United States Government Accountability Office

Testimony

Before the Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, December 2, 2021

CYBERSECURITY

Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure

Statement of Nick Marinos, Director,
Information Technology and Cybersecurity

Chairman DeFazio, Ranking Member Graves, and Members of the Committee:

Thank you for the opportunity to contribute to today's discussion on federal perspectives to secure the nation's infrastructure. As you know, our nation's critical infrastructure sectors are dependent on information technology (IT) systems and digital data to carry out operations and to process, maintain, and report essential information.[1] The security of these systems and data is vital to public confidence and national security, prosperity, and well-being.

We have long stressed the urgent need for effective cybersecurity, as underscored by increasingly sophisticated threats and frequent cyber incidents.[2] Recent events, including the ransomware attack that led to a shutdown of a major U.S. fuel pipeline, have illustrated that the nation's critical infrastructure and the federal government's IT systems continue to face growing cyber threats.[3] The cybersecurity of critical infrastructure sectors has been a long-standing challenge for the federal government, underscored by the need for federal agencies to improve their own cybersecurity posture and enhance the cybersecurity support provided to the nation's critical infrastructure.

[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 policies identify 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2] See, for example, GAO, *Cybersecurity and Information Technology: Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas*, GAO-21-105325 (Washington, D.C.: July 28, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[3] For more information regarding such recent events, see GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks*, GAO-21-594T (Washington, D.C.: May 25, 2021). 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.

At your request, my remarks today will focus on the federal government's efforts to address the cybersecurity of the nation's critical infrastructure and will highlight critical areas where we have identified an urgent need for improvement. This statement is based on the results of our prior work, which includes the reports and testimonies that we cite throughout this statement. To develop the statement, we reviewed prior reports and testimonies that described cyber-related challenges faced by the nation and the extent to which federal entities have taken actions to address them. More detailed information about our scope and methodology can be found in the products cited throughout this statement.

We conducted the work on which this statement is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

Background

Information systems supporting federal agencies and our nation's critical infrastructure—such as transportation systems, communications, education, energy, and financial services—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 *2021 Annual 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.[4] According to the 2020 assessment, both criminal groups and nation cyber actors—motivated by profit, espionage, or disruption—will exploit the Coronavirus Disease 2019 (COVID-19) pandemic by targeting the U.S. health care and public health sector, government response entities, and the broader emergency services sector.

Recent events highlight the significant cyber threats facing the nation. For example,

- In May 7, 2021, the Colonial Pipeline Company learned that it was the victim of a cyberattack. A joint alert from the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) indicated that malicious actors used ransomware against Colonial Pipeline’s information technology network.[5] The alert also explained that, to ensure the safety of the pipeline, the company disconnected certain industrial control systems that monitor and control physical pipeline functions so that they would not be compromised by the criminals. According to CISA and the FBI, as of May 11, 2021, there was no indication that the threat actors had compromised the industrial control

[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (April 9, 2021). Department of Homeland Security, *Homeland Threat Assessment* (October 6, 2020).

[5] CISA and the FBI, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Alert (AA21-131A), May 11, 2021.

systems. However, disconnecting these systems resulted in a temporary halt to all pipeline operations. This, in turn, led to gasoline shortages throughout the southeast United States.

- 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. According to CISA, threat actors likely accessed systems by exploiting cybersecurity weakness, including poor password security and an outdated operating system.

- In December 2020, 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.

GAO Has Previously Identified Four Major Cybersecurity Challenges Facing the Nation

To underscore the importance of this issue, we have designated information security as a government-wide high-risk area since 1997.[6] In 2003, we added the protection of critical

[6] GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: Feb. 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies

infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.[7]

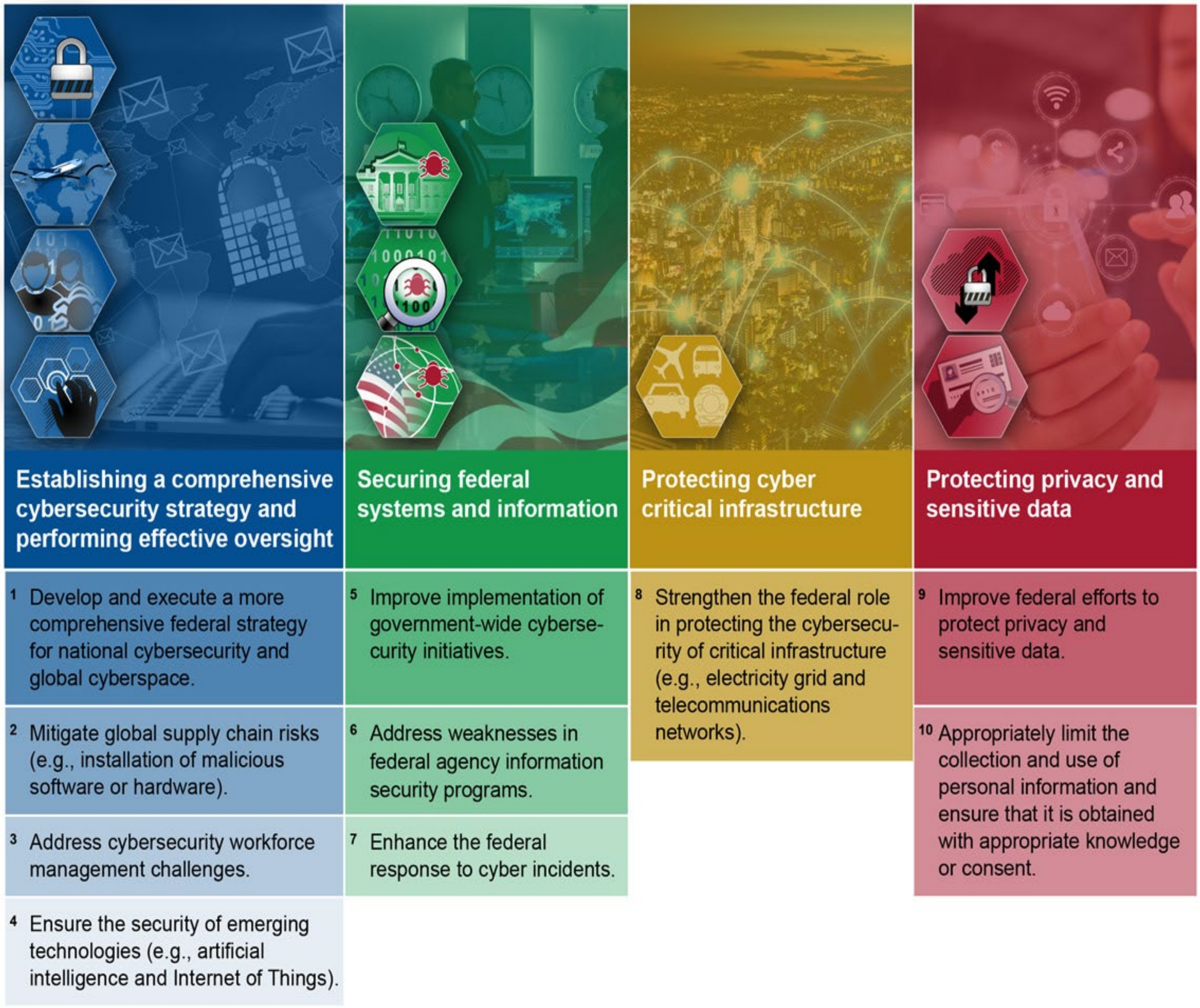
In our high-risk updates from September 2018 and March 2021, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government faces.[8] These challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Figure 1 provides an overview of the critical actions needed to address these major cybersecurity challenges.

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.

[7] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015) and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: Jan. 2003).

[8] GAO-21-288 and GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

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



Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

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.

Protecting cyber critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-22-105530

Since 2010, we have made about 3,700 recommendations related to our high-risk area focused on enhancing our nation’s cybersecurity efforts. As of November 2021, about 900 of those recommendations had yet to be implemented.

As indicated by the figure above, these recommendations include but also extend far beyond topics related to critical infrastructure cybersecurity, representing work across all of the high-risk challenge areas and calling for urgent actions to help address them. The following examples reflect the wide range of challenge areas:

- **Cybersecurity workforce management.** In December 2020, we reported that the U.S. Department of Transportation's (DOT) workforce faced challenges related to overseeing the safety of automated technologies, such as those that control a function or task of a plane, train, or vehicle without human intervention.[9] These technologies require regulatory expertise as well as engineering, data analysis, and cybersecurity skills. Although DOT had identified most skills it needed to oversee automated technologies, it had not fully assessed whether its workforce had these skills. Accordingly, we recommended that DOT (1) assess skill gaps in key occupations involved in overseeing automated technologies and (2) regularly measure the progress of strategies implemented to close skill gaps. As of November 2021, these recommendations had not yet been fully implemented, although DOT reported it intended to so by June 2022.
- **Government-wide cybersecurity initiatives.** Federal agencies face cyber threats against that continue to grow in number and sophistication. 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. In August 2020, we reported that selected agencies—the Federal Aviation Administration (FAA), Indian Health Services, and Small Business Administration—had generally deployed these tools intended to provide cybersecurity data to support the

[9] GAO, *Automated Technologies: DOT Should Take Steps to Ensure Its Workforce Has Skills Needed to Oversee Safety*, GAO-21-197 (Washington, D.C.: Dec. 18, 2020).

Department of Homeland Security's (DHS) CDM program.[10] 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 November 2021, only one of the recommendations made to DHS had been implemented.

- **Federal agency cybersecurity risk management.** 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.[11] 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 (1) establishing a cybersecurity risk management strategy to delineate boundaries for risk-based decisions; (2) establishing a process for assessing agency-wide cybersecurity risks; and (3) establishing a process for coordinating between cybersecurity and enterprise risk management programs for managing all major risks.[12] We made 57 recommendations to the 23 agencies to address the

[10] 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).

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

[12] 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.

challenges identified in our report. As of November 2021, 25 of these recommendations had yet to be implemented.

Federal Law and Policy Establish Requirements for Critical Infrastructure Cybersecurity

Federal law and policy establish roles and responsibilities for the protection of critical infrastructure, discussed in chronological order.

- **Executive Order 13636.** In February 2013, the White House issued *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, which called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing.[13] To do so, the order established mechanisms for promoting engagement between federal and private organizations. Among other things, the order designated nine federal sector-specific agencies with lead roles in protecting critical infrastructure sectors. The lead agencies coordinate federally sponsored activities within their respective sectors. Further, the order directed DHS, with help from the lead agencies, to identify, annually review, and update a list of critical infrastructure sectors for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security.

- **Presidential Policy Directive 21.** Also, in February 2013, the White House issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, to further

[13] The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013), 78 Fed. Reg. 11739 (Feb. 19, 2013).

specify critical infrastructure responsibilities.[14] Among other things, the policy directed DHS to coordinate with lead agencies to develop a description of functional relationships across the federal government related to critical infrastructure security and resilience. The policy further prescribed DHS, in coordination with lead agencies, to conduct an analysis and recommend options for improving public-private partnership effectiveness.

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework.** Executive Order 13636 directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes.[15] Further, the order directed the lead agencies, in consultation with DHS and other interested agencies, to coordinate with critical infrastructure partners to review the cybersecurity framework. The agencies, if necessary, should develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

In response to the order, in February 2014, NIST first published its framework—a voluntary, flexible, performance-based framework of cybersecurity standards and procedures. The framework, which was updated in April 2018, outlines a risk-based approach to managing cybersecurity that is composed of three major parts: a framework core, profiles, and

[14] The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*, (Washington, D.C.: Feb. 12, 2013).

[15] The Cybersecurity Enhancement Act of 2014 authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure. 15 U.S.C. § 272(c)(15). *The Framework for Improving Critical Infrastructure Cybersecurity* represents that voluntary set of standards.

implementation tiers.[16] The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes.

- **Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018.** The November 2018 act established CISA,[17] within DHS, to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.

- **National Defense Authorization Act (NDAA) for Fiscal Year 2021.** The act established roles and responsibilities for lead agencies, known as sector risk management agencies, in protecting the 16 critical infrastructure agencies.[18] According to the act, the lead agencies are required to (1) coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) support sector risk management, in coordination with CISA; (3) assess sector risk, in coordination with CISA; (4) coordinate the sector, including by serving as a day-to-day federal interface for the prioritization and

[16] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 2018).

[17] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169, (Nov. 16, 2018) (codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[18] The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 states that the term "sector risk management agency" replaces the term "sector-specific agency" in the Homeland Security Act of 2002. The NDAA amends the Homeland Security Act of 2002 and sets out sector risk management agency responsibilities within this critical infrastructure framework. Pub. L. No. 116-283, § 9002, 134 Stat. 3388, 4768 (Jan. 1, 2021).

coordination of sector-specific activities; and (5) support incident management, including supporting CISA, upon request, in asset response activities.

Federal Actions Urgently Needed to Protect Critical Infrastructure from Cyber Threats

Over the last several decades, we have emphasized the urgent need for the federal government to improve its ability to protect against cyber threats to our nation's infrastructure. In recent high-risk updates, we emphasized the critical need for the federal government to address major cybersecurity challenges through critical actions. This includes the need for the federal government to (1) develop and execute a comprehensive national cyber strategy and (2) strengthen the federal role in protecting the cybersecurity of critical infrastructure.

Executive Branch Urgently Needs to Establish and Implement a Comprehensive National Cyber Strategy

We and others have reported on the challenges in establishing a comprehensive national strategy to guide how the United States government will engage both domestically and internationally on cybersecurity related matters. In September 2020, we reported that the prior administration's 2018 *National Cyber Strategy*[19] and associated 2019 *Implementation Plan* had collectively detailed the executive branch's approach to managing the nation's cybersecurity. However, these documents only addressed some, but not all, of the desirable characteristics of national strategies,

[19] The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

such as goals and resources needed.[20] Accordingly, we recommended that the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include goals and resource information, among other things.[21] The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it.

We have also stressed the urgency and necessity of clearly defining a central leadership role in order to coordinate the government's efforts to overcome the nation's cyber-related threats and challenges. In September 2020, we also reported that, in light of the elimination of the White House Cybersecurity Coordinator position in May 2018, it was unclear which official within the executive branch ultimately maintained responsibility for coordinating the execution of the National Cyber Strategy and related implementation plan. Accordingly, we suggested that Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, the NDAA for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President.[22] Among other responsibilities, the Director is to serve as the principal advisor to the White House on cybersecurity policy and strategy, including coordination of implementation of national cyber policy and strategy.

In June 2021, the Senate confirmed a Director to lead this new office. In October 2021, the National Cyber Director issued a strategic intent statement, outlining a vision for the Director's office and the high-level lines of efforts it intends to focus on, including national and federal

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

[21] The *National Cyber Strategy* assigns National Security Council staff to coordinate with departments, agencies, and the Office of Management and Budget on a plan to implement the strategy.

[22] Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 4144 (Jan. 1, 2021) (codified at 6 U.S.C. § 1500).

cybersecurity; budget review and assessment; and planning and incident response, among others.[23]

The establishment of a National Cyber Director is an important step toward positioning the federal government to better direct activities to overcome the nation's cyber threats and challenges and to perform effective oversight. Nevertheless, the implementation of our recommendation to fully develop and execute a comprehensive national cyber strategy remains more urgent than ever to ensure that there is a clear roadmap for overcoming the cyber challenges facing our nation, including its critical infrastructure.

Federal Government Needs to Strengthen Its Role in Protecting the Cybersecurity of Critical Infrastructure

The federal government has been challenged in working with the private sector to protect cyber critical infrastructure. We have made recommendations aimed at strengthening the federal role in critical infrastructure cybersecurity, including by (1) enhancing the capabilities and services of DHS' Cybersecurity and Infrastructure Security Agency and (2) ensuring that federal agencies with sector-specific responsibilities are providing their sector partners with effective guidance and support.

DHS Needs to Complete CISA Transformation Activities to Better Support Critical Infrastructure Owners and Operators

The importance of clear cybersecurity leadership extends beyond the White House to other key executive branch agencies, including DHS. Federal legislation enacted in November 2018 established CISA within the department to advance the mission of protecting federal civilian

[23] The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, D.C.: Oct. 28, 2021).

agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats. 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.[24]

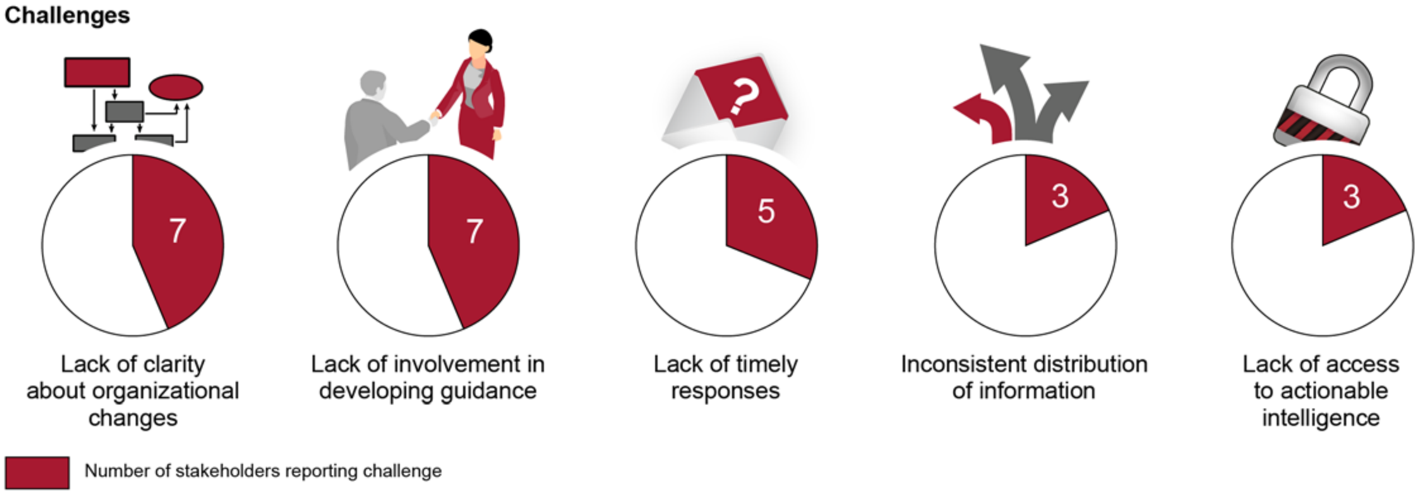
To implement the statutory requirements, CISA leadership launched an organizational transformation initiative. In March 2021, we reported that while CISA had completed the first two of the three phases of its organizational transformation initiative.[25] Specifically, we noted DHS had not fully implemented its phase three transformation, which included finalizing the agency's mission-essential functions and completing workforce-planning activities, that was intended to be completed by December 2020.

We also reported that of 10 selected key practices for effective agency reforms we previously identified, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. Further, we reported on a number of challenges that selected government and private-sector stakeholders had noted when coordinating with CISA, including a lack of clarity surrounding its organizational changes and the lack of stakeholder involvement in developing guidance. 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. Figure 2 below describes the coordination challenges identified by private-sector stakeholders.

[24] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2,132 Stat. 4168, 4169, (Nov. 16, 2018)(codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[25] 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).

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



Source: GAO analysis of stakeholder interviews. | GAO-22-105530

To address these weaknesses, we made 11 recommendations to DHS. The department concurred with our recommendations and, as of September 2021, reported that it intends to fully implement them by the end of calendar year 2022. Implementing these recommendations will better position CISA to ensure the success of its reorganization efforts and carry out its mission to lead national efforts to identify and respond to cyber and other risks to our nation's infrastructure.

Sector Risk Management Agencies Need to Ensure Effective Guidance and Support of Critical Infrastructure Owners and Operators

Since 2010, we have made about 80 recommendations for various federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the NIST framework of voluntary cyber standards and correct sector-specific weaknesses. Specifically, we reported that most sector lead agencies—known as sector risk management agencies[26]—were not collecting and reporting on improvements in the

[26] Sector-specific agencies was a term formally used to describe the nine agencies that have a lead role in protecting the 16 critical infrastructure sectors. Pursuant to the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002, any reference to sector-

protection of critical infrastructure as a result of using the framework across the sectors.[27] We concluded that collecting and reporting on these improvements would help the sectors understand the extent to which sectors are better protecting their critical infrastructure from cyber threats.

To address these issues, we made 10 recommendations—one to NIST on establishing time frames for completing selected programs—and nine to the lead agencies, to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. However, as of November 2021, none of the recommendations had been implemented. Until the lead agencies collect and report on improvements gained from adopting the framework, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructure from threats will be largely unknown.

We have also frequently reported on the need for lead agencies to enhance the cybersecurity of their related critical infrastructure sectors and subsectors—such as transportation systems, communications, energy, education, and financial services.[28]

- **Aviation.**[29] The Federal Aviation Administration (FAA) is responsible for overseeing the safety of commercial aviation, including avionics systems. The growing connectivity between airplanes and these systems may present increasing opportunities for cyberattacks on commercial planes. In October 2020, we reported that FAA had established a process for

specific agencies in any law, regulation, document, or other paper of the United States shall be deemed a reference to the sector risk management agency of the relevant critical infrastructure sector.

[27] GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Apr. 9, 2020).

[28] GAO-21-288.

[29] The transportation systems sector consists of seven key subsectors, including aviation.

certification and oversight of U.S. commercial airplanes, including their operations.[30] However, FAA had not prioritized risk-based cybersecurity oversight or included periodic testing as part of its monitoring process, among other things. To address these and other related issues, we made six recommendations to FAA; however, as of November 2021, the agency had not implemented the recommendations.

- **Mass Transit and Passenger Rail.**[31] Recent physical and cyberattacks on rail systems in U.S. and foreign cities highlight the 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).[32] TSA uses these risk assessments to evaluate threat, vulnerability, and consequence for attack scenarios across various transportation modes. In April 2020, we reported[33] 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

[30] 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).

[31] The transportation systems sector consists of seven key subsectors, including mass transit and passenger rail.

[32] 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.

[33] 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).

NIST's Cybersecurity Framework,[34] nor did it include the framework in a list of available cyber resources.[35] 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 November 2021, one recommendation had not been implemented.

- **Pipeline Systems.**[36] The nation depends on the interstate pipeline system to deliver critical resources such as oil and natural gas. This increasingly computerized system is an attractive target for hackers and terrorists. In December 2018, we found weaknesses in the Transportation Security Administration's (TSA) management of its pipeline security efforts.[37] We reported that TSA, a component agency of DHS, had issued revised pipeline security guidelines; however, the revisions did not include all elements from the NIST Cybersecurity Framework and did not include clear definitions to ensure the identification of critical facilities by pipeline operators.[38] We also reported that the agency had conducted pipeline security reviews to assess pipeline systems vulnerabilities; however, the quantity of

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

[35] 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.

[36] The transportation systems sector consists of seven key subsectors, including pipeline systems.

[37] 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).

[38] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0 (Gaithersburg, MD: Feb. 12, 2014).

TSA's reviews of corporate and critical facilities security had varied considerably. To address these and other issues we made 10 recommendations to TSA. The agency agreed with all of our recommendations. In July 2021, we testified that the TSA had not fully addressed pipeline cybersecurity-related weaknesses that GAO had previously identified, such as aged protocols for responding to pipeline security incidents.[39] As of November 2021, TSA had implemented 10 of the 13 recommendations from 2018 and 2019 and had not implemented three.

- **Communications.** The Communications sector is an integral component of the U.S. economy and faces serious cyber-related threats that could affect the operations of local, regional, and national level networks. In November 2021, we reported that CISA has a leadership role in coordinating federal efforts intended to aid in the resilience of the Communications Sector.[40] The agency fulfills its responsibilities to private sector owners and operators through a variety of programs and services, including incident management and information sharing. We found CISA had not assessed the effectiveness of these activities, nor updated a strategic sector guidance document, despite being recommended by DHS to do so every 4 years. Specifically, the current plan, from 2015, lacks information on new and emerging threats to the Communications Sector, such as security threats to the communications technology supply chain. Developing and issuing updated guidance would enable CISA to set goals, objectives, and priorities that address threats and risks to the sector, and help meet its sector risk management agency responsibilities. As such, we made three

[39] GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, GAO-21-105263 (Washington, D.C.: July 27, 2021).

[40] GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, GAO-20-104462 (Washington, D.C.: Nov. 23, 2021).

recommendations to CISA, including that the agency assess the effectiveness of support provided to sector, and revise the sector plan to include, among other things, new and emerging threats and risks. DHS concurred with the recommendations and described initial actions under way or planned to address them in a 2021 letter in response to our report.

- **Energy.** The U.S. grid's distributing systems—which carry electricity from transmission systems to consumers and are regulated primarily by states—are increasingly at risk from cyberattacks. In August 2019, we reported that the electric grid faced various cybersecurity risks.[41] We noted that the Department of Energy (DOE) had developed plans and an assessment to address the risks. However, these documents did not fully address all of the key characteristics of a national strategy. Subsequently, in March 2021, we reported that the electric grid's distribution systems continued to face various cybersecurity risks.[42] DOE had developed plans and an assessment to address the risks to the electric grid; however, these documents did not fully address risks to the grid's distribution systems. To mitigate this issue, we recommended that the department more fully address cyber risks to the grid's distribution systems in its plans to implement the national cybersecurity strategy for the grid. DOE agreed with our recommendation; however, as of November 2021, the department had not implemented our recommendation.

- **Education.** When the COVID-19 pandemic forced the closure of schools across the nation, many kindergarten through grade 12 (K-12) schools moved from in-person to remote

[41] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).
[42] GAO, *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, D.C.: Mar. 18, 2021).

education, increasing their dependence on IT and making them potentially more vulnerable to cyberattacks. In October 2021, we reported that the Department of Education's sector-specific plan for the Education Facilities subsector had not been updated since 2010 and did not reflect substantially changed cybersecurity risks affecting K-12 schools.[43] Further, Education had not determined whether sector-specific guidance was needed for K-12 schools to help protect against cyber threats, including against the increasing threat of ransomware attacks. To address these issues, we recommended that Education initiate a meeting with CISA to determine how to update its sector-specific plan and determine whether sector-specific guidance is needed. Education concurred with GAO's recommendations and described actions that it would take to address them.

- **Financial Services.** The federal government has long identified the financial services sector as a critical component of the nation's infrastructure. In September 2020, we reported that the Department of the Treasury and other federal agencies were taking steps to reduce risks and bolster the financial sector's efforts to improve its cybersecurity.[44] However, Treasury had not worked with other federal agencies and sector partners to better measure progress and to prioritize efforts in line with sector cybersecurity goals laid out in the implementation plan of the 2018 *National Cyber Strategy*. To address these issues, we made two recommendations to Treasury. The department agreed with our recommendations; however, as of November 2021, Treasury had not implemented the recommendations.

[43] GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats,* GAO-22-105024 (Washington, D.C.: Oct. 13, 2021).

[44] 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).

Overall, federal agencies have not addressed most of our recommendations related to protecting critical infrastructure.[45] About 50 of the about 80 recommendations made in our public reports since 2010 have not been implemented, as of November 2021. We also designated 14 of these as priority recommendations; as of November 2021, 11 had not been implemented. Until our recommendations are fully addressed, federal agencies will not be effectively positioned to ensure critical infrastructure sectors are adequately protected from potentially harmful cybersecurity threats.

In summary, the federal government needs to move with a greater sense of urgency in response to the serious cybersecurity threats faced by the nation and its critical infrastructure. This would include developing and executing a comprehensive national strategy and strengthening the federal role in protecting the cybersecurity of critical infrastructure. Without implementing our recommendations, the federal government will continue to be hindered in its ability to provide effective support to the cybersecurity of the nation's critical infrastructure. As a result, the risk of unprotected infrastructure being harmed is heightened.

Chairman DeFazio, Ranking Member Graves, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Nick Marinos, Director of Information Technology and Cybersecurity, at (202) 512-9342 or

[45] GAO-21-288.

marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony included Kush K. Malhotra (Assistant Director), Chris Businsky, Donna Epler, Hiama Halay, Kaelin Kuhn, Scott Pettis, Sukhjoot Singh, Kevin Smith, and Umesh Thakkar (Analyst in Charge).

(105530)