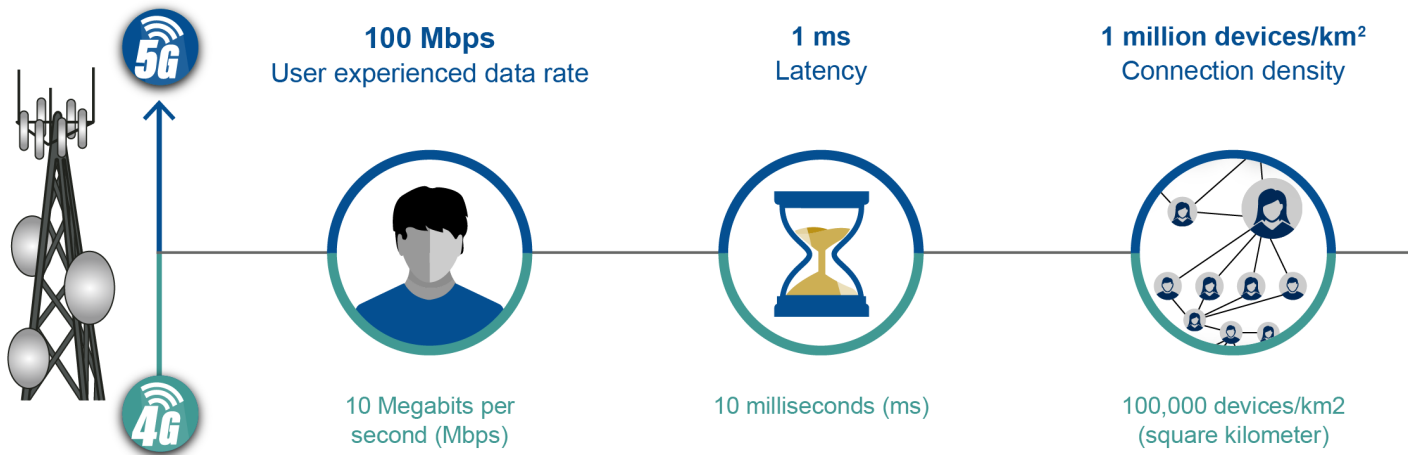
Source: GAO depiction of International Telecommunication Union data. | GAO-21-288

Note: Megabits per second (Mbps) is a measure of the rate at which data is transmitted, milliseconds (ms) is a measure of time equal to one thousandth of a second, and square kilometer (km²) is a measure of area.

While 5G has the potential to greatly improve mobile communication, 5G networks can also introduce cybersecurity challenges. For example, in their specifications for 5G, the 3rd Generation Partnership Project, the international partnership project that develops specifications, included security enhancements that could address some existing 4G/LTE vulnerabilities. However, most of these enhancements will only be realized when standalone 5G, which relies exclusively on 5G equipment, is deployed on a large scale, which may take a decade. Moreover, the 3rd Generation Partnership Project security enhancements are not activated by default; some are optional for carriers to implement.

Our prior work has identified potential solutions to address these cybersecurity risks and challenges presented by 5G networks. For example, in our November 2020 report, we described policy options related to cyber risks that lawmakers and agencies could consider adopting to address these risks.[74] These options included supporting nationwide, coordinated cybersecurity monitoring of 5G networks, and adopting cybersecurity requirements for 5G networks.

---

[74]GAO-21-26SP.

In March 2020, the White House issued the 5G national strategy to provide direction on how the U.S. government will secure 5G infrastructure domestically and abroad. However, we reported in October 2020 that the 5G national strategy did not fully address all of the characteristics, such as having information about expected cost and the types of resources and investments needed, as summarized in table 4.[75]

---

[75]GAO-21-155R.

Table 4: Extent to Which the March 2020 National Strategy to Secure 5G (5G National Strategy) Addressed the Desirable Characteristics of a National Strategy

Desirable characteristic	Elements of the desirable characteristic that should be addressed in a national strategy	Our assessment of the 5G national strategy against the elements of the desirable characteristics
Purpose, scope, and methodology	Why the strategy was produced, the scope of its coverage, and the process by which it was developed	Partially addressed
Problem definition and risk assessment	The particular national problems, assesses the risks to critical assets and operations—including the threats to, and vulnerabilities of, critical operations—and discusses the quality of data available regarding the risk assessment	Partially addressed
Goals, subordinate objectives, activities, and performance measures	What the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability	Partially addressed
Results, investments, and risk management	What the strategy will cost and the types of resources and investments needed	Did not address
Organizational roles, responsibilities, and coordination	Who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts	Partially addressed
Integration and implementation	How a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy	Partially addressed

Source: GAO analysis of the 5G strategy. | GAO-21-288

Note: In GAO-04-408T, we reported that national strategies are not required to include a single, consistent set of characteristics, and they contain varying degrees of detail based on their different scopes. In line with the methodology described in GAO-04-408T, we consider the national strategy to fully address a characteristic if it explicitly includes all elements of that characteristic. We consider it to partially address a characteristic if it includes some, but not all elements of a characteristic, and it does not address a characteristic if it includes none of these elements. GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

To address these issues, we made one recommendation to NSC to ensure that the plan to implement the 5G national strategy fully addresses all elements of our six desirable characteristics of a national strategy. NSC had no comments on our draft report.

- **AI automated systems are susceptible to cybersecurity risks.** AI was founded on the idea that algorithms could be developed to simulate human intelligence. In cybersecurity, although AI holds substantial opportunity in a variety of capacities, the use of AI also poses unique challenges. For example, AI automated systems and algorithms can help identify and patch vulnerabilities and defend against attacks. Automating computer network defense offers many potential gains in terms of efficiency and effectiveness.

However, automated systems themselves are susceptible to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly identify. These threats are amplified by the ongoing delegation of decision making, sensing, and authentication roles to potentially vulnerable automated systems. Moreover, broader deployment could become riskier as the reliance on autonomous decision-making increases.

In March 2018, we reported on the results of a forum we convened to discuss emerging opportunities, challenges, and implications associated with AI.[76] 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 AI. For example, if the data used by AI are biased or become corrupted by hackers, the results could be biased or cause harm.

As AI technologies continue to advance at an incredible speed, federal oversight considerations need to evolve alongside them. Both the prior administration and the Congress took steps in this direction. For example, the prior administration's national AI strategy discussed, among other things, the need for additional research and development, including for mitigating cyber risks of certain AI techniques.[77] Also, provisions in a recently enacted law, such as the creation of a government-wide National AI Initiative,[78] provide avenues for increased focus on the challenges and opportunities presented by AI.

---

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

[77]National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (June 2019).

[78]National Artificial Intelligence Initiative Act of 2020, Pub. L. No. 116-283, div. E, 134 Stat. at 4523.

In March 2021, the National Security Commission on Artificial Intelligence[79] issued its final report in which the commission described additional cybersecurity risks associated with AI and recommendations to address them.[80] Specifically, the commission stated that AI will enable malware to mutate into thousands of different forms, find vulnerabilities, and attack selectively. The commission added that the expanding application of AI cyber capabilities will make cyberattacks more precise and tailored; further accelerate and automate cyber warfare; enable stealthier and more persistent cyber weapons; and make cyber campaigns more effective on a larger scale.

To address these threats, the commission's final report contains the following recommendations:

- Congress must continue implementing the Cyberspace Solarium Commission's recommendations, such as the establishment of a Joint Cyber Planning and Operations Center to serve as a centralized cyber intelligence sharing and collaboration unit.

- National security agencies need to acquire the sensors and instrumentation needed to train AI systems to detect and respond to threats on their networks.

- Government agencies should create a framework to address how key AI systems could be attacked and should be defended.

- DOD and the ODNI should consider establishing government-wide communities of AI red teaming capabilities.[81]

- **Quantum computing has the potential to create major cybersecurity risks.** Quantum technologies build on the study of the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies. Quantum computers are available with dozens of the fundamental components known as physical qubits, although a general use

---

[79]Section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the National Security Commission on Artificial Intelligence as an independent commission to consider the methods and means necessary to advance the development of AI, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States. Pub. L. No. 115-232, § 1051, 132 Stat. at 1962.

[80]National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

[81]According to NIST, a red team exercise is a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems under real-world conditions.

quantum computer may need more than 100,000 physical qubits. As we reported in May 2020, a full-scale quantum computer has the potential to break standard encryption technologies, creating a major information security risk.[82] The cybersecurity infrastructure will need to evolve to create quantum-proof encryption and protect existing information.

The Cyberspace Solarium Commission has also highlighted the cybersecurity challenges related to quantum computing. In particular, the commission recommended that Congress should require DOD to comprehensively assess the threats and risks posed by quantum computing to national security systems and develop a plan to secure those systems. Subsequently, in January 2021, Congress enacted a law that called for the department to prepare such an assessment and to develop recommendations for research, development, and acquisition activities for securing critical national security systems against threats to quantum computing.[83]

Agencies Need to Address Three Actions on Securing Federal Systems and Information

The federal government has been challenged in securing federal systems and information. To address this challenge, federal agencies need to improve the implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents.

However, federal agencies have not addressed many of our recommendations related to establishing secure federal systems and information. We have made almost 600 recommendations in public reports since 2010 and about 150 had not been implemented as of December 2020. Further, we have also designated 62 as priority recommendations, and as of December 2020, 41 had not been implemented. Until our recommendations are fully implemented, federal agencies may be limited in their ability to improve the implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents.

---

[82]GAO, *Science & Tech Spotlight: Quantum Technologies*, GAO-20-527SP (Washington, D.C.: May 28, 2020).

[83]Pub. L. Nol. 116-283, § 1722, 134 Stat. at 4109.

Action 5—Improve
Implementation of
Government-Wide
Cybersecurity Initiatives

Federal agencies face cyber threats that continue to grow in number and sophistication. To protect against cyber threats, federal law and policies give DHS and OMB broad authorities to improve and promote the cybersecurity of federal networks. Although DHS and OMB have established and made important progress in implementing government-wide initiatives aimed at helping to protect against cyber threats, the agencies need to take additional actions to ensure that these initiatives are effectively implemented and widely adopted on federal networks. For example:

- **DHS and selected agencies need to address shortcomings in the implementation of its network monitoring program.** The Continuous Diagnostics and Mitigation (CDM) program was established to provide federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels.[84] As depicted in figure 8, the program relies on automated tools to identify hardware and software residing on agency networks.

---

[84]DHS developed and made available the CDM program to strengthen the cybersecurity of government networks and systems by providing tools and services to agencies to support continuous monitoring of their networks. The CDM program uses hardware and software products (also referred to as tools) that have been installed on an agency's network. These tools automate the detection of hardware and software present on a network. The CDM program includes capabilities intended to help agencies identify cybersecurity risks on an ongoing basis, use CDM information to prioritize the risks based on potential impacts, and then mitigate the most significant vulnerabilities first. Each capability relies on several underlying tools.

Figure 8: Continuous Diagnostics and Mitigation Program Data Flow from Agencies to the Federal Dashboard
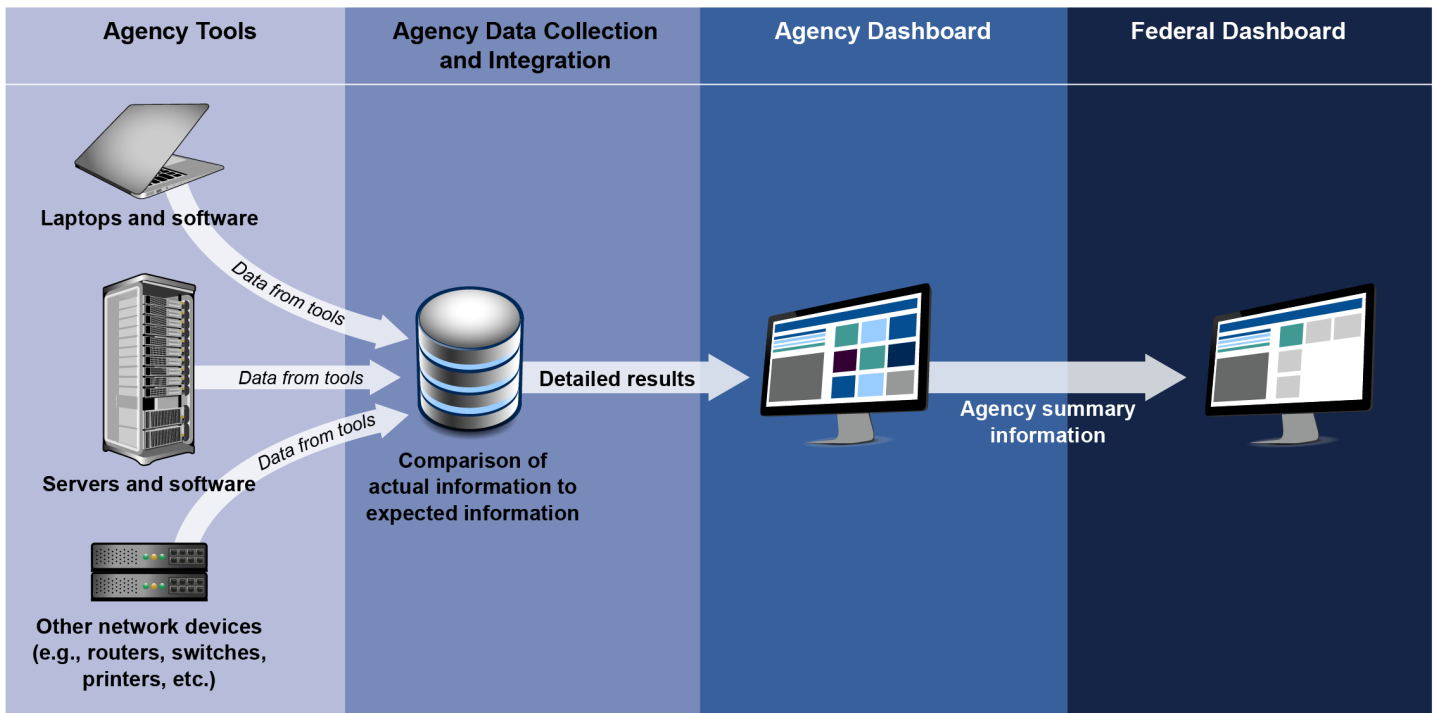
Source: GAO analysis of Department of Homeland Security data. | GAO-21-288

In August 2020,[85] we reported that selected agencies—the FAA, Indian Health Services, and Small Business Administration—had generally deployed these tools intended to provide cybersecurity data to support DHS's CDM program. However, while agencies reported that the program improved their network awareness, none of the three agencies had effectively implemented all key CDM program requirements. As part of our review, we made six recommendations to DHS and nine recommendations to the three selected agencies. DHS and the selected agencies concurred with the recommendations. As of December 2020, our recommendations had not been implemented.

- **DHS needs to develop a strategy to validate selected agencies' actions on meeting binding operational directive requirements.** DHS, in consultation with OMB, develops and oversees the implementation of compulsory directives—referred to as binding

---

[85]GAO, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020).

operational directives—covering executive branch civilian agencies. These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk. As of February 2021, DHS had issued nine directives that instructed agencies to, among other things, (1) mitigate critical vulnerabilities discovered by DHS through its scanning of agencies' internet-accessible systems; (2) address urgent vulnerabilities in network infrastructure devices identified by DHS; and (3) better secure the government's highest value and most critical information and system assets.

In February 2020, we reported that the directives' implementation often had been effective in strengthening federal cybersecurity.[86] For example, a 2016 directive addressed, among other things, several urgent vulnerabilities in the targeting of firewalls across federal networks and provided technical mitigation solutions. In response to the directive, agencies reported progress in mitigating risks to more than 11,000 network infrastructure devices as of October 2018.

However, we also reported that DHS did not consistently validate agencies' self-reported actions. In addition, we found that not all agencies had been able to address all the directives' requirements within the required timelines established in four out of the five directives we reviewed. We made three recommendations to DHS to address these issues. DHS concurred with our recommendations and outlined steps and timelines to address the recommendations. As of December 2020, one of the three recommendations—to develop a strategy to independently validate selected agencies' self-reported actions on meeting binding operational directive requirements—had not been implemented.

- **DHS needs to develop a plan for reassessing the high value asset program.** According to Binding Operational Directive 18-02, *Securing High Value Assets*, DHS was to enhance its approach to secure the federal government's high value assets (HVA) from cybersecurity threats.[87] In February 2020, we reported that in response to the directive and supplemental guidance, most of the

---

[86]GAO, *Information Technology: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed*, GAO-20-133 (Washington, D.C.: Feb. 4, 2020).

[87]A HVA is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission, or is considered essential to an agency's security and resilience.

federal civilian agencies had taken several steps to address the directive's requirements.[88] We also reported that DHS had taken steps to identify major or critical weaknesses from the HVA assessments.

However, the agencies and DHS had not completed the required assessments and mitigations consistent with OMB guidance and DHS policy. For example:

- To address the review requirement for Tier 1 HVAs (i.e., systems of critical impact to both the agency and the nation), DHS should have completed at least a total of 142 assessments a year. However, DHS completed only about half of the required annual assessments with 73 assessments completed in fiscal year 2019.

- As of February 2020, DHS had yet to issue the guidance, standards, and methodologies for Tier 2 or Tier 3 HVA assessments, which are to be conducted by third parties and agencies, respectively. As a result, agencies were not able to begin conducting assessments for the remaining 639 HVA systems.

- Agencies had not been able to mitigate the identified weaknesses within the required time frames. For instance, CISA's October 2019 data showed that of the 196 major or critical weaknesses identified in HVAs government-wide, agencies were not able to mitigate 160 within the required initial 30-day time frame; 75 major or critical weaknesses were still not mitigated as of early October 2019.

According to DHS officials from the HVA office, the department was reassessing key aspects of the program. However, we reported that it did not have a schedule or plan for completing this reassessment, or to address outstanding issues on completing required assessments, identifying needed resources, and finalizing guidance to agencies and third parties. We recommended that DHS develop a schedule and plan for completing this reassessment. DHS agreed with this recommendation but, as of December 2020, it had not been implemented.

- **OMB and others need to improve oversight and implementation of the federal cloud services program.** Established by OMB and managed by the General Services Administration (GSA), the Federal Risk and Authorization Management Program (FedRAMP) is intended

---

[88]GAO-20-133.

to provide a standardized approach to securing systems, assessing security controls, and continuously monitoring cloud services used by federal agencies. However, we reported in December 2019 that, while OMB required agencies to use FedRAMP to authorize the use of cloud services, it did not monitor or ensure that agencies were doing so.[89]

We also reported that FedRAMP participants identified a number of challenges, such as a lack of agency resources required to authorize a cloud service or those needed by the provider to implement the program's requirements. While GSA had taken steps aimed at addressing these challenges, its guidance on FedRAMP's requirements and participant's responsibilities were not always clear and the program's process for monitoring the status of security controls over cloud services was limited. Among other recommendations, we made one recommendation to OMB to enhance oversight and two to GSA to improve guidance and monitoring of the program. GSA agreed with the recommendations and OMB neither agreed nor disagreed. As of December 2020, these recommendations had not been implemented.

- **DHS and OMB need to fully establish initiatives to assist agencies in managing cybersecurity and address challenges.** In July 2019, we reported that, in response to Executive Order 13800, OMB and DHS identified areas for improvement in agencies' capabilities for managing cyber risks.[90] Further, we found that the initiatives under way should help address four challenges identified by agencies—hiring and retention, standardizing capabilities, receiving quality risk data, and using guidance. However, OMB and DHS did not establish initiatives to address other challenges on managing conflicting priorities, establishing and implementing consistent policies, developing risk management strategies, and incorporating cyber risks to agency enterprise risk management programs. To address these issues, we made one recommendation to OMB, in coordination with DHS, to assist agencies in addressing challenges. OMB did not state whether it agreed or disagreed with the recommendation. As of December 2020, our recommendation had not been implemented.

---

[89]GAO, *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed*, GAO-20-126 (Washington, D.C.: Dec. 12, 2019).

[90]GAO*, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019).

| Action 6—Address Weaknesses in Federal Information Security Programs | The federal government has been challenged in securing federal information and systems. Legislation and executive orders require agencies to implement security programs and manage cybersecurity risk to their enterprises. For example: |

- 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.[91] The act retains many of the requirements for federal agencies' information security programs previously set by the Federal Information Security Management Act of 2002.[92] 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.

- Executive Order 13800[93] 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.

We have performed numerous government-wide reviews to determine how well federal civilian agencies are managing information security risk to their systems and data. While improvements continue to be made, there are a number of weaknesses that federal agencies must continue to address. For example:

- **Agencies need to strengthen cybersecurity policies and practices.** Inspectors general determined that few agencies covered by the CFO Act of 1990 had effective agency-wide information security programs during fiscal year 2019. FISMA requires inspectors general to determine the effectiveness of their respective agencies'

---

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

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

[93]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

information security programs. To do so, OMB's FISMA guidance instructed inspectors general to provide a maturity model rating for agency information security policies, procedures, and practices related to the five core security functions established in the NIST cybersecurity framework, as well as for the agency-wide information security program.

The maturity model is designed to summarize the status of agencies' information security programs on a five-level capability maturity scale. The five maturity levels are defined as follows:

- Level 1 (Ad hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.

- Level 2 (Defined): Policies, procedures, and strategies are formalized and documented, but not consistently implemented.

- Level 3 (Consistently Implemented): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

- Level 4 (Managed and Measurable): Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.

- Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

According to this maturity model, Level 4 (managed and measurable) represents an effective level of security for each core function. Therefore, if an inspector general rates three or more of the agency's core security functions at Level 4 or Level 5, then the inspector general can consider that agency to have an effective information security program. However, the inspector general has the discretion to have a different conclusion on program effectiveness if he or she deems it appropriate to do so.

For fiscal year 2019, the inspectors general for only five of the 23 civilian CFO Act agencies reported that their agencies had an effective agency-wide information security program. The remaining 18 agencies were reported as having ineffective information security programs. When considering each of the five core security functions, most inspectors general reported that their agencies were at Level 2 (defined) or Level 3 (consistently implemented) for the Identify function, and at Level 3 (consistently implemented) for the Recover

function. A plurality of inspectors general reported that their agencies were at Level 2 (defined) for the Protect and Detect functions, and at Level 4 (managed and measurable) for the Respond function, as shown in figure 9.

Figure 9: Inspector General Ratings of the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Policies, Procedures, and Practices Related to the Cybersecurity Framework Core Security Functions

Total agencies with rating

Core security function

Level 1 - Ad-hoc
Level 2 - Defined
Level 3 - Consistently implemented
Level 4 - Managed and measurable
Level 5 - Optimized
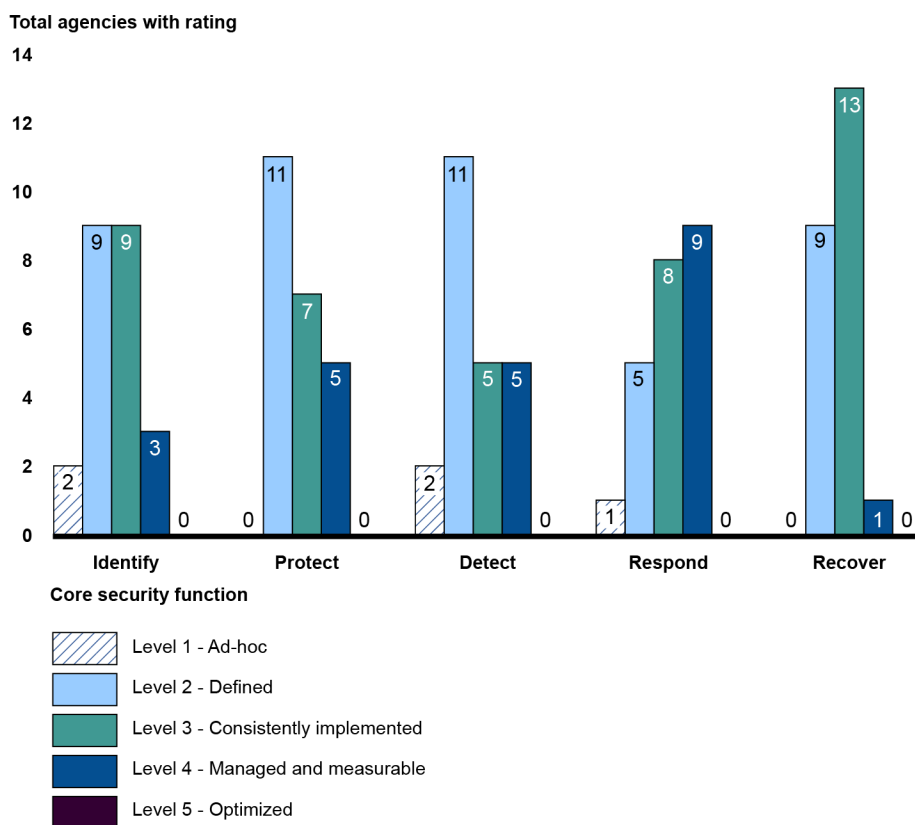
Source: GAO analysis of agency fiscal year 2019 Federal Information Security Modernization Act of 2014 reports. | GAO-21-288

In its efforts toward strengthening the federal government's cybersecurity, OMB also requires agencies to submit related cybersecurity metrics as part of its Cross-Agency Priority goals.[94] In

---

[94]The President's Management Agenda is intended to lay out a long-term vision for modernizing the federal government in key areas that will improve the ability of agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people. The Cross-Agency Priority goals described within the President's Management Agenda are 4-year outcome-oriented goals that measure federal progress toward implementing the agenda.

particular, OMB developed a goal so that federal agencies will be able to build and maintain more modern, secure, and resilient IT. A key part of this goal is to reduce cybersecurity risks to the federal mission through three strategies: limit personnel access, manage asset security, and protect networks and data. The key targets supporting each of these strategies correspond to areas within the FISMA metrics. Table 5 outlines the strategies, their associated targets, and the 23 civilian CFO Act agencies' progress in meeting those targets, as of June 2020.

Table 5: Civilian Agencies' Progress in Meeting the Office of Management and Budget's (OMB) Targets to Reduce Cybersecurity Risks, as Reported by OMB as of June 2020

Strategies to reduce cybersecurity risks	OMB's target(s)	Number of civilian agencies meeting the target (out of 23 agencies)
Limit Personnel Access	**Privileged Network Access Management:** 100 percent of privileged users are required to use a personal identity verification card or Authenticator Assurance Level 3 multifactor authentication method to access the agency's network.	18
	High Value Asset (HVA) Access Management: 90 percent of HVAs require all users to authenticate using a personal identity verification card or Authenticator Assurance Level 3 multifactor authentication method.	15
	Automated Access Management: 95 percent of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	19
Manage Asset Security	**Hardware Asset Management:** 95 percent of the organization's unclassified network has implemented a technology solution to detect and alert upon the connection of unauthorized hardware assets.	17
	Software Asset Management: 95 percent of the organization's assets are covered by a capability that is able to detect unauthorized software and alert appropriate security personnel.	17
	Authorization Management: 100 percent of high and moderate impact systems are covered by a valid security authorization to operate.	13
	Mobile Device Management: 95 percent of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	22
Protect Networks and Data	**Intrusion Detection and Prevention:** At least four of six intrusion prevention metrics have met an implementation target of at least 90 percent and 100 percent of email traffic is analyzed using domain-based message authentication, reporting, and conformance email authentication protocols.	16
	Exfiltration and Enhanced Defenses: 90 percent of outbound communications traffic is checked at the external boundaries to detect potential unauthorized exfiltration of information.	20
	Data Protection: At least four of six data protection metrics have met an implementation target of at least 90 percent.	16

Source: GAO summary of Office of Management and Budget data. | GAO-21-288

We and agency inspector generals have previously made recommendations aimed at addressing these weaknesses. For example:

- In July 2019,[95] we reported that OMB had not submitted its required FISMA report to Congress for fiscal year 2018 and had reduced the number of agencies at which it held CyberStat meetings from 24 in fiscal year 2016 to three in fiscal year 2018—

---

[95]GAO-19-545.

thereby restricting key activities for overseeing agencies' implementation of information security.[96] We made three recommendations to OMB, including to submit its FISMA report to Congress for fiscal year 2018 and expand its coordination of CyberStat meetings with agencies. OMB generally agreed with our recommendations, and as of December 2020, one recommendation related to submitting the FISMA report had been implemented.

- The inspectors general have previously made numerous recommendations to agencies to address weaknesses in their information security programs. However, many of these recommendations had not been implemented.

- **Agencies need to address information security control deficiencies that place financial information at risk.** During our audit of the U.S. government's fiscal years 2019 and 2018 consolidated financial statements, we found that the federal government's inability to identify and resolve information security control deficiencies was a material weakness.[97] Specifically, we reported that 18 of the 24 CFO Act agencies reported information security as a material weakness or significant deficiency for fiscal year 2019.

We identified control deficiencies related to (1) security management; (2) access to computer data, equipment, and facilities; (3) changes to and configuration of information system resources; (4) segregation of incompatible duties; and (5) contingency planning. For example, in May 2020, we reported that new and continuing deficiencies in the Internal Revenue Service's (IRS) information system security controls over financial and tax processing systems included deficiencies related to access controls, segregation of duties, and other areas.[98] These collectively represented a significant deficiency in risks of unauthorized access to, modification of, or disclosure of financial

---

[96]OMB, in coordination with DHS, is responsible for coordinating CyberStat review meetings. As mentioned previously, FISMA requires OMB to oversee agency compliance with requirements to provide information security protections on information and information systems. One means of fulfilling this oversight responsibility is through CyberStat engagements.

[97]GAO, *Financial Audit, FY 2019 and FY 2018 Consolidated Financial Statements of the U.S. Government*, GAO-20-315R (Washington, D.C.: Feb. 27, 2020).

[98]GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*, GAO-20-411R (Washington, D.C.: May 13, 2020).

reporting and taxpayer data and disruption of critical operations. We made 18 new recommendations to address these deficiencies, bringing the total number of cybersecurity recommendations that IRS has not yet implemented to 132. Until agencies identify and resolve these deficiencies and effectively manage information security risks on an ongoing basis, federal data and systems, including financial information, will remain at risk.

- **Agencies need to fully establish risk management programs and address challenges.** As previously mentioned, in July 2019, we reported on key practices for establishing an agency-wide cybersecurity risk management program that include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management program.[99] Although the 23 agencies we reviewed almost always designated a risk executive, they often did not fully incorporate other key practices in their programs, such as:

  - establishing a cybersecurity risk management strategy to delineate boundaries for risk-based decisions;

  - establishing agency- and system-level policies for assessing, responding to, and monitoring risk;

  - establishing a process for assessing agency-wide cybersecurity risks; and

  - establishing a process for coordinating between cybersecurity and enterprise risk management programs for managing all major risk.

  We made 57 recommendations to the 23 agencies to address the challenges identified in our report. Seventeen agencies agreed with the recommendations, one partially agreed, and five did not state whether they agreed or disagreed. However, as of December 2020, only 17 of our recommendations had been implemented.

- **Agencies need to develop modernization plans for critical legacy systems.** In June 2019, we reported that among the 10 most critical legacy systems we identified as in need of modernization, several used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.[100] For example, a DHS legacy system had a large number of reported

---

[99]GAO-19-384.

[100]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: June 11, 2019).

vulnerabilities, which were considered a high or critical risk to its network. In addition, a Department of the Interior system contained obsolete hardware that was not supported by the manufacturers, resulting in long-term exposure to security and performance weaknesses.

Furthermore, we reported that of the 10 agencies responsible for these legacy systems, seven agencies had documented plans for modernizing the systems, while three did not have documented modernization plans. Prolonging the lifespan of these increasingly vulnerable and obsolete systems exposed the agencies and system clients to security threats and significant performance issues. In our sensitive report, we made eight recommendations to ensure that agencies document modernization plans for selected legacy systems. The agencies agreed with our recommendations.[101] As of December 2020, the recommendations had not been implemented.

It is also critically important that agencies address cybersecurity risks to the (1) COVID-19 response; the (2) 2020 Decennial Census; and (3) DOD systems, including DOD-wide cybersecurity practices, as well as cybersecurity risks facing weapons systems and financial systems.

- **The Department of Health and Human Services (HHS) needs to address cybersecurity risks to the COVID-19 response.** Since March 2020, malicious cyber actors have taken advantage of the attention being given to the COVID-19 pandemic to target organizations that make up the health care and public health critical infrastructure sector, including government entities, such as HHS. We have identified numerous cybersecurity weaknesses at multiple HHS component agencies—including the Centers for Medicare & Medicaid Services (CMS), Centers for Disease Control and Prevention, and Food and Drug Administration—over the last 6 years, such as weaknesses in key safeguards to limit, prevent, and detect inappropriate access to computer resources. In September 2020, we recommended that HHS expedite implementation of our prior recommendations regarding cybersecurity weaknesses at its component agencies.[102] HHS agreed with the recommendation and,

---

[101]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-351SU (Washington, D.C.: June 11, 2019).

[102]GAO, *COVID-19: Federal Efforts Could Be Strengthened by Timely and Concerted Actions*, GAO-20-701 (Washington, D.C.: Sept. 21, 2020).

as of November 2020, the component agencies had made significant progress by implementing 404 (about 93 percent) of the 434 recommendations we issued in previous reports.[103]

- **The Census Bureau (Bureau) needs to take further actions to reduce key cybersecurity risks to the 2020 Census.** Cybersecurity of the Bureau's IT systems continues to remain important as the Bureau processes the PII data on over a hundred million households across the country in an effort to produce data products that are to be released starting in 2021. As we testified in April 2019, the 2020 Decennial Census was on our list of high-risk programs primarily because the Bureau (1) was using innovations that were not expected to be fully tested, (2) continued to face challenges in implementing IT systems, and (3) faced significant cybersecurity risks to its systems and data.[104] Specifically, we reported that the Bureau had established a risk management framework that required it to conduct a full security assessment for each system expected to be used for the 2020 Census and, if deficiencies were identified, to determine the corrective actions needed to remediate those deficiencies.

  This framework required the agency to develop and implement a plan of actions and milestones (POA&M) for addressing the deficiency or weakness. As of March 2019, the Bureau had over 500 POA&Ms to remediate for issues identified during security assessment activities, with nearly half considered "high-risk" or "very high-risk." Furthermore, of the open POA&Ms we reviewed, over 100 were identified as being delayed. To address this issue, we made a recommendation to Commerce to direct the Bureau to better ensure that cybersecurity weaknesses were addressed within prescribed time frames. Commerce agreed with our recommendation.

  As of December 2020, the Bureau had made some progress toward addressing this recommendation; however, the recommendation had not been fully implemented.

- **DOD needs to take actions to improve its implementation of key department-wide cybersecurity practices.** In April 2020, we reported that DOD had not fully implemented three of its key initiatives

---

[103]GAO, *COVID-19: Urgent Actions Needed to Better Ensure an Effective Federal Response,* GAO-21-191 (Washington, D.C.: Nov. 30, 2020).

[104]GAO, *2020 Census: Further Actions Needed to Reduce Key Risks to a Successful Enumeration*, GAO-19-431T (Washington, D.C.: Apr. 30, 2019).

and practices aimed at improving cyber hygiene.[105] For example, the DOD Culture and Compliance Initiative set forth 11 overall tasks to improve cyber hygiene, of which seven were not fully implemented. In addition, we reported that DOD had identified techniques that adversaries used most frequently against its networks, and identified practices to protect the networks and systems against these techniques. However, the department did not know the extent to which these practices had been implemented.

Furthermore, we reported that two recurring reports provided updates to senior DOD leaders on cybersecurity information. However, these reports did not provide leadership with information on two cyber hygiene initiatives or the implementation of cyber hygiene practices. We made seven recommendations to DOD to address these issues and other concerns. Of the seven, the department concurred with one, partially concurred with four, and did not concur with two. We believed that all our recommendations were warranted. As of December 2020, our recommendations had not been implemented.

- **DOD needs to address cybersecurity risks facing major weapon programs and systems.** In October 2018, we reported that DOD faced mounting challenges in protecting its weapon systems from increasingly sophisticated cyber threats.[106] This was due to the computerized nature of weapon systems, DOD's late start in prioritizing weapons systems cybersecurity, and DOD's nascent understanding of how to develop more secure weapon systems. In addition, we reported that DOD routinely found mission critical cyber vulnerabilities in systems that were under development. Testers were able to take control of systems and largely operate undetected using relatively simple tools and techniques. Also, the vulnerabilities that DOD was aware of likely represented a fraction of total vulnerabilities due to testing limitations. Furthermore, we reported that the department had barriers that could limit the effectiveness of these steps, such as cybersecurity workforce challenges and difficulties sharing information and lessons about vulnerabilities.

  To its credit, we reported that DOD had undertaken initiatives, in part directed by Congress, to help understand and address weapon systems cyber vulnerabilities. For example, we reported that DOD was compiling existing vulnerability information and conducting some

---

[105]GAO, *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene,* GAO-20-241 (Washington, D.C.: Apr. 13, 2020).

[106]GAO, *Weapon System Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

new tests to provide information about the cybersecurity posture of individual systems. In addition, we noted that the military services established weapon system cybersecurity-focused offices to improve their cybersecurity postures.

Although we did not make any recommendations to DOD in our 2018 report, we stated that it was essential that the department sustain its momentum in developing and implementing key initiatives for improving the state of weapon systems cybersecurity. In March 2020, the Cyberspace Solarium Commission echoed this conclusion and called for Congress to direct the department to institutionalize a continuous assessment process and annually report these vulnerabilities to sustain its momentum in implementing key initiatives. In January 2021, Congress enacted a law that directed the department to develop a comprehensive plan for the annual assessment of cyber vulnerabilities of its major weapon systems.[107]

In March 2021, we reported that since our 2018 report, DOD had made strides in improving weapon systems cybersecurity, including greater access to cyber expertise, increased use of cyber assessments, better tailoring of security controls, and additional cybersecurity guidance.[108] Although it had taken promising steps, we reported that DOD still had challenges to overcome in order to improve weapon systems cybersecurity. In particular, DOD was still learning how to contract for cybersecurity in weapon systems, and selected programs we reviewed have struggled to incorporate systems' cybersecurity requirements into contracts. In addition, DOD and contractor officials told us that contracting for cybersecurity requirements was a general challenge. Although DOD and the military services had developed a range of policy and guidance documents to improve weapon systems cybersecurity, the guidance usually did not specifically address how acquisition programs should include cybersecurity requirements, acceptance criteria, and verification processes in contracts.

We made three recommendations to DOD, including recommending that the Army and Navy issue guidance on incorporating weapon systems cybersecurity requirements into contract language. DOD concurred with two of our recommendations and partially concurred

---

[107]Pub. L. No. 116-283, § 1712, 134 Stat. at 4087.

[108]GAO, *Weapons Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*, GAO-21-179 (Washington, D.C.: Mar. 4. 2021).

with one of our recommendations. As of March 2021, these recommendations had not yet been implemented.

- **DOD needs to address cybersecurity challenges that limited its ability to present accurate financial statements.** In September 2020, we reported that data supporting DOD's fiscal year 2019 financial statements were not reliable, according to DOD's Office of Inspector General and independent auditors.[109] In January 2020, the office reported that the department had wide-ranging weaknesses in its financial management systems that prevented it from collecting and reporting financial and performance information that was accurate, reliable, and timely.[110] Specifically, the Inspector General reported 25 material weaknesses that impacted DOD's ability to achieve an unmodified audit opinion in its fiscal year 2019 department-wide financial statements. These material weaknesses are based, in large part, on identified deficiencies and corresponding recommendations, also known as notices of findings and recommendations (NFRs).

  In fiscal year 2019, independent public accountants issued 2,100 new and reissued NFRs to the military services and in January 2020, DOD's Office of the Inspector General reported that the department remediated approximately 26 percent of the military services' NFRs from fiscal year 2018. Of the 2,100 fiscal year 2019 NFRs, 1,008 were related to IT and cybersecurity issues. We reported that DOD had a strategy to address the NFRs and the department's underlying financial management system weaknesses. However, this strategy did not include measures for tracking progress in achieving the strategy's goals. Specifically, DOD had developed a plan to begin to address the IT and cybersecurity issues, but it lacked performance goals (including performance indicators, targets, and time frames) to effectively monitor the status of remediating the issues. Furthermore, DOD had not developed an enterprise road map to implement its strategy, as called for by OMB. We made six recommendations to address these and other weaknesses. DOD concurred with our recommendations. However, as of December 2020, the recommendations had not been implemented.

---

[109]GAO, *Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment*, GAO-20-252 (Washington, D.C.: Sept. 30, 2020).

[110]Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020).

Action 7—Enhance the Federal Response in Cyber Incidents	Cyber incidents are increasingly posing a threat to government and private sector entities. Presidential Policy Directive-41 (PPD-41)[111] 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 are to undertake three concurrent lines of effort when responding to any cyber incident: threat response;[112] asset response;[113] and intelligence support and related activities.[114] In addition, when a federal agency is an affected entity, the directive states it is to undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce. Further, the directive calls for a Cyber Unified Coordination Group (UCG) to be formed to coordinate the federal response to a significant cyber incident.[115]

As previously mentioned, in December 2020, CISA issued an emergency directive and alert explaining that an advanced persistent threat actor had been observed leveraging, among other techniques, a software supply chain compromise of an enterprise network management software suite and inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine

---

[111]The White House, *United States Cyber Incident Coordination*, Presidential Policy Directive/PPD-41 (Washington, D.C.: July 26, 2016).

[112]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 and operational coordination with asset response.

[113]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.

[114]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.

[115]According to PPD-41, a UCG is the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating private sector partners into incident response efforts.

version of that software product.[116] The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations. CISA's alert further explained that the advanced persistent threat actor had demonstrated complex intrusion techniques and the agency expects that removing this threat actor from compromised environments will be highly complex and challenging. According to CISA, this threat poses a grave risk to federal, state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations.

Subsequently, in December 2020, the NSC staff formed a UCG in accordance with PPD-41 to coordinate a whole of government response to the cyberattack. The UCG is composed of the FBI, CISA, and ODNI, with support from the National Security Agency. According to a January 2021 update from the UCG, the advanced persistent threat actor was likely of Russian origin whose activities are believed to be related to intelligence gathering efforts. The update also noted that of the approximately 18,000 affected enterprise network management software suite customers, a much smaller number of customers have been compromised. For example, the UCG reported that fewer than 10 U.S. government agencies' systems were compromised. In addition, the update emphasized that the UCG is continuing its investigation and that it was working to identify and notify the nongovernment entities that also may be impacted.

Nevertheless, our prior work has identified weaknesses that may hamper the response to this cyberattack where a federal agency is an affected entity.

- **Agencies and OMB need to strengthen information security policies and practices, including incident response.**[117] FISMA requires agencies to develop, document, and implement an agency-wide information security program that includes procedures for reporting security incidents to the United States Computer Emergency Readiness Team (US-CERT). In addition, NIST guidance states that agencies should have specific incident reporting requirements for reporting suspected security incidents to an internal incident reporting

---

[116]CISA, *Emergency Directive 21-01* and *Alert AA20-352A.*

[117]GAO-19-545.

organization.[118] However, in July 2019, we reported that most of our 16 selected federal agencies had deficiencies in at least one of the activities associated with incident response processes, as shown in figure 10.

Figure 10: Number of 16 Selected Agencies with Deficiencies in Incident Response

Number of agencies

Incident response
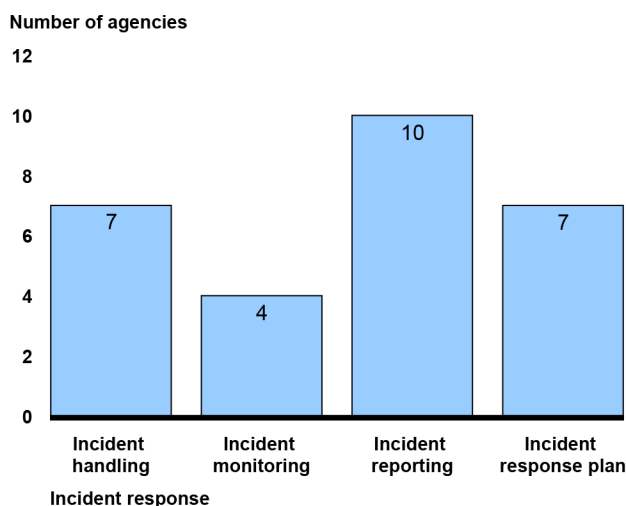
Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-21-288

As shown in figure 10, agencies had deficiencies in their implementation of incident reporting. While only two agencies did not clearly define incident reporting requirements, eight agencies did not effectively implement those requirements. For example, these agencies did not consistently categorize incidents or ensure timely reporting of incidents to US-CERT and internal reporting organizations. We and the Inspectors General have made thousands of recommendations aimed at improving information security programs and practices—including those related to incident response processes over the years. However, as we previously reported, many of these recommendations remained unimplemented.

The Cyberspace Solarium Commission has also identified weaknesses and made recommendations related to three areas of cyber incident

---

[118]NIST, *Computer Security Incident Handling Guide,* SP 800-61, Rev. 2 (Gaithersburg, Md.: Aug. 2012).

response—threat response, asset response, and intelligence support, including the following:[119]

- *Threat response.* The commission identified actions Congress and the executive branch could take to respond to threat actors that carry out cyberattacks, including actions in the following areas:

  - improving law enforcement tools for pursuing international crimes;

  - ensuring that the FBI is properly resourced to carry out its cyber mission; and

  - developing and issuing a new national cyber strategy reflecting a strategic approach of a layered cyber deterrence,[120] with an emphasis on the concept of "defend forward."[121]

- *Asset response.* The commission identified actions Congress and the executive branch should take to establish a national capacity to respond to and recover from a significant cyber disruption. For example, according to the commission, while continuity of operations and continuity of government have long been cornerstones of government contingency planning, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major cyber disruption. Accordingly, the commission recommended that Congress should direct the executive branch to develop and maintain "Continuity of the Economy" planning to ensure the continuous operation of the economy in the event of a major cyber disruption. In January 2021, Congress enacted a law that required the executive branch to establish a continuity of the economy planning

---

[119]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[120]According to the commission, "layered cyber deterrence" encompasses the following three actions (1) shape behavior—that is, work with allies and partners to promote responsible behavior in space; (2) deny benefits to adversaries by securing critical networks in collaboration with the private sector and increasing the security of the cyber ecosystem; and (3) impose costs—that is, maintain the capability, capacity, and credibility needed to retaliate against actors who target the United States in and through cyberspace.

[121]According to the commission, "defend forward" posits that, in order to disrupt and defeat ongoing adversary campaigns, the United States must actively observe, pursue, and counter adversaries operations and impose costs short of armed conflict. This posture signals to adversaries that the U.S. government will respond to cyberattacks—even those below the level of armed conflict that do not cause physical destruction or death—with all the tools at its disposal and consistent with international law.

effort to facilitate the restart and recovery of the U.S. economy after a major cyber disruption.[122]

- *Intelligence support.* The commission identified several actions that agencies can take to improve attribution analysis.[123] For example, the commission stated that ODNI—in partnership with the private sector through DHS and the FBI—could improve attribution analysis by (1) standardizing ODNI's attribution guidelines and assessment timeline; (2) establishing an attribution analysis working group, which should include key private sector analysis and data to accelerate the federal government's response; and (3) advancing analytic capabilities by applying emerging technologies and diversifying data sources to overcome evolving technical challenges.

Agencies Need to Address Action on Protecting Cyber Critical Infrastructure

The federal government has been challenged in working with the private sector to protect cyber 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.

However, federal agencies have not addressed most of our recommendations related to the challenge of protecting critical infrastructure. Of the nearly 80 recommendations made in our public reports since 2010, nearly 50 had not been implemented as of December 2020. We have also designated 11 as priority recommendations, and as of December 2020, nine had not been implemented. Until our recommendations are fully implemented, federal agencies may be limited in their ability to ensure the critical infrastructures are protected from potentially harmful cybersecurity threats.

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

The nation's critical infrastructure includes both public and private systems vital to national security and other efforts including providing the essential services that underpin American society. In particular, Presidential Policy Directive 21 identifies the nation's 16 critical

---

[122]Pub. L. No. 116-283, § 9603, 134 Stat. at 4829.

[123]According to the commission, attribution refers to the identification of technical evidence of a cyber event and/or the assignment of responsibility for a cyber event. Accurate and timely attribution of a cyber event enables U.S. leaders to make the most informed decisions to protect the country through consideration of appropriate response actions in order to enforce norms of accountability in cyberspace.

infrastructure sectors that include key areas such as banking, water, and electricity.[124]

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[125] 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, 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*.[126] The framework is intended 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.

We and agency inspectors general have made recommendations aimed at protecting the cybersecurity of critical infrastructure in the following three areas: (1) adoption of the framework for improving critical infrastructure cybersecurity, (2) cyber threat information sharing, and (3) sector-specific weaknesses.

Specifically, we have identified additional actions that agencies need to take to improve adoption of the framework.

- **Federal agencies with lead roles in protecting critical infrastructure need to collect and report on improvements from using NIST's framework**.[127] In February 2020, we reported that the

---

[124]The White House, Presidential Policy Directive 21/PPD-21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: February 2013).

[125]The White House, *Improving Critical Infrastructure Cybersecurity,* Executive Order 13636 (Washington, D.C.: Feb. 12, 2013).

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

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

nine sector-specific agencies (SSAs)[128] were adopting the framework and seeing resulting improvements from its adoption.[129] However, the agencies with lead roles in protecting critical infrastructure were not collecting and reporting on improvements from using the framework. We concluded that collecting and reporting on these improvements would help SSAs understand the extent to which sectors are better protecting their critical infrastructures from cyber threats. To address these issues, we made 10 recommendations, including one recommendation to NIST and nine to the SSAs. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. We believed that all 10 recommendations were warranted. As of December 2020, none of the recommendations had been implemented.

Agency inspectors general and the Cyberspace Solarium Commission have made recommendations aimed at improving the sharing of cyber threat information between federal agencies. For example:

- **Agencies need to fully address recommendations related to the implementation of the *Cybersecurity Information Sharing Act of 2015*.** In December 2015, the President signed the *Cybersecurity Information Sharing Act of 2015* into law to encourage the sharing of cyber threat information between the public and private sectors in a timely manner.[130] The act designated seven federal agencies to coordinate and develop government-wide, publicly available policies, procedures, and guidance to assist federal and nonfederal entities in their efforts to receive and share cyber threat indicators and defensive

---

[128]SSA was the term formerly used to describe the nine agencies that have a lead role in protecting the 16 critical infrastructure sectors identified in PPD-21. Pursuant to the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116 283, § 9002(c)(3), 134 Stat. at 4773, any reference to an SSA in any law, regulation, document, or other paper of the United States shall be deemed a reference to the Sector Risk Management Agency (SRMA) of the relevant critical infrastructure sector. According to the act, SRMA has the meaning that had been given to SSA in 6 U.S.C. § 651(5).

[129]GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Feb. 25, 2020).

[130]Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2242, 2936-56 (2015) (codified at 6 U.S.C. §§ 1501-10).

measures.[131] In December 2019, the inspectors general of the seven agencies issued a report on the implementation of this law.[132] Specifically, the inspectors general reported that sharing of cyber threat indicators and defensive measures had improved over the past 2 years and efforts were underway to expand accessibility to information.

However, the report also identified barriers that had hindered cybersecurity information sharing, such as

- the number of nongovernmental entities using the Automated Indicator Sharing system[133] was minimal, and other challenges with the Automated Indicator Sharing information deterred its use;

- restrictive classifications;

- inability of machines to communicate with each other; and

- uncertainty about protection from liability, which impacts the willingness of private sector entities to share cyber threat information.

To address these barriers, the agency inspectors general made recommendations aimed at improving cybersecurity information sharing, including recommending that DHS develop an approach to encourage federal and private sector participants to share information with the department.

In March 2020, the Cyberspace Solarium Commission also made several recommendations aimed at improving cyber threat information sharing, such as

- improving the intelligence community's ability to develop and share cyber threat information with critical infrastructure organizations,

- notifying owners and operators of known vulnerable or comprised systems, and

---

[131]These seven agencies were DHS, DOJ, DOD, Commerce, Energy, and the Treasury, and ODNI.

[132]Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, AUD-2019-005-U (Dec. 19, 2019).

[133]As required by statute, DHS developed the Automated Indicator Sharing capability from which federal entities and nonfederal entities share cyber threat information in real time.

- creating a voluntary network monitoring and threat detection program with the private sector to enable the rapid detection and identification of cyber threats.

We have also reported on critical infrastructure protection issues to specific critical infrastructure sectors that need to be addressed. For example:

- **FAA should prioritize oversight of evolving cyber threats and increasing connectivity between airplanes and other systems.** In October 2020, we reported that FAA had established a process for the certification and oversight of U.S. commercial airplanes, including their operations.[134] However, FAA had not prioritized risk-based cybersecurity oversight, through an assessment of its oversight program to determine the priority of avionics cybersecurity risks, the development of an avionics cybersecurity training program, the issuance of guidance for independent cybersecurity testing, or the inclusion of periodic testing as part of its monitoring process.

  We also reported that FAA coordinated with other key federal agencies and industry to address aviation cybersecurity issues. However, FAA's internal coordination activities did not fully reflect our key collaboration practices. For example, FAA had not established a tracking program for monitoring progress on issues raised at meetings and its oversight was not supported through dedicated agency resources in its budget.

  To address these issues we made six recommendations to FAA. FAA agreed with most of our recommendations; however, as of December 2020, the recommendations had not been implemented.

- **The Department of the Treasury (Treasury) needs to work with other financial sector federal agencies and partners to better measure progress and to prioritize efforts in line with sector cybersecurity goals.** In September 2020, we reported that Treasury and other federal agencies were taking steps to reduce risks and bolster the financial sector's efforts to improve its cybersecurity.[135] However, Treasury had not worked with other federal agencies and sector partners to better measure progress and to prioritize efforts in

---

[134]GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks,* GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

[135]GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts,* GAO-20-631 (Washington, D.C.: Sept. 17, 2020).

line with sector cybersecurity goals laid out in the 2019 *National Cyber Strategy Implementation Plan*. To address these issues, we made two recommendations to Treasury. The department agreed with our recommendations; however, as of December 2020, the recommendations had not been implemented.

- **DHS should update guidance for the Chemical Facility Anti-Terrorism Standards (CFATS) program.**[136] Thousands of high-risk chemical facilities may be subject to the risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass causalities to surrounding populations. In May 2020, we reported that DHS had guidance designed to help the estimated 3,300 facilities covered by CFATS comply with cybersecurity and other standards.[137]

  However, we found that DHS had not reviewed or updated the CFATS program guidance in over 10 years. DHS also did not have a process to routinely review its cybersecurity guidance to ensure that it was up to date with current threats and technological advances. We also reported that the CFATS program had a cybersecurity training program for its inspectors. However, the training did not fully address three of four key training practices, or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance.

  Accordingly, we made six recommendations to DHS, including recommending that the CFATS program routinely review its cybersecurity guidance and update, as needed; fully incorporate key training practices; and identify workforce cybersecurity needs. DHS concurred with the recommendations. However, as of December 2020, the recommendations had not been implemented.

- **The Transportation Security Administration (TSA) should fully incorporate NIST cybersecurity standards into select assessments for the transportation sector.** Recent physical and cyberattacks on rail systems in U.S. and foreign cities highlight the

---

[136]The CFATS program within DHS evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures.

[137]GAO, *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities,* GAO-20-453 (Washington, D.C.: May 14, 2020).

importance of strengthening and securing passenger rail systems around the world. TSA is the primary federal agency responsible for securing transportation in the United States. To assess risk elements for physical and cyber security in passenger rail, TSA utilizes various risk assessments, including, among other things, the Baseline Assessment for Security Enhancement (BASE).[138] TSA uses these risk assessments to evaluate threat, vulnerability, and consequence for attack scenarios across various transportation modes.

In April 2020, we reported[139] that while TSA had taken initial steps to share cybersecurity key practices and other information with passenger rail stakeholders, the BASE assessment did not fully reflect the updated cybersecurity key practices presented in NIST's Cybersecurity Framework,[140] nor did it include the framework in a list of available cyber resources.[141] Our review of the BASE cybersecurity questions in the template found that they covered selected activities associated with three of the five functions outlined in the framework— Identify, Protect, and Respond. However, the remaining two functions—Detect and Recover—were not represented in the BASE.

We made two recommendations to TSA, including that the agency update the BASE cybersecurity questions to ensure they reflect key practices. DHS agreed with our recommendations; as of December 2020, one recommendation had not been implemented.

---

[138]The BASE is a voluntary security assessment of national mass transit, passenger rail, and highway systems conducted by TSA surface transportation inspectors that addresses potential vulnerabilities, among other things. The BASE is a nonregulatory security assessment, which requires surface transportation entities' voluntary participation. It consists of an assessment template with 17 security action items developed by TSA and the Federal Transit Administration that address, among other best practices, security training programs, risk information sharing, and cybersecurity. TSA developed this assessment in 2006 to increase domain awareness, enhance prevention and protection capabilities, and further response preparedness of passenger transit systems nationwide.

[139]GAO, *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices,* GAO-20-404 (Washington, D.C.: Apr. 3, 2020).

[140]NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

[141]For example, TSA has shared cybersecurity information through American Public Transportation Association working groups, through training exercises such as the Intermodal Security Training and Exercise Program, and through regional cybersecurity workshops promoting the NIST Cybersecurity Framework. TSA further shares cybersecurity key practices through questions in the BASE.

- **The Department of Energy (DOE) needs to develop plans for electric grid cybersecurity that address the key characteristics that are desirable for a national strategy**. In August 2019, we reported that the electric grid faced various cybersecurity risks.[142] DOE had developed plans and an assessment to address these risks. However, we found that these documents did not fully address all of the key characteristics of a national strategy.

  In addition, we reported that FERC had approved mandatory grid cybersecurity standards. However, it had not ensured that those standards address federal guidance, specifically NIST's Cybersecurity Framework.[143] To address these issues, we made three recommendations—one to DOE and two to FERC. DOE and FERC agreed with our recommendations; however, as of December 2020, these recommendations had not been implemented.

  Similarly, in March 2021, we reported that the electric grid's distribution systems also faced various cybersecurity risks.[144] DOE had developed plans and an assessment to address the risk to the electric grid; however, we found that these documents did not fully address risks to the grid's distribution systems. To address this issue, we recommended that DOE more fully address cyber risks to the grid's distribution systems in its plans to implement the national cybersecurity strategy for the grid. As of March 2021, our recommendation had not been implemented.

- **TSA should address weaknesses in its management of pipeline cybersecurity efforts.** In December 2018, we found weaknesses in TSA's management of its pipeline security efforts.[145] We reported that TSA had issued revised pipeline security guidelines; however, the revisions did not include all elements from NIST's Cybersecurity Framework and did not include clear definitions to ensure the identification of critical facilities by pipeline operators.[146] We also reported that the agency conducted pipeline security reviews to

---

[142]GAO, *Critical Infrastructure Protection: Actions Needed to Address Electric Grid Cybersecurity Risks,* GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[143]National Institute of Standards and Technology, *Cybersecurity Framework*.

[144]GAO, *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: March 18, 2021).

[145]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

[146]National Institute of Standards and Technology, *Cybersecurity Framework*.

assess pipeline systems vulnerabilities; however, the quantity of TSA's reviews of corporate and critical facilities security had varied considerably. Figure 11 shows the U.S. pipeline system's basic components and vulnerabilities.

Figure 10: U.S. Pipeline Systems' Basic Components and Vulnerabilities
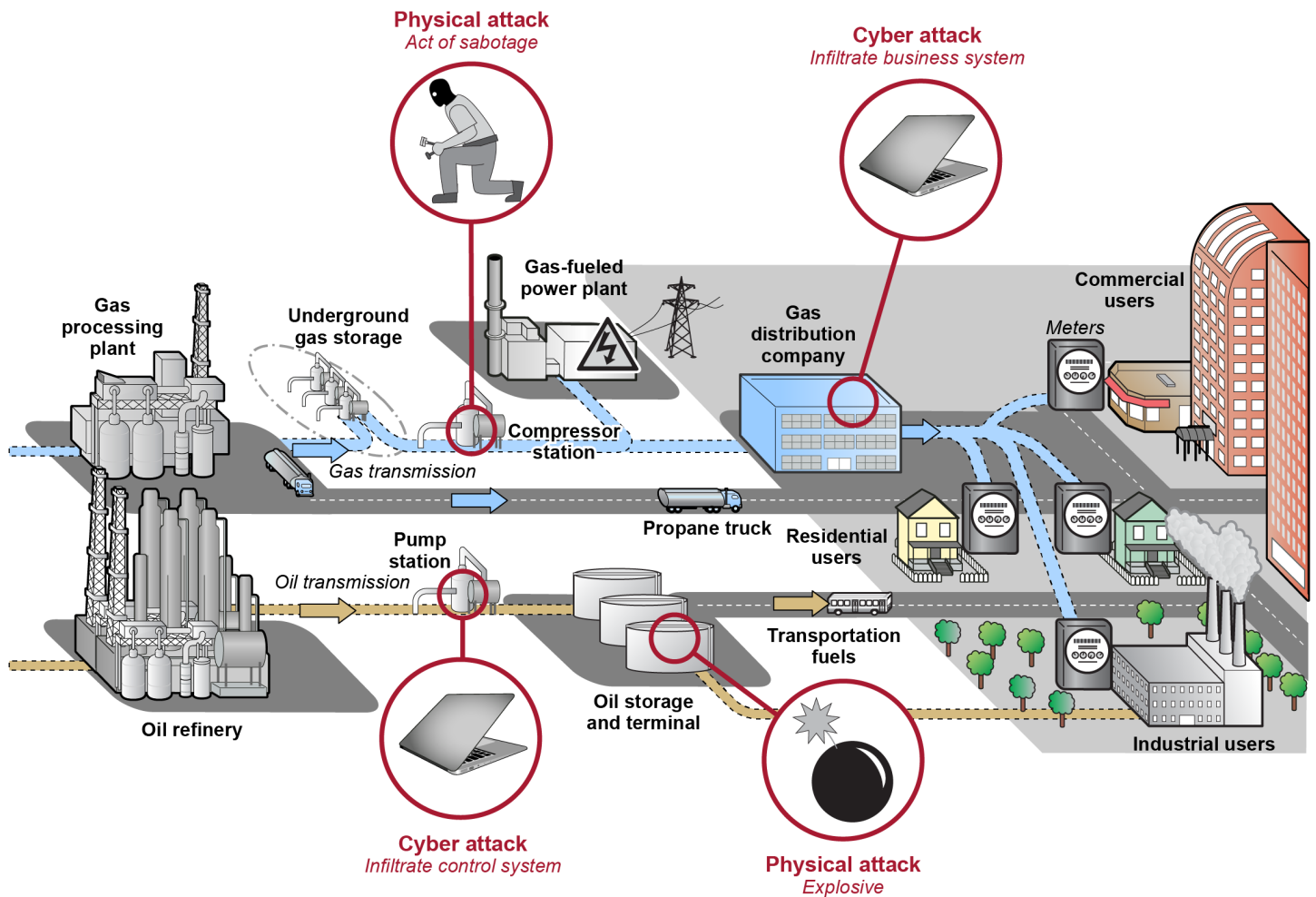
Additionally, we identified limitations to the usefulness of TSA's risk assessments methodology. For instance, the methodology had not been updated since 2014, data sources for threat and vulnerability inputs were not fully documented, and the risk assessment had not been peer reviewed since 2007. Further, we reported that the agency had established performance measures to monitor pipeline security

review recommendations, analyze their results, and assess effectiveness in reducing risks. However, these measures did not possess key attributes—such as clarity and having measurable targets—that we have found are key to successful performance measures.

To address these issues we made 10 recommendations to TSA. The agency agreed with all of our recommendations. As of December 2020, TSA implemented six of the recommendations and had not implemented the remaining four.

Agencies Need to Address Two Actions Related to Protecting Privacy and Sensitive Data

The federal government has been challenged in protecting privacy and sensitive data. Advances in technology have made it easy to correlate information about individuals across large and numerous databases. Further, ubiquitous internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices.

However, federal agencies have not addressed many of our recommendations related to the challenge of protecting privacy and sensitive data. Of the nearly 130 recommendations we have made in public reports since 2010, nearly 60 had not been implemented as of December 2020. We have also designated 12 as priority recommendations, and as of December 2020, three had not been implemented. Until our recommendations are fully implemented, federal agencies may be limited in their ability to protect private and sensitive data entrusted to them.

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. Further, ubiquitous internet and cellular connectivity make it easier to track individuals by allowing easy access to information pinpointing their locations.

Federal agencies hold millions of sensitive records for people all over the country. We have previously identified actions that need to be taken to better protect these data, including fully implementing practices for overseeing sensitive information that federal agencies exchange with other entities. For example:

- **The Department of Housing and Urban Development (HUD) needs to effectively protect sensitive information exchanged with external entities**. To administer housing, community investment, and mortgage loan programs, HUD collects a vast amount of sensitive personal information and shares it with external entities, including federal agencies; contractors; and state, local, and tribal organizations. However, we reported in September 2020 that HUD was not effectively protecting sensitive information exchanged with external entities.[147] Of the four leading practices for such oversight, HUD did not address one practice and only minimally addressed the other three in its security and privacy policies and procedures (see table 6).

Table 6: Extent to Which the Department of Housing and Urban Development (HUD) Policies and Procedures Address Leading Practices for Overseeing the Protection of Sensitive Information

Practice	Rating
Require risk-based security and privacy controls	◕
Independently assess implementation of controls	○
Identify and track corrective actions needed	◕
Monitor progress implementing controls	◕

Legend: ◕=Minimally addressed—leading practice was addressed to a limited extent; ○=Not addressed—leading practice was not addressed.

Source: GAO analysis of HUD data. | GAO-21-288

In addition, HUD was not fully able to identify external entities that process, store, or share sensitive information with its systems used to support housing, community investment, or mortgage loan programs.

We made five recommendations to HUD to fully implement the four leading practices and fully identify the extent to which sensitive information is shared with external entities. HUD did not agree or disagree with the recommendations, but described actions intended to address them. As of December 2020, the recommendations had not been implemented.

- **Selected federal agencies need to coordinate on data protection requirements with states.** To protect data that are shared with state government agencies, federal agencies have established cybersecurity requirements and related compliance assessment

---

[147]GAO, *Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities,* GAO-20-431 (Washington, D.C.: Sept. 21, 2020).

programs. Specifically, they have numerous cybersecurity requirements for states to follow when accessing, storing, and transmitting federal data. In May 2020,[148] we reported that four selected federal agencies had a significant number of variances in the cybersecurity requirements that they had established for protecting data exchanged with state agencies.[149]

Specifically, our review identified hundreds of instances in which the four agencies either had (1) included a requirement in their cybersecurity policies that was not a requirement of the other three agencies; (2) established a requirement with specific, organization-defined technical thresholds that differed from at least one of the other three agencies for a related control; or (3) did not fully address NIST guidelines.[150] As a result of our work, we made 12 recommendations to the four selected agencies and to OMB, including recommending that OMB improve its coordination of state cybersecurity requirements among federal agencies. Three agencies agreed with the recommendations and one agency partially agreed or disagreed with them. OMB did not provide comments. However, we believed all recommendations were warranted. As of December 2020, our recommendations had not been implemented.

- **IRS needs to ensure that security requirements for third-party providers provides assurance that information is being protected**. IRS seeks to help safeguard taxpayers' information and the electronic filing system by prescribing requirements for various types of third-party providers through its Authorized e-file Provider program. IRS Revenue Procedure 2007-40 states that the security of taxpayer accounts and personal information is a top priority for the agency.[151] However, we reported in May 2019 that taxpayer information held by third-party providers—such as paid tax return preparers—generally falls outside of these requirements, according to

---

[148]GAO, *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States,* GAO-20-123 (Washington, D.C.: May 27, 2020).

[149]The selected agencies were CMS within HHS, the FBI Criminal Justice Information Services within DOJ, IRS within the Treasury, and the Social Security Administration.

[150]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations,* SP 800-53, Rev. 4 (Gaithersburg, Md.: Apr. 2013).

[151]IRS Rev. Proc. 2007-40, § 5.03 (June 25, 2007).

IRS officials.[152] According to IRS's Office of Chief Counsel, a recent court case that found that IRS does not have the authority to regulate the competency of paid preparers.[153]

Additionally, while IRS established six security, privacy, and business standards for online providers, including requirements for developing information privacy and security policies and reporting security incidents, the agency had not substantially updated them since January 1, 2010. To address these issues, we made eight recommendations to IRS. IRS agreed with our recommendations; however, as of January 2021, six of the eight recommendations had not been implemented.

- **Federal Student Aid (FSA) needs to provide consistent oversight of non-school partners' protection of student aid data.** FSA shares a variety of PII on borrowers with its non-school partners.[154] This includes names, addresses, phone numbers, email addresses, Social Security numbers, and financial information. We reported in September 2018 that FSA established oversight policies and procedures for loan servicers and private collection agencies that generally address key practices for overseeing the protection of PII shared with nonfederal entities. However, we found that FSA exercised minimal oversight of lenders' protection of student data (see table 7).[155]

---

[152]GAO, *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices,* GAO-19-340 (Washington, D.C.: May 9, 2019).

[153]Pursuant to 31 U.S.C. § 330(a)(1), IRS is authorized to "regulate the practice of representatives of persons before the Department of the Treasury," and the court held that return preparation does not constitute representing persons before IRS. *Loving v. IRS,* 917 F. Supp. 2d 67 (D.D.C. 2013), *aff'd*, 742 F.3d 1013 (D.C. Cir. 2014).

[154]FSA partners with various entities ("non-school partners") that are involved primarily in supporting the repayment and collection of student loans. They include federal loan servicers who are responsible for collecting payments on loans and providing customer service to borrowers on behalf of the Department of Education through its Direct Loan program, private collection agencies who collect loans that are in default and work with borrowers to help them get out of default, guaranty agencies who insure lenders against loss due to borrower default and carry out a variety of loan administration activities, and Federal Family Education Loan lenders who are nonfederal lenders, such as banks, credit unions, or other lending institutions, that made loans to students in the past and continue to service these loans.

[155]GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*, GAO-18-518 (Washington, D.C.: Sept. 17, 2018).

Table 7: Extent to Which Federal Student Aid's (FSA) Processes Addressed Key Practices for Overseeing the Protection of Personally Identifiable Information

Non-school partner	Security and privacy controls	Independent assessments	Corrective actions	Ongoing monitoring
Loan servicers	●	●	●	◖
Private collection agencies	●	●	●	◖
Guaranty agencies	◖	●	●	○
Federal Family Education Loan Lenders	◖	○	○	○

Key: ● = FSA provided evidence of processes and procedures that addressed all aspects of the key practice; ◖ = FSA provided evidence of processes and procedures that addressed some but not all aspects of the key practice; ○ = FSA did not provide evidence of processes and procedures that addressed the key practice

Source: GAO analysis of Federal Student Aid data. | GAO-21-288

FSA officials maintained that the lenders were subject to other legal and regulatory requirements for protecting customer data. However, FSA did not have a process for ensuring lenders were complying with these requirements, and thus lacked assurance that appropriate risk-based safeguards were being effectively implemented, tested, and monitored. To address these issues, we made six recommendations to FSA. The agency agreed with three, partially agreed with two, and did not agree with one recommendation. As of December 2020, none of these recommendations had been implemented.

- **Selected federal agencies need to strengthen online identity verification processes.** Remote identity proofing is the process federal agencies and other entities use to verify that the individuals who apply online for benefits and services are who they claim to be. To perform remote identity proofing, agencies have traditionally relied on consumer reporting agencies (CRAs) to conduct a procedure known as knowledge-based verification. This type of verification involves asking applicants seeking federal benefits or services personal questions derived from information found in their credit files, with the assumption that only the true owner of the identity would know the answers. If the applicant responds correctly, their identity is considered to be verified.

  However, data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently to respond to knowledge-based

verification questions. In particular, in August 2018,[156] we issued a report on the July 2017 Equifax data breach noting that hackers had accessed people's names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. While there was no breach of federal systems or information, agencies sought to determine which of their customers were directly affected by the breach, recognizing that those individuals could be at heightened risk of identity fraud.

We reported that agency officials had expressed concern about how the breached data could be used to compromise sensitive information or fraudulently procure government services, even from agencies that were not direct customers of Equifax. The risk that an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and impersonate that individual led NIST to issue guidance in 2017 that effectively prohibits agencies from using knowledge-based verification for sensitive applications.[157]

In May 2019,[158] we reported that several of our six selected agencies had taken steps to better ensure the effectiveness of their remote identity proofing processes, but only two had eliminated the use of knowledge-based verification.[159] Further, one selected agency, CMS, did not have plans to reduce or eliminate knowledge-based verification for remote identity proofing. To address these issues, we made six recommendations to six agencies.[160]

Most of the six agencies agreed with our recommendations; however, one agency did not state whether it agreed or disagreed with our recommendation and one agency disagreed with our recommendation. We believed our recommendation was warranted.

---

[156]GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

[157]NIST, *Digital Identity Guidelines,* SP 800-63-3 (Gaithersburg, Md.: June 2017)*; and Digital Identity Guidelines: Enrollment and Identity Proofing*, SP 800-63A (Gaithersburg, Md.: June 2017).

[158]GAO, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes,* GAO-19-288 (Washington, D.C.: May 17, 2019).

[159]We selected six agencies to review: CMS, GSA, IRS, Social Security Administration, United States Postal Service, and the Department of Veterans Affairs.

[160]We made recommendations to NIST, CMS, the Department of Veterans Affairs, OMB, the Social Security Administration, and the United States Postal Service.

As of December 2020, the agencies had implemented four of the six recommendations.

Our work has also highlighted the need for congressional action to improve federal efforts to protect privacy and sensitive data. For example:

- **Congress and Consumer Financial Protection Bureau (CFPB) should consider taking action to improve oversight of consumer reporting agencies protection of sensitive customer data**. CRAs collect, maintain, and sell to third parties large amounts of sensitive data about consumers, including Social Security numbers and credit card numbers. The Federal Trade Commission (FTC) and CFPB are the federal agencies primarily responsible for overseeing CRAs. In particular, the FTC enforces compliance with consumer protection laws under authorities provided in, among others, the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley Act (GLBA).[161] Since 2008, the FTC has settled 34 enforcement actions against various entities related to consumer reporting violations of the FCRA, including 17 actions against CRAs.

    However, as we reported in February 2019, FTC did not have civil penalty authority for violations of requirements under the GLBA, which, unlike FCRA, included a provision directing federal regulators and FTC to establish standards for financial institutions to protect against any anticipated threats or hazards to the security of customer records.[162] To obtain monetary redress for these violations, FTC must identify affected consumers and any monetary harm they may have experienced. However, harm resulting from privacy and security violations can be difficult to measure and can occur years in the future, making it difficult to trace a particular harm to a specific breach.

    In addition, according to CFPB staff, the bureau did not have authority to examine for or enforce the GLBA's safeguards provisions. After the Equifax breach, however, CFPB used its existing supervisory authority to examine the data security of certain CRAs. CFPB's process for prioritizing which CRAs to examine did not routinely include an assessment of companies' data security risks, but doing so could help CFPB better detect such risks and prevent the further exposure or compromise of consumer information.

---

[161]See 15 U.S.C. §§ 1681s(a)(1) and 6805(a)(7), respectively.

[162]GAO, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019).

To address these issues, we recommended that Congress consider giving FTC civil penalty authority to enforce GLBA's safeguarding provisions. We also made two recommendations to CFPB, including that it reassess its prioritization of examinations to address CRA data security. CFPB neither agreed nor disagreed with our recommendations. As of December 2020, the recommendations had not been implemented.

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 PII maintained by government agencies or on their behalf are protected both from inappropriate access (e.g., data breaches) as well as inappropriate use (e.g., 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.

Our prior work has highlighted the need for comprehensive legislation to govern this increased collection of personal information, including consumer information and facial images. Specifically:

- **Congress should consider developing legislation on internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving internet environment.** In January 2019, we reported that the United States does not have a comprehensive internet privacy law governing the collection, use, and sale or other disclosure of consumers' personal information.[163] At the federal level, two agencies have a role in overseeing internet privacy: FTC and FCC.

  - *FTC.* The FTC currently has the lead in overseeing internet privacy, using its statutory authority under the FTC Act to protect consumers from unfair and deceptive trade practices.[164] However, FTC has not issued regulations for internet privacy other than those protecting financial privacy and the internet privacy of children, which were required by law. For FTC Act violations, FTC may promulgate regulations, but it is required to use procedures

---

[163]GAO, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility,* GAO-19-52 (Washington, D.C.: Jan. 15, 2019).

[164]15 U.S.C. § 45(a)(1).

that differ from traditional notice-and-comment processes that FTC staff said add time and complexity.

- *FCC.* The FCC has had a limited role in overseeing internet privacy. From 2015 to 2017, FCC asserted jurisdiction over the privacy practices of internet service providers. In 2016, FCC promulgated privacy rules for internet service providers that Congress later repealed. FTC resumed privacy oversight of internet service providers in June 2018.

Stakeholders we interviewed had varied views on the current internet privacy enforcement approach and how it could be enhanced. Most internet industry stakeholders said they favored FTC's current approach—direct enforcement of its unfair and deceptive practices statutory authority, rather than promulgating and enforcing regulations implementing that authority. These stakeholders said that the current approach allows for flexibility and that regulations could hinder innovation. Other stakeholders, including consumer advocates and most former FTC and FCC commissioners we interviewed, favored having FTC issue and enforce regulations. Some stakeholders said a new data protection agency was needed to oversee consumer privacy. Stakeholders identified three main areas in which internet privacy oversight could be enhanced:

- *Statute.* Some stakeholders told us that an overarching internet privacy statute could enhance consumer protection by clearly articulating to consumers, industry, and agencies what behaviors are prohibited.

- *Rulemaking.* Some stakeholders said that regulations can provide clarity, enforcement fairness, and flexibility. Officials from two other consumer protection agencies said their rulemaking authority assists in their oversight efforts and works together with enforcement actions.

- *Civil penalty authority.* Some stakeholders said FTC's internet privacy enforcement could be more effective with authority to levy civil penalties for first-time violations of the FTC Act.

Accordingly, we suggested that Congress consider developing comprehensive legislation on internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving internet environment. As of December 2020, our suggestion had not been implemented.

- **Congress should consider strengthening the consumer privacy framework to reflect changes in facial recognition technology (FRT) and the marketplace**. FRT—which can be used to verify or

identify an individual from a facial image—has increasingly been used in commercial settings since our 2015 report on the topic.[165] More recently, in July 2020 we reported on concerns related to privacy and the use of facial recognition technology, such as the inability of individuals to remain anonymous in public or the use of the technology without individuals' consent. Some federal and state laws and the European Union's General Data Protection Regulation imposed requirements on U.S. companies related to facial recognition technology.[166] However, we reported that no federal law expressly regulated the commercial use of FRT, including the identifying and tracking of individuals.[167] Further, in most contexts, we found that federal law did not address how personal data derived from FRT may be used or shared.

Accordingly, we reiterated our previous suggestion from a 2013 report[168] that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace. As of December 2020, our suggestion had not been implemented.

We have also reported that agencies need to take additional steps to ensure that the collection and use of personal information by federal and nonfederal organizations is obtained with appropriate knowledge and consent. For example:

- **CFPB needs to update its model privacy notice form and consider including more information about third-party sharing.** Banks and credit unions collect, use, and share consumers' personal information—such as income level and credit card transactions—to conduct everyday business and market products and services. They

---

[165]GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015).

[166]Companies do not need a physical presence in the European Union to be covered under General Data Protection Regulation, according to European Data Protection Supervisor officials. These officials and a former individual with expertise in General Data Protection Regulation said that it would apply to (1) entities that are established in the European Union and (2) entities that do not have a presence in the European Union but offer services or goods to people in the European Union or monitor the data from subjects in the European Union.

[167]GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses,* GAO-20-522 (Washington, D.C.: July 13, 2020).

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

share this information with a variety of third parties, such as service providers and retailers.

The GLBA requires financial institutions to provide consumers with a privacy notice describing their information sharing practices.[169] Many banks and credit unions elect to use a model form—issued by regulators in 2009—which provides a safe harbor for complying with the law. However, we reported in October 2020 that the form gives a limited view of what information is collected and with whom it is shared.[170] Since Congress transferred authority to CFPB for implementing GLBA privacy provisions, the agency had not reassessed if the model form meets consumer expectations for disclosures of information sharing. CFPB officials said they had not considered a re-evaluation because they had not heard concerns from industry or consumer groups about privacy notices. However, our discussions with consumer and privacy groups showed that such concerns existed.

To address this issue, we made one recommendation to CFPB to update the model form and consider whether to include more comprehensive information about financial institutions sharing consumer personal information with third parties. CFPB neither agreed nor agreed with our recommendation. As of December 2020, the recommendation has not been implemented.

- **DHS's U.S. Customs and Border Protection (CBP) needs to ensure that its privacy notices for FRT are complete and available at locations using this technology, and that it develops a plan to audit its 27 airline partners**. In September 2020, we reported that, as of May 2020, CBP, in partnership with airlines, had deployed FRT to 27 airports to biometrically confirm travelers' identities as they depart the United States (air exit) and was in the early stages of assessing FRT at sea and land ports of entry.[171] CBP

---

[169]15 U.S.C. § 6803. In general, financial institutions must provide an initial privacy notice when a consumer becomes a customer (e.g., opens a new account), and annual notices thereafter for the duration of the customer relationship. Initial or annual notices may not be required in some cases, such as when disclosures are made only to process or service a transaction requested by the consumer or under other exceptions to GLBA's opt-out requirement. 12 C.F.R. §§ 1016.4-1016.6, 1016.8.

[170]GAO, *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions*, GAO-21-36 (Washington, D.C.: Oct. 22, 2020).

[171]GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: Sept. 2, 2020).

had taken steps to incorporate some privacy principles in its program, such as publishing the legislative authorities used to implement its program, but had not consistently provided complete information in privacy notices or ensured notices were posted and visible to travelers.

Further, CBP required its commercial partners, such as airlines, to follow CBP's privacy requirements and could audit partners to assess compliance. However, as of May 2020, CBP had audited only one of its more than 20 airline partners and did not have a plan to ensure all partners were audited. To address these and other issues, we made five recommendations to CBP. DHS concurred with our recommendations and described actions planned or underway to address them. As of December 2020, the recommendations had not been implemented.

Agency Comments

We requested comments on a draft of this report from DHS, NSC, and OMB. DHS provided technical comments, which we incorporated as appropriate. NSC staff and OMB's liaison to GAO both provided comments via email.

Specifically, NSC staff stated that, as the administration charts a course for cyber policy issues, the draft offered a comprehensive review of the cybersecurity challenges facing the nation and the opportunities available to make concrete improvements. Further, NSC staff stated that the administration's preliminary views about the four major cybersecurity challenges identified in our report were as follows:

- **Establishing a comprehensive cybersecurity strategy and performing effective oversight.** The administration will review the 2018 national cybersecurity strategy and its implementation plan. The administration will look for gaps in the existing strategy and the evolution of the cyber threat landscape in the intervening years, and will examine where updates are warranted.

- **Securing federal systems and information.** The administration is looking to take early action to secure federal systems and information. These efforts should improve the government's ability to prevent compromises, as well as its resilience and ability to respond quickly when intrusions occur.

- **Protecting cyber critical infrastructure.** The administration is also focused on enhancing cybersecurity protections for critical infrastructure. An early emphasis will be placed on interruptions to services that could pose serious risks to health and safety.

- **Protecting privacy and sensitive data.** The administration is committed to protecting privacy and sensitive data. Americans should have not just security but privacy as well. The administration will look for opportunities to improve privacy of data, especially in light of how threats and technologies continue to evolve.

In its comments, OMB highlighted ongoing and planned efforts that the office is taking for two major challenges. For example:

- **Securing federal systems and information.** With respect to the oversight and implementation of the FEDRAMP program, OMB stated that holding agencies accountable for complying with FedRAMP policies is paramount to standardize cloud security implementation. Further, OMB stated it is exploring options, such as gathering performance metrics to identify cloud services utilized by agencies and their compliance with FedRAMP.

  Regarding OMB's initiatives aimed at assisting agencies in managing cybersecurity and addressing challenges, OMB stated that it concurred with our prior recommendation in this area. OMB added that it intends to establish an interagency working group under the Chief Information Security Officer Council to allow for the exchange of ideas and approaches on cybersecurity risk management. OMB also noted that it will consider additional actions based on the findings of this working group.

- **Protecting privacy and sensitive data.** Regarding the need for federal agencies to coordinate on data protection requirements with states, OMB stated that, although there is not a requirement for agencies and the office to streamline cybersecurity requirements around data protection for state agencies, it appreciated that this effort would provide significant value to the states. It also added that such streamlining would help to provide a unified direction in cybersecurity from the federal government. In addition, OMB added that it and the CIO Council will review the recommendations further, talk with other agencies that are currently providing services for states, and evaluate the most direct and productive manner in which to engage state agencies.

We are sending copies of this report to appropriate congressional committees. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.
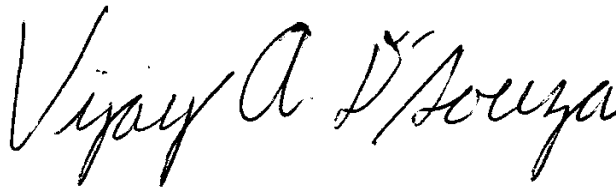
If you or your staffs have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov, or Jennifer R. Franks
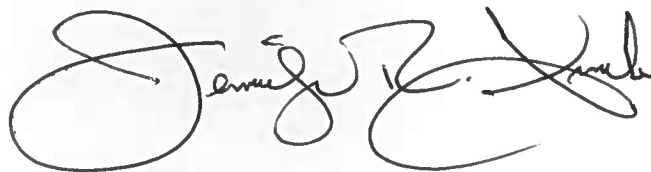
at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Nick Marinos
Director, Information Technology and Cybersecurity

Vijay A. D'Souza
Director, Information Technology and Cybersecurity

Jennifer R. Franks
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark R. Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Margaret Wood Hassan
Chairwoman
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Honorable Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology
House of Representatives

The Honorable Yvette D. Clarke
Chairwoman
Subcommittee on Cybersecurity, Infrastructure Protection,
 & Innovation
Committee on Homeland Security
House of Representatives

The Honorable Marsha Blackburn
United States Senate

The Honorable John Cornyn
United States Senate

The Honorable Angus S. King, Jr.
United States Senate

The Honorable Jim Langevin
House of Representatives

The Honorable Ben Sasse
United States Senate

The Honorable Thom Tillis
United States Senate

The Honorable Mike Gallagher
House of Representatives

Appendix I: Past GAO Reports Related to the Cybersecurity Major Challenges

Major challenge area	Critical action area	Related GAO reports
Major challenge 1: Establishing a comprehensive cybersecurity strategy and performing effective oversight	Action 1: Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	• *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236 (Washington, D.C.: Mar. 10, 2021). • *Cyber Diplomacy: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies*, GAO-21-266R (Washington, D.C.: Jan. 28, 2021). • *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020). • *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau*, GAO-20-607R (Washington, D.C.: Sept. 22, 2020). • *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, GAO-20-123 (Washington, D.C.: May 27, 2020).
	Action 2: Mitigate global supply chain risks.	• *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020). • *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: Nov. 24, 2020). • *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020). • *National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy*, GAO-21-155R (Washington, D.C.: Oct. 7, 2020). • *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).
	Action 3: Address cybersecurity workforce management challenges.	• *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities*, GAO-20-453 (Washington, D.C.: May 14, 2020). • *Federal Management: Selected Reforms Could Be Strengthened By Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: Apr. 23, 2020). • *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019). • *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019). • *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

Major challenge area	Critical action area	Related GAO reports
	Action 4: Ensure the security of emerging technologies.	• *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: Nov. 24, 2020). • *National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy*, GAO-21-155R (Washington, D.C.: Oct. 7, 2020). • *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020). • *Science & Tech Spotlight: Quantum Technologies*, GAO-20-527SP (Washington, D.C.: May 28, 2020). • *Science & Tech Spotlight: 5G Wireless*, GAO-20-412SP (Washington, D.C.: Mar. 26, 2020). • *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018). • *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017). • *Internet of Things: Status and implications of an increasingly connected world*, GAO-17-75 (Washington, D.C.: May 15, 2017).
Major challenge 2: Securing federal systems and information	Action 5: Improve implementation of government-wide cybersecurity initiatives.	• *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020). • *Information Technology: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed*, GAO-20-133 (Washington, D.C.: Feb. 4, 2020). • *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed*, GAO-20-126 (Washington, D.C.: Dec. 12, 2019). • *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019). • *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019). • *Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions*, GAO-19-105 (Washington, D.C.: Dec. 18, 2018).

Action 6: Address weaknesses in federal agency information security programs.	•	*Weapons Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*, GAO-21-179 (Washington, D.C.: Mar. 4, 2021).
	•	*Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-21-182 (Washington, D.C.: Dec. 23, 2020).
	•	*COVID-19: Urgent Actions Needed to Better Ensure an Effective Federal Response*, GAO-21-191 (Washington, D.C.: Nov. 30, 2020).
	•	*Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment*, GAO-20-252 (Washington, D.C.: Sept. 30, 2020).
	•	*COVID-19: Federal Efforts Could Be Strengthened by Timely and Concerted Actions*, GAO-20-701 (Washington, D.C.: Sept. 21, 2020).
	•	*Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020).
	•	*Information Technology: Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity*, GAO-20-691T (Washington, D.C.: Aug. 3, 2020).
	•	*Internet Protocol Version 6: DOD Needs to Improve Transition Planning*, GAO-20-402 (Washington, D.C.: June 1, 2020).
	•	*Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*, GAO-20-411R (Washington, D.C.: May 13, 2020).
	•	*Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241 (Washington, D.C.: Apr. 13, 2020).
	•	*Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program*, GAO-20-265 (Washington D.C.: Mar. 25, 2020).
	•	*Financial Audit: FY 2019 and FY 2018 Consolidated Financial Statements of the U.S. Government*, GAO-20-315R (Washington, D.C.: Feb. 27, 2020).
	•	*Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*, GAO-20-256T (Washington D.C.: Nov. 14, 2019).
	•	*Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019).
	•	*Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019).
	•	*Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: June 11, 2019).
	•	*2020 Census: Further Actions Needed to Reduce Key Risks to a Successful Enumeration*, GAO-19-431T (Washington, D.C.: Apr. 30, 2019).
	•	*Information Security: Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program*, GAO-19-70 (Washington, D.C.: Dec. 20, 2018).
	•	*Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions*, GAO-19-105 (Washington, D.C.: Dec. 18, 2018).
	•	*Weapon System Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

Major challenge area	Critical action area	Related GAO reports
	Action 7: Enhance the federal response to cyber incidents targeting federal systems.	• *Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve Its Program*, GAO-20-265 (Washington, D.C.: Mar. 25, 2020). • *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019). • *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, GAO-18-559 (Washington, D.C.: Aug. 30, 2018).
Major challenge 3: Protecting the cybersecurity of critical infrastructure	Action 8: Strengthen the federal role in protecting the cybersecurity of critical infrastructure.	• *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021). • *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020). • *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Washington, D.C.: Sept. 17, 2020). • *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities*, GAO-20-453 (Washington, D.C.: May 14, 2020). • *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices*, GAO-20-404 (Washington, D.C.: Apr. 3, 2020). • *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Feb. 25, 2020). • *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, GAO-20-267 (Washington, D.C.: Feb. 6, 2020). • *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019). • *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

Major challenge area	Critical action area	Related GAO reports
Major challenge 4: Protecting privacy and sensitive data	Action 9: Improve federal efforts to protect privacy and sensitive data.	• *Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans*, GAO-21-25 (Washington, D.C.: Feb. 11, 2021).
		• *2020 Census: The Bureau Concluded Field Work but Uncertainty about Data Quality, Accuracy, and Protection Remain*, GAO-21-206R (Washington, D.C.: Dec. 9, 2020).
		• 2020 Census: Census Bureau Needs to Assess Data Quality Concerns Stemming from Recent Design Changes, GAO-21-142 (Washington, D.C.: Dec. 3, 2020).
		• *Financial Audit: IRS's FY 2020 and FY 2019 Financial Statements*, GAO-21-162 (Washington, D.C.: Nov. 10, 2020).
		• *Data Security: Recent K-12 Data Breaches Show that Students are Vulnerable to Harm*, GAO-20-644 (Washington, D.C.: Sept. 15, 2020).
		• *Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities*, GAO-20-431 (Washington, D.C.: Sept. 21, 2020).
		• *2020 Census: Recent Decision to Compress Census Timeframes Poses Additional Risks to an Accurate Count*, GAO-20-671R (Washington, D.C.: Aug. 27, 2020).
		• *2020 Census: COVID-19 Presents Delays and Risks to Census Count*, GAO-20-551R (Washington, D.C.: June 9, 2020).
		• *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*, GAO-20-123 (Washington, D.C.: May 27, 2020).
		• *Consumer Reporting Agencies: CFPB Should Define Its Supervisory Expectations*, GAO-19-459 (Washington, D.C.: July 16, 2019).
		• *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, GAO-19-288 (Washington, D.C.: May 17, 2019).
		• *Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices*, GAO-19-340 (Washington, D.C.: May 9, 2019).
		• *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*, GAO-19-230 (Washington, D.C.: Mar. 27 2019).
		• *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019).
		• *Cybersecurity: Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information*, GAO-19-114R (Washington, D.C.: Dec. 6, 2018).
		• *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*, GAO-18-518 (Washington, D.C.: Sept. 17, 2018).
		• *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

Major challenge area	Critical action area	Related GAO reports
	Action 10: Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.	• *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions*, GAO-21-36 (Washington, D.C.: Oct. 22, 2020). • *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: Sept. 2, 2020). • *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020). • *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020). • *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Washington, D.C.: Jan. 15, 2019). • *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015). • *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

Source: GAO. | GAO-21-288

Appendix II: Ongoing GAO Work Related to the Cybersecurity Major Challenges

Major challenge area	Critical action area	Related ongoing GAO work
Major challenge 1: Establishing a comprehensive cybersecurity strategy and performing effective oversight	Action 1: Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	There are two ongoing reviews related to this action area, including reviews of: • the strategy and effectiveness of federal government's efforts to build the capacity of allies and partner nations to combat cybercrime; and • federal assistance provided to states for ransomware[a] incident protection and response.
	Action 2: Mitigate global supply chain risks.	There is one ongoing review related to this action area; specifically, a review related to the recent supply chain compromise of a widely used back-end information technology (IT) management software, including what steps federal agencies are taking and what remains to be done to coordinate and respond to the incident.
	Action 3: Address cybersecurity workforce management challenges.	There is one ongoing review related to this action area; specifically, a review related to the Department of State's IT workforce.
	Action 4: Ensure the security of emerging technologies.	There are three ongoing reviews related to this action area, including reviews of: • the Department of Defense's (DOD) artificial intelligence (AI) capabilities and strategy; • what tools and practices, consistent with our auditing and internal controls standards, can be applied in third-party assessments and audits to assure complete, accurate, and valid information processing of AI systems; and • the potential applications of quantum computing and communications technologies, including the potential benefits and drawbacks from their development and use.
Major challenge 2: Securing federal systems and information	Action 5: Improve implementation of government-wide cybersecurity initiatives.	There are two ongoing reviews related to this action area, including reviews of: • the reported effectiveness of federal agencies' implementation of cybersecurity policies and practices; and • the extent to which selected agencies addressed federal information security guidance when implementing their IT telework solutions.

Major challenge area	Critical action area	Related ongoing GAO work
	Action 6: Address weaknesses in federal agency information security programs.	There are 13 ongoing reviews related to this action area, including reviews of: • the extent to which the Department of the Treasury has implemented information security controls for the data that agencies submit under the Digital Accountability and Transparency Act of 2014; • whether the National Nuclear Security Administration and its contractors implemented organizational risk management practices to address the risks in the three cybersecurity environments; • the extent to which the National Institutes of Health implemented information security to effectively protect the confidentiality, integrity, and availability of its information on selected information systems; • what roles and responsibilities has the Department of Health and Human Services defined for its entities to manage cybersecurity within the department; • whether the Department of State has an effective process for responding to and recovering from incidents, to include the resources necessary for handling security breaches; • whether the Office of Personnel Management's modernization program adopted leading IT management practices in requirements management, cost and schedule estimation, and cybersecurity; • the Census Bureau's innovations for the 2020 Census, including efforts to mitigate cybersecurity risks and ensure the privacy of the data collected; • the extent to which DOD has included and implemented industry practices to enhance the organization-wide management of cybersecurity risks; • the extent to which the Defense Logistics Agency implemented key risk management practices to address cybersecurity risks to its inventory management systems; • the extent to which each of DOD's components have implemented cyber hygiene practices; • whether the Internal Revenue Service maintains effective internal control over financial reporting; • the risks and challenges associated with DOD's major IT program's software development and cybersecurity practices; and • DOD's financial management system governance and management.
	Action 7: Enhance the federal response to cyber incidents targeting federal systems.	There are two ongoing reviews related to this action area, including reviews of: • the federal response to the significant cyberattack campaign discovered in December 2020; and • DOD's cyber incident management.

Major challenge area	Critical action area	Related ongoing GAO work
Major challenge 3: Protecting the cybersecurity of critical infrastructure	Action 8: Strengthen the federal role in protecting the cybersecurity of critical infrastructure.	There are five ongoing reviews related to this action area, including reviews of: • the extent to which DOD has included and implemented practices to enhance the organization-wide management of cybersecurity risks to DOD utilities, and conducted security control tests of selected systems; • the key security risks to the internet architecture and to what extent have U.S. federal agencies taken actions to address security risks to the internet architecture; • DOD's implementation of the Cybersecurity Maturity Model Certification; • the insurance coverage available for losses related to cyber risk, including cyber terrorism, and if the Terrorism Risk Insurance Program[b] is effective for insuring critical infrastructure against events like cyberattacks and cyber terrorism; and • communications sector cybersecurity risks.
Major challenge 4: Protecting privacy and sensitive data	Action 9: Improve federal efforts to protect privacy and sensitive data.	There are five ongoing reviews related to this action area, including reviews of: • the extent to which the Department of Homeland (DHS) has developed policies and procedures for the protection of personally identifiable information (PII) and what actions it takes to ensure that data breaches involving PII are identified and remediated in a timely manner; • the extent to which the Census Bureau's policies and procedures for managing and protecting PII align with federal requirements and guidance; • the programs and activities at key federal agencies to protect personal information and the privacy, civil rights, and civil liberties of Americans; • the extent to which federal financial regulators collect, use, and share PII and ensure the privacy of PII in accordance with federal requirements and guidance; and • to what extent federal law enforcement agencies track their use of external systems with facial recognition technology.
	Action 10: Appropriately Limit the Collection and Use of Personal Information and Ensure That It Is Obtained with Appropriate Knowledge or Consent	There is one ongoing review related to this action area; specifically, a review of federal agencies' privacy programs.

Source: GAO. | GAO-21-288

[a]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.

[b]The Terrorism Risk Insurance Program was created by the Terrorism Risk Insurance Act in 2002 and was reauthorized most recently in 2019. It is a temporary program to provide a system of public and private compensation for certain insured losses resulting from a certified act of terrorism.

[c]The Cybersecurity Maturity Model Certification assesses cybersecurity maturity processes and cybersecurity best practices drawn from existing cybersecurity standards and other frameworks and references. The framework includes, among other things, five levels of cybersecurity best practices, such as Level 1 "basic cyber hygiene;" Level 2 "intermediate cyber hygiene;" and Level 3 "good cyber hygiene."

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts	Nick Marinos, (202) 512-9342 or marinosn@gao.gov
	Vijay A. D'Souza, (202) 512-6240 or dsouzav@gao.gov
	Jennifer R. Franks, (404)-679-1831 or franksj@gao.gov
Staff Acknowledgments	In addition to the contacts named above, individuals making contributions to this report included Kaelin Kuhn (Assistant Director), Sukhjoot Singh (Analyst in Charge), Anna Bennett, Kiana Beshir, Christopher Businsky, John deFerrari, Linda Erickson, Rebecca Eyler, Keith Kim, Hoyt Lacy, Catherine Maloney, and Carlo Mozo.