United States Government Accountability Office

Report to Congressional Requesters

September 2020

CYBERSECURITY

Clarity of Leadership Urgently Needed to Fully Implement the National Strategy

Accessible Version

GAO-20-629

September 2020

CYBERSECURITY

Clarity of Leadership Urgently Needed to Fully Implement the National Strategy

GAO Highlights

Highlights of GAO-20-629, a report to congressional requesters

Why GAO Did This Study

Increasingly sophisticated cyber threats have underscored the need to manage and bolster the cybersecurity of key government systems and the nation's cybersecurity. The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. In 2018, GAO noted that the need to establish a national cybersecurity strategy with effective oversight was a major challenge facing the federal government.

GAO was requested to review efforts to protect the nation's cyber critical infrastructure. The objectives of this report were to (1) describe roles and responsibilities of federal entities tasked with supporting national cybersecurity, and (2) determine the extent to which the executive branch has developed a national strategy and a plan to manage its implementation.

To do so, GAO identified 23 federal entities responsible for enhancing the nation's cybersecurity. Specifically, GAO selected 13 federal agencies based on their specialized or support functions regarding critical infrastructure security and resilience, and 10 additional entities based on analysis of its prior reviews of national cybersecurity, relevant executive policy, and national strategy documents. GAO also analyzed the *National Cyber Strategy* and *Implementation Plan* to determine if they aligned with the desirable characteristics of a national strategy.

View GAO-20-629. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

Federal entities have a variety of roles and responsibilities for supporting efforts to enhance the cybersecurity of the nation. Among other things, 23 federal entities have roles and responsibilities for developing policies, monitoring critical infrastructure protection efforts, sharing information to enhance cybersecurity across the nation, responding to cyber incidents, investigating cyberattacks, and conducting cybersecurity-related research. To fulfill their roles and responsibilities, federal entities identified activities undertaken in support of the nation's cybersecurity. For example, National Security Council (NSC) staff, on behalf of the President, and the National Institute of Standards and Technology, have developed policies, strategies, standards, and plans to guide cybersecurity efforts. The Department of Homeland Security has helped secure the nation's critical infrastructure through developing security policy and coordinating security initiatives, among other efforts. Other agencies have established initiatives to gather intelligence and share actual or possible cyberattack information. Multiple agencies have mechanisms in place to assist in responding to cyberattacks, and law enforcement components, including the Federal Bureau of Investigation, are responsible for investigating them.

The White House's September 2018 *National Cyber Strategy* and the NSC's accompanying June 2019 *Implementation Plan* detail the executive branch's approach to managing the nation's cybersecurity. When evaluated together, these documents addressed several of the desirable characteristics of national strategies, but lacked certain key elements for addressing others.

***National Cyber Strategy* and *Implementation Plan* are Missing Desirable Characteristics of a National Strategy**

Characteristic	Cyber Strategy and Plan Coverage of Issue
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-20-629

For example, the *Implementation Plan* details 191 activities that federal entities are to undertake to execute the priority actions outlined in the *National Cyber Strategy.* These activities are assigned a level, or tier, based on the coordination efforts required to execute the activity and the extent to which NSC staff is expected to be involved. Thirty-five of these activities are designated as the highest level (tier 1), and are coordinated by a functional entity within the NSC. Ten entities are assigned to lead or co-lead these critical activities while also tasked to lead or co-lead lower tier activities.

What GAO Recommends

GAO is making one matter for congressional consideration, that Congress should consider legislation to designate a leadership position in the White House with the commensurate authority to implement and encourage action in support of the nation's cybersecurity.

GAO is also making one recommendation to the National Security Council to work with relevant federal entities to update cybersecurity strategy documents to include goals, performance measures, and resource information, among other things. The National Security Council neither agreed nor disagreed with GAO's recommendation.

Leadership Roles for Federal Entities Assigned as Leads or Co-Leads for National Cyber Strategy Implementation Plan Activities

Entity	Tier 1 Activities	Tier 2 Activities	Tier 3 Activities
National Security Council	15	7	3
Department of Homeland Security	14	19	15
Office of Management and Budget	7	6	5
Department of Commerce	5	9	35
Department of State	2	5	11
Department of Defense	1	6	17
Department of Justice	1	10	5
Department of Transportation	1	0	5
Executive Office of the President	1	0	0
General Services Administration	1	2	1

Source: GAO analysis of 2018 *National Cyber Strategy* and 2019 *Implementation Plan*. | GAO-20-629

Although the *Implementation Plan* defined the entities responsible for leading each of the activities; it did not include goals and timelines for 46 of the activities or identify the resources needed to execute 160 activities. Additionally, discussion of risk in the *National Cyber Strategy* and *Implementation Plan* was not based on an analysis of threats and vulnerabilities. Further, the documents did not specify a process for monitoring agency progress in executing *Implementation Plan* activities. Instead, NSC staff stated that they performed periodic check-ins with responsible entities, but did not provide an explanation or definition of specific level of NSC staff involvement for each of the three tier designations. Without a consistent approach to engaging with responsible entities and a comprehensive understanding of what is needed to implement all 191 activities, the NSC will face challenges in ensuring that the *National Cyber Strategy* is efficiently executed.

GAO and others have reported on 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. The White House identified the NSC staff as 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 remains unclear which official ultimately maintains responsibility for not only coordinating execution of the *Implementation Plan*, but also holding federal agencies accountable once activities are implemented. 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. NSC staff also stated that federal entities are ultimately responsible for determining the status of the activities that they lead or support and for communicating implementation status to relevant NSC staff. However, without a clear central leader to coordinate activities, as well as a process for monitoring performance of the *Implementation Plan* activities, the White House cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and ultimately overcome this urgent challenge.

Contents

Tables

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CFO Act	*Chief Financial Officers Act of 1990*

DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DIB	defense industrial base
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HIPAA	*Health Insurance Portability and Accountability Act of 1996*
IRS	Internal Revenue Service
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSF	National Science Foundation
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PII	personally identifiable information
PPD-21	Presidential Policy Directive 21
SP	special publication
SSA	sector-specific agency
State	Department of State

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

September 22, 2020

Congressional Requesters:

Our nation is dependent on computer-based (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all federal and nonfederal operations are supported by cyber information systems and electronic data, and entities would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. As such, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being.

However, cyber-based intrusions and attacks on both federal and nonfederal systems have become not only more numerous and diverse, but also more damaging and disruptive. Moreover, the risks to systems supporting the federal government and the nation's critical infrastructure are increasing. Insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks threaten to undermine our utilization of cyber information systems. Laws, policies, and strategies have directed multiple federal entities to address cyber-related threats to federal systems and, in partnership with nonfederal entities, encouraged better protection of systems supporting the nation's critical infrastructure—such as energy, communications, and financial services—and to address the global nature of cybersecurity.[1]

In recognition of the growing threat, we have designated information security as a government-wide high-risk area since 1997. In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded the information

[1]The term "critical infrastructure" as defined in the *Critical Infrastructures Protection 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.

security high-risk area in 2015 to include protecting the privacy of personally identifiable information.[2]

You requested that we review the progress of efforts to protect the nation's critical infrastructure, including federal civilian, defense, and intelligence organizations' involvement in protecting and determining whether there is a cohesive national cybersecurity strategy as it relates to critical infrastructure. Our objectives were to: (1) describe the roles and responsibilities of federal entities that are tasked with supporting the nation's cybersecurity and (2) determine the extent to which the executive branch has developed a national strategy for cybersecurity and a plan to manage its implementation.

To address the first objective, we analyzed applicable policies, strategies, and laws to confirm the key federal entities with roles and responsibilities for supporting the nation's cybersecurity, as reported in our prior work, and to identify other relevant federal entities.[3] For example, Presidential Policy Directive 21 (PPD-21) designates federal entities as sector-specific agencies that are to partner with critical infrastructure owners and operators to strengthen the cybersecurity of the nation's critical infrastructure and, along with the *2013 National Infrastructure Protection Plan*, identifies their roles and responsibilities within this mission.[4]

We identified 23 federal entities for this review. Specifically, we selected 13 federal agencies based on their specialized or support functions related to critical infrastructure security and resilience, as identified in PPD-21.[5] We then analyzed documentation from our prior review of

[2]For our most recent update on this high-risk area see GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas,* GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[3]GAO, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems,* GAO-02-474 (Washington, D.C.: July 15, 2002).

[4]The White House, *Critical Infrastructure Security and Resilience,* Presidential Policy Directive/PPD-21*:* (Washington, D.C.: Feb. 12, 2013); Department of Homeland Security, *National Infrastructure Protection Plan, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

[5]The 13 key federal agencies identified in PPD-21 were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Transportation, and Treasury; the Environmental Protection Agency; the Federal Communications Commission; and the General Services Administration.

national cybersecurity, White House Executive Order 13800, the 2017 *National Security Strategy*, as well as the Department of Homeland Security's (DHS) May 2018 cybersecurity strategy and the 2018 *National Cyber Strategy*, to identify other key federal entities with roles and responsibilities in supporting the nation's cybersecurity.[6] Based on this analysis, we identified 10 additional entities.[7] We interviewed relevant officials from each of these federal entities to confirm their cybersecurity-related roles and responsibilities.

To address the second objective, we analyzed the September 2018 *National Cyber Strategy* developed by the White House and the June 2019 *Implementation Plan* developed by National Security Council (NSC) staff on behalf of the President, to determine whether they collectively possessed the desirable characteristics of a national strategy, as described in our prior work.[8] Specifically, we analyzed the *National Cyber Strategy* and *Implementation Plan* for possible indicators related to the six desirable characteristics of a national strategy. For example, we analyzed the documents to determine whether indicators of the problem definition and risk assessment characteristic included risk descriptions, issue areas, and vulnerabilities.

In addition, to evaluate the executive branch's plan to manage the strategy's implementation, we provided to each federal entity identified in the first objective a list of all the activities for which they were assigned a lead or supporting role in the *Implementation Plan*. Further, we developed and disseminated a data collection instrument to each entity and documented their responses regarding the extent to which they were aware of their assigned activities and examples of actions they had taken

[6]GAO-02-474; The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800, 82 Fed. Reg. 22391 (Washington, D.C.: May 11, 2017); The White House, *National Security Strategy* (Washington, D.C.: December 2017); Department of Homeland Security, *U.S. Department of Homeland Security Cybersecurity Strategy* (May 15, 2018); The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

[7]The 10 entities were the Central Intelligence Agency; the Federal Chief Information Officers Council; the National Science Foundation; the Office of the Director of National Intelligence; entities within the Executive Office of the President including the National Security Council, the Office of Management and Budget, and the Office of Science and Technology Policy; and Presidential Advisory Committees including the National Science and Technology Council, the President's Council of Advisors on Science and Technology Policy, and the President's National Security Telecommunications Advisory Committee.

[8]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

to fulfill them. We also obtained information from NSC staff to understand the process for developing the *Implementation Plan* as well as the executive branch's approach and mechanisms to oversee the plan's activities. (See appendix I for more details on our objectives, scope, and methodology.)

We conducted this performance audit from November 2018 to September 2020 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

The Nation Faces an Evolving Array of Cyber-based Threats

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

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

Further, advancements in technology, such as data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data (including personally identifiable information, or PII) and track them across large and numerous databases. For example, social media has been used as a mass communication tool where PII can be gathered in vast amounts.

In addition, ubiquitous internet and cellular connectivity makes it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of PII being exposed and compromised.

Cybersecurity Incidents Affect Federal and Nonfederal Systems

Cybersecurity incidents pose a serious challenge to economic, national, and personal privacy and security. The following examples highlight the impact of such incidents:

- In its 2020 annual data breach investigations report, Verizon reported analyzing 32,002 security incidents, identified across 81 countries in the 12 months since its 2019 report.[9] Of these incidents, 3,950 were confirmed to be data breaches.[10] Further, according to the report, more than a quarter of breaches go undiscovered for months or more.
- 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 computer systems of the credit-reporting agency Equifax. In July 2017, Equifax system administrators discovered that cyberattackers had gained unauthorized access via the internet to the online dispute portal that maintained documents used to resolve consumer disputes. The Equifax breach resulted in the attackers accessing the personal information of at least 145.5 million individuals, including individuals' names, Social Security numbers, birth dates, addresses, and driver's license numbers.
- Between May and July 2019, the Defense Information Systems Agency network was breached, potentially compromising personal information, including Social Security numbers.

[9]Verizon, *2020 Data Breach Investigation Report-13th Edition* (May 2020).

[10]A data breach can be defined as an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security.

- In May 2019, the Mayor of Baltimore, Maryland, reported that the city was the victim of a ransomware attack.[11] 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 response to the attack, Baltimore noted that it was working with federal partners to investigate and respond to the attack as well as restore systems.
- In January 2019, the DOJ announced that it had indicted two Ukrainian men for their role in a large-scale, international conspiracy to hack into the Securities and Exchange Commission's computer systems and profit by trading on critical information they stole.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation (FBI) stated that, since at least March 2016, hackers acting on behalf of the Russian government had targeted U.S. government agencies and critical infrastructure sectors, including the energy, nuclear, water, aviation, and critical manufacturing sectors.
- In April 2017, the Commissioner of the Internal Revenue Service (IRS) testified that the IRS had disabled its data retrieval tool in early March 2017 after becoming concerned about the misuse of taxpayer data. Specifically, the agency suspected that PII obtained outside the agency's tax system had been used to access the agency's online federal student aid application in an attempt to secure tax information through the data retrieval tool. In April 2017, the agency began notifying taxpayers who could have been affected by the breach.
- In June 2015, the Office of Personnel Management reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate, but related, incident had compromised its systems and the files related to background investigations for 21.5 million individuals.

These concerns are further highlighted by the number of information security incidents reported by federal executive branch civilian agencies

[11]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 remain unavailable, or data may be deleted.

to DHS's Cybersecurity and Infrastructure Security Agency (CISA).[12] For fiscal year 2019, 28,581 such incidents were reported by the Office of Management and Budget (OMB) in its 2019 annual report to Congress, as mandated by the *Federal Information Security Modernization Act of 2014*.[13] These incidents included, among others, web-based attacks, phishing, and the loss or theft of computing equipment.[14] Further, the FBI's Internet Crime Complaint Center reported receiving 467,361 complaints in 2019 from non-public entities, with the reported losses from these information security incidents exceeding $3.5 billion. The most prevalent crime types were phishing, non-payment/non-delivery, extortion, and personal data breach.

Federal Law, Policy and Strategy Establish Roles and Responsibilities for Entities in Supporting National Cybersecurity

Various federal legislation and policies require federal agencies to protect their networks and cyber infrastructure. For example, in February 2013, PPD-21 was established to advance a national unity of effort to strengthen and maintain a secure, functioning, and resilient critical infrastructure.[15] The directive establishes sector-specific agencies (SSAs) as the federal entities responsible for providing institutional knowledge and specialized expertise for securing the nation's critical infrastructure. SSAs are responsible for leading, facilitating, or supporting infrastructure protection activities, against all-hazards, in their designated critical

[12]CISA includes a central federal information security incident center that compiles and analyzes information about incidents that threaten information security, known as CISA Central.

[13]The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

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

[15]The White House, PPD-21. The term "all hazards" is defined by the directive as a threat or an incident, natural or manmade, which warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. "All hazards" includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

infrastructure sector. Additionally, the President concurrently issued Executive Order 13636 to enhance the security and resilience of the nation's critical infrastructure and maintain a cyber environment that promotes safety, security, and privacy.[16]

Further, the *Federal Information Security Modernization Act of 2014* requires federal agencies in the executive branch to develop, document, and implement an information security program for their information systems and evaluate it for effectiveness. Specifically, 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.

Additionally, Presidential Policy Directive 41, issued in July 2016, set forth principles governing the federal government's response to cyber incidents involving government or private sector entities.[17] For significant cyber incidents, this PPD establishes lead federal agencies and a process for coordinating the broader federal government response. PPD-41 also requires the DOJ and DHS to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities. The directive instructs federal agencies to undertake three concurrent lines of effort: threat response, led by FBI; asset response, led by CISA; and intelligence support and related activities, led by the Office of the Director of National Intelligence (ODNI) and SSAs.

Also, in May 2017, the President issued Executive Order 13800, which states that the President will hold agency heads accountable for managing cybersecurity risk to their enterprises.[18] 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. Additionally, the order states the executive branch should promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic

[16]The White House, Executive Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

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

[18]The White House, Executive Order 13800.

prosperity. It also reflected the need for deterrence and international cooperation. Further, in December 2017, the President issued the *National Security Strategy*, citing cybersecurity as a national priority and identifying needed actions, such as identifying and prioritizing risk, building defensible government networks, and deterring and disrupting malicious cyber actors.[19]

The *Cybersecurity and Infrastructure Security Agency Act of 2018* renamed DHS's National Protection and Programs Directorate as CISA. Responsibilities of the agency's director include, among other things, leading cybersecurity and critical infrastructure activities of the agency and coordinating with federal and nonfederal entities to carry out these activities.[20]

National Plans and Strategies Define Federal Agencies' Responsibilities for Supporting Cyber Infrastructure

The *National Infrastructure Protection Plan* (NIPP) originally developed by DHS in 2006 and subsequently updated in March 2009 and December 2013, aims to further integrate critical infrastructure protection efforts between government and private sectors.[21] It describes a voluntary partnership model as the primary means of coordinating government and private-sector efforts to protect critical infrastructure. As part of the partnership structure, the designated SSAs serve as the lead coordinators for the security programs of their respective sectors.

The *National Cyber Strategy*, issued by the White House in September 2018, describes actions that federal agencies and the executive branch are to take to secure critical infrastructure, among other things.[22] For example, the strategy outlines activities such as securing critical infrastructure, federal networks, and associated information, as well as developing the cybersecurity workforce. Additionally, the *National Cyber Strategy* outlined the executive branch's approach to cybersecurity through a variety of priority actions needed to address the nation's

[19]The White House, *National Security Strategy*.

[20]The *Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. No. 115–278, title XXII, 132 Stat. 4168-4186 (Jan. 3, 2018).

[21]DHS, *National Infrastructure Protection Plan, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

[22]The White House, *National Cyber Strategy of the United States of America*.

cybersecurity challenges, such as centralizing management and oversight of federal civilian department and agency network cybersecurity and working with other countries to contribute to greater predictability and stability in cyberspace. The *National Cyber Strategy* assigns NSC staff to coordinate with departments, agencies, and OMB on a plan to implement the strategy.

Federal Cybersecurity Challenges Have been Long Reported

We have reported since 1997 on cybersecurity challenges the federal government faces. More recently, in our September 2018 update to the 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.[23] The challenges derived primarily through reviews of more than 40 products issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas.

Since the issuance of the 2018 high-risk report, we have completed several reviews that continued to highlight aspects of the critical actions needed to address the previously identified challenges:

- In July 2019, we reported that key practices for establishing an agency-wide cybersecurity risk management program 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.[24] Although the 23 agencies that we reviewed had almost always designated a risk executive, they often had not fully incorporated other key practices in their programs, such as not fully establishing agency- and system-level policies for assessing, responding to, and monitoring risks, and not fully establishing a process for coordinating between their cybersecurity and enterprise risk management programs for

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

[24]GAO-19-384.

managing all major risks. We made a total of 58 recommendations, 57 to the 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) agencies in our review and one to the Director of OMB,[25] in coordination with the Secretary of Homeland Security, to address challenges in developing an agency-wide cybersecurity risk management program.

- In August 2019, we reported that the electric grid faces significant cybersecurity risks.[26] We stressed that the electric grid is becoming more vulnerable to cyberattacks—particularly those involving industrial control systems that support grid operations. We recommended that the Department of Energy (DOE) develop a plan aimed at implementing the federal cybersecurity strategy for the electric grid. We also recommended that the Federal Energy Regulatory Commission consider adopting changes to its cybersecurity standards and assess the risks of cyberattacks on distributed targets. While our review in this case focused on the electric grid, several news sources suggest that the same risk assessment is to varying degrees true of other critical infrastructure sector systems.
- In December 2019, we reported that 15 of 24 CFO Act agencies surveyed did not always use the Federal Risk and Authorization Management Program (FedRAMP) for authorizing cloud services.[27] For example, one agency reported that it used 90 cloud services that were not authorized through FedRAMP and the other 14 agencies reported using a total of 157 cloud service that were not authorized

[25]The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. These 24 entities, often referred to collectively as CFO Act agencies, are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. 31 U.S.C. § 901(b).

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

[27]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).

through the program. We recommended that OMB establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP in addition to 24 recommendations for federal agencies in the review to address concerns with their cloud service processes.

- In February 2020, we reported that most of the nine SSAs had not developed methods to determine the level and type of adoption of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*,[28] as we previously recommended.[29]
- In April 2020, we reported that OMB and DHS had partially addressed most leading practices associated with government reform through their efforts to implement several projects, such as reskilling employees to fill vacant cybersecurity positions.[30] However, we noted that the agencies had not established a dedicated implementation team, nor a government-wide implementation plan, among other practices. Without these practices in place, OMB and DHS may not be able to monitor implementation activities and determine progress made toward solving the cybersecurity workforce shortage. We recommended, among other things, that OMB, working with DHS, should develop a government-wide implementation plan with goals, timelines, key milestones, and deliverables to track and communicate implementation progress of the reform proposal to solve the cybersecurity workforce shortage, among other actions.

Since 2010, we have made over 3,000 recommendations to agencies aimed at addressing cybersecurity challenges facing the government—over 370 of which were made since the last high-risk update in March 2019. Nevertheless, many agencies continue to face challenges in safeguarding their information systems and information, in part, because many of these recommendations have not been fully implemented.

Of the roughly 3,000 recommendations made since 2010, nearly 600 had not been fully implemented as of early September 2020. Of these nearly

[28]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Gaithersburg, MD: April 2018).

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

[30]GAO, *Federal Management: Selected Reforms Could Be Strengthened By Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: April 23, 2020).

600 recommendations, we designated 75 as priority recommendations, meaning that we believe these recommendations warrant priority attention from heads of key departments and agencies.

GAO has repeatedly reported on the importance of a comprehensive national strategy and high-level, centralized leadership for national cybersecurity

For more than a decade, we have been reporting on the importance of a comprehensive strategy and clearly defined leadership to address national cybersecurity issues.

- In early 2009, we convened a panel of experts to discuss the national cybersecurity strategy and its implementation, and other critical aspects of the strategy, including areas for improvements. Panel members included former federal officials, academics, and private sector executives with cybersecurity expertise. The panelists highlighted 12 key improvements that are, in their view, essential to enhancing the strategy and strengthening our national cybersecurity posture.[31]

  One of the 12 recommended improvements is that responsibility and accountability for leading and overseeing national cybersecurity policy be elevated to the White House. According to the panelists, to be effective, this office must have, among other things, commensurate authority—for example, over budgets and resources—to implement and employ appropriate incentives to encourage action.

- In July 2010, we reported on additional challenges the government faced regarding international cooperation in addressing global cybersecurity and governance.[32] Specifically, we reported that the government faced a number of challenges that impeded its ability to formulate and implement a coherent approach to addressing the global aspects of cybersecurity. For example, we observed that the White House Cybersecurity Coordinator's authority and capacity to

[31]GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture,* GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

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

effectively coordinate and forge a coherent national approach to cybersecurity policy were still under development.[33]

- In February 2013, we observed that the government's cybersecurity strategy documents, at the time, generally addressed several of the desirable characteristics of national strategies; however, the documents lacked certain key elements, such as milestones and performance measures, costs and resources, roles and responsibilities, and linkages with other key strategy documents.[34] As a result, we recommended that the White House Cybersecurity Coordinator develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy, in order to provide a more effective framework for implementing cybersecurity activities and better ensure that such activities will lead to progress in cybersecurity. The Executive Office of the President agreed that more needs to be done to develop a coherent and comprehensive strategy on cybersecurity but did not believe producing another strategy document would be beneficial.
- In September 2018, we reported that the executive branch had made progress toward outlining a federal strategy for confronting cyber threats, but that more effort was needed to address all of the desirable characteristics of a national strategy that we recommended.[35] We noted, for example, that most of the existing executive branch strategy documents related to cybersecurity lacked clearly defined roles and responsibilities for key agencies, such as DHS, the Department of Defense (DOD), and OMB, which contribute substantially to the nation's cybersecurity programs. Shortly after the issuance of our report, the White House released its *National Cyber Strategy*.
- In March 2019, we reported that the September 2018 *National Cyber Strategy* outlined the executive branch's approach to cybersecurity through a variety of priority actions, such as centralizing management

[33]In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator.

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

[35]Because a current national cybersecurity strategy did not exist the time of our review, we evaluated other relevant executive branch documents including Executive Order 13800, the *National Security Strategy*, and DHS Cybersecurity Strategy.

and oversight of federal civilian cybersecurity.[36] However, we pointed out that the strategy lacked key elements that we have previously reported can enhance the usefulness of a national strategy, including clearly defined roles and responsibilities, and information on the resources needed to carry out the goals and objectives. Although the strategy stated that NSC staff are to coordinate with departments, agencies, and OMB to determine the resources needed to support the strategy's implementation, the *National Cyber Strategy* did not identify which official maintained overall responsibility for coordinating these efforts, especially in light of the elimination of the White House Cybersecurity Coordinator position in May 2018.[37] We stressed that, going forward, it would be critical for the White House to clearly define the roles and responsibilities of key agencies and officials in order to foster effective coordination and hold agencies accountable for carrying out planned activities to address the cybersecurity challenges facing the nation.

Commissions during the Bush, Obama, and Trump administrations have highlighted the lack of cybersecurity leadership as an enduring challenge

Commissions have consistently highlighted the importance of central leadership to overcome cyber threats to the nation and have made related recommendations aimed at establishing clear roles and responsibilities for a leadership position.

- In December 2008, the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency issued a report that outlined a series of recommendations for the new administration to consider in support of a comprehensive national approach to securing cyberspace.[38] The report stressed the need to lead

[36]GAO-19-157SP.

[37]The White House Cybersecurity Coordinator position was created in December 2009 to, among other things, coordinate interagency cybersecurity policies and strategies, and to develop a comprehensive national strategy to secure the nation's digital infrastructure.

[38]Center for Strategic & International Studies, *Securing Cyberspace for the 44th Presidency*, (Washington, D.C.: Dec. 2008). The Center for Strategic & International Studies Commission on Cybersecurity for the 44th Presidency was established in August 2007 to examine existing plans and strategies and to assess what a new administration should continue, what it should change, and what new policies it should adopt and what new authorities it should seek from Congress.

cybersecurity from the White House. As such, the commission proposed creating a new office for cyberspace in the Executive Office of the President, which would combine existing entities and work with the NSC to manage the many aspects of securing national networks.

- In February 2016, President Obama directed the creation of the Commission on Enhancing National Cybersecurity, a group tasked with assessing the state of the nation's cybersecurity and developing actionable recommendations for securing and growing the digital economy by strengthening cybersecurity in the public and private sectors. In its final report, the commission identified six essential areas, or imperatives, for enhancing cybersecurity, along with specific recommendations and action items supporting each imperative.[39]

  Among other actions, the report recommended that the federal government better match cybersecurity responsibilities with the structure of, and positions in, the Executive Office of the President. The commission noted that the current leadership and organizational construct for cybersecurity within the federal government were not commensurate with the challenge of securing the digital economy and supporting the national and economic security of the United States. It stressed that effective implementation of cybersecurity priorities would require strong leadership, beginning at the top, and that agencies must receive clear direction from the President and be granted corresponding authorities.

- In March 2020, the Cyberspace Solarium Commission[40] issued the *U.S. Cyberspace Solarium Commission Final Report*, which addressed the strategic approach needed to defend the nation against cyberattacks and the policies and legislation needed to implement that strategy.[41] The Solarium Commission suggested that a layered cyber defense strategic approach to cybersecurity is needed to reduce the probability and impact of cyberattacks.

  The Solarium Commission's report contained 82 recommendations, including several that addressed the federal structure to secure

[39]Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Washington, D.C.: Dec. 1, 2016).

[40]*John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140. The act established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees and officials from the Office of the Director of National Intelligence, DHS, DOD, and the FBI.

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

cyberspace and respond to attacks. Those recommendations included updating the *National Cyber Strategy*, establishing permanent congressional committees on cybersecurity, and strengthening the capabilities of DHS's CISA with resources and clear authorities.

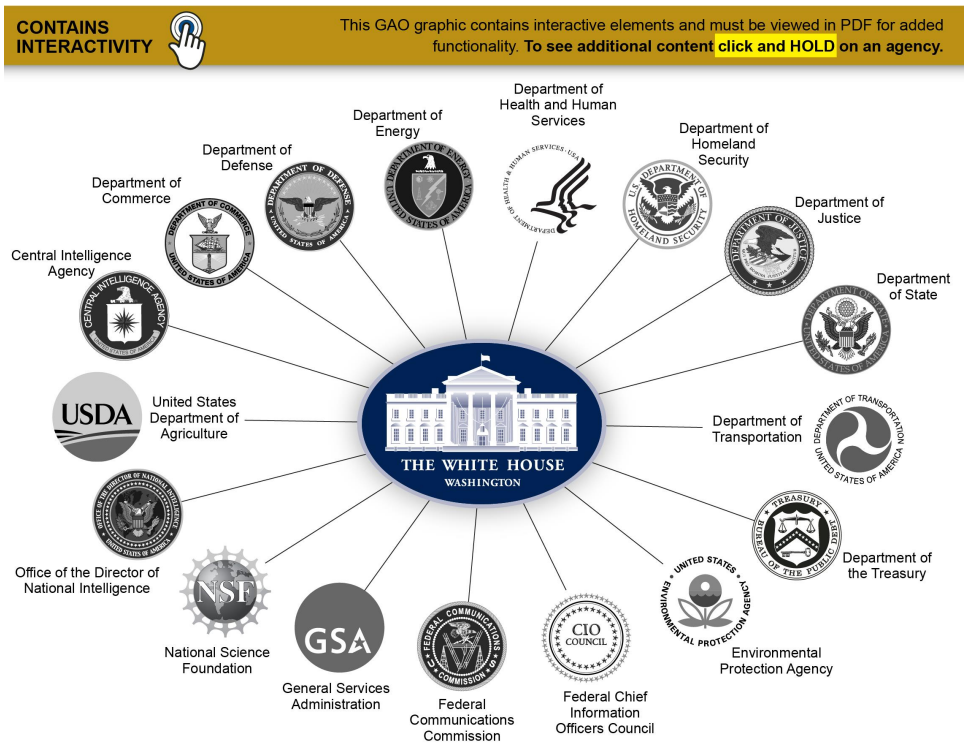
Additionally, the Solarium Commission recommended that the Congress establish a National Cyber Director within the Executive Office of the President, who would be Senate-confirmed and supported by the Office of the National Cyber Director. According to the Commission, the National Cyber Director would serve as the President's principal adviser for cybersecurity and associated emerging technology issues; the lead for national-level coordination for cyber strategy, policy, and defensive cyber operations; and the chief U.S. representative and spokesperson on cybersecurity issues. Further, the National Cyber Director would be responsible for the integration of cybersecurity policy and operations across the executive branch and would not direct or manage day-to-day cybersecurity policy or the operations of any one federal agency.[42]

Federal Entities Have Various Roles and Responsibilities for Helping to Enhance the Nation's Cybersecurity

Federal entities have a variety of roles and responsibilities for supporting efforts to enhance the cybersecurity of the nation. Specifically, 23 federal entities have roles and responsibilities related to developing policies, monitoring critical infrastructure protection efforts, sharing information to enhance cybersecurity across the nation, responding to cyber incidents, investigating cyberattacks, and conducting cybersecurity-related research, among other activities. Figure 1 identifies the key federal entities, and components within each of them, that have roles and responsibilities for supporting the nation's cybersecurity.

[42]Section 1132 of H.R. 6395 (116th Congress) would establish, within the Executive Office of the President, the Office of the National Cyber Director. The Office would be headed by a National Cyber Director, a presidentially appointed Senate confirmed position.

Figure 1: Key Federal Entities that are Responsible for Supporting the Nation's Cybersecurity



Source: GAO analysis of entities' data. | GAO-20-629

To fulfill their roles and responsibilities, federal entities identified a variety of activities that they have undertaken in support of the nation's cybersecurity. Certain entities, such as NSC and NIST, have developed policies, strategies, standards, and plans to guide cybersecurity efforts. Other agencies, such as DHS's CISA, described initiatives that they have undertaken to gather intelligence and share information regarding actual or possible cyberattacks on the nation's critical infrastructure. When cyberattacks occur, multiple agencies have mechanisms in place to assist in responding to such attacks; and law enforcement components, including the FBI, are responsible for investigating such incidents. To supplement the discussion that follows, appendix II provides descriptions of each of the 23 federal entities' cybersecurity-related roles and responsibilities.

Federal Entities Develop Policies for Securing the Nation's Cyber Infrastructure

To secure the nation's cyber infrastructure, several federal entities including DHS, General Services Administration (GSA), NIST, and OMB are responsible for developing policies, creating strategies, issuing standards, and identifying best practices. For example,

- DHS has used its authority to develop and oversee the implementation of compulsory directives to federal civilian agencies—referred to as binding operational directives. These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk. Since 2015, DHS has issued at least eight such directives impacting federal civilian agencies. In addition to binding operational directives, DHS also has the authority to issue emergency directives in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. This emergency directive authority was contained in the *Federal Cybersecurity Enhancement Act of 2015*.[43]
- GSA, through the Federal Information Processing Standard (FIPS) 201 evaluation program, maintains a list of physical access control system equipment that is compliant with identification standards.[44] Listed products have been tested and approved by the federal government for use by federal agencies.
- NIST developed the *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST cybersecurity framework).[45] This voluntary, risk-based framework comprises a set of industry standards and best practices to help organizations manage cybersecurity risks. In addition, NIST develops FIPS, which are

[43]The *Federal Cybersecurity Enhancement Act of 2015* is a part of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, div. N, title II, subtitle B, 129 Stat. 2242, 2963-2975 (Dec. 18, 2015).

[44]National Institute of Standards and Technology*, Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards (FIPS) Publication 201-2, (Gaithersburg, MD: Aug. 2013). (This supersedes FIPS 201-1 (June 2006).)

[45]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

information technology standards for adoption and use by federal entities to achieve a common level of quality or some level of interoperability.

- OMB issued a memorandum in May 2019 that set forth the federal government's Identity, Credential, and Access Management policy. This memorandum, among other things, requires agencies to implement NIST Special Publication (SP) 800-63-3.[46] The guidelines provide technical requirements for federal agencies implementing digital identity services, and covering identity proofing and authentication of users interacting with government IT systems over open networks.

Federal Agencies Monitor and Coordinate Efforts to Secure the Nation's Cyber Infrastructure

Federal policy, plans, and strategies establish oversight roles and responsibilities for the protection of critical infrastructure. Specifically, PPD-21, the NIPP, and the *National Cyber Strategy*, identify ways federal agencies may work with the private sector to manage risks to protect the nation's critical infrastructure. Federal entities including DOD, the Department of Health and Human Services (HHS), DHS, and the Environmental Protection Agency (EPA), fulfill these roles for various critical infrastructure sectors. For example,

- DOD, as the SSA for the defense industrial base (DIB), amended the Defense Federal Acquisition Regulation Supplement to safeguard unclassified DOD information on DIB company networks.[47] For example, it generally requires the inclusion of certain contract clauses that in turn require contractors to report cyber incidents that affect the contractor's information system or the DOD information residing therein.
- HHS Office for Civil Rights is responsible for enforcing the HIPAA privacy, security, enforcement and breach notification regulations (HIPAA rules), which protect the privacy and security of patients' health information. The HIPAA rules were promulgated pursuant to the *Health Insurance Portability and Accountability Act of 1996*

[46]National Institute of Standards and Technology, *Digital Identity Guidelines*, SP 800-63-3 (Gaithersburg, MD: June 2017) (updated March 2020).

[47]The Defense Acquisition Regulations System develops and maintains acquisition rules and guidance to facilitate the acquisition workforce as they acquire the goods and services DOD requires to ensure America's warfighters' continued worldwide success.

(HIPAA) and modified by the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, and the *Genetic Information Nondiscrimination Act of 2008*.

- DHS's CISA serves as the SSA for eight of the 16 infrastructure sectors—chemical, commercial facilities, communications, critical manufacturing, dams, emergency services, information technology, and nuclear reactors, materials, and waste—and for the elections subsector. CISA fulfills all SSA functions as defined in the NIPP, and conducts physical and cybersecurity focused exercises to help agencies and organizations evaluate their activities in response to an incident. The exercises are conducted with the intent of enhancing agencies' and organizations' security readiness and their ability to respond quickly and efficiently to an incident.
- EPA, as the SSA for the water and wastewater systems sector, has developed cybersecurity guidance and tools to advance the security and resilience of the sector, including nationwide training and tabletop exercises on cybersecurity threats, risk assessment, vulnerabilities, consequences, incident response, and program development.

Federal Agencies Share Cybersecurity-related Information

To facilitate the detection of, and protection against, computer-based attacks, federal entities including DOD, HHS, DHS, and the ODNI, collect and disseminate information to alert organizations of potential and actual infrastructure attacks. For example,

- DOD established the DIB Cybersecurity Program to improve DIB network defenses, reduce damage to critical programs, and increase DOD and DIB cyber situational awareness. Under the DIB Cybersecurity Program, DOD and DIB participants share unclassified and classified cyber threat information.
- HHS maintains the Health Threat Operations Center that supports both direct sharing with other healthcare and public health agencies, and HHS's cyber threat sharing platform. In addition, HHS's Health Sector Cybersecurity Coordination Center conducts sector outreach, hosts threat briefings, and educates the public health sector about cybersecurity products' risks and vulnerabilities and associated mitigation strategies.
- DHS's CISA detects and disseminates cyber incident information utilizing the US-CERT website, the Automated Indicator Sharing

program, social media, and the Homeland Security Information Network portal to distribute alerts, recommendations, best practices, indicators, and critical technical information regarding cyber incidents to stakeholders.

- ODNI serves as a center for government partners to coordinate with and receive contextualized threat intelligence, among other things. ODNI disseminates integrated intelligence community assessments and whole-of-government response options and initiatives to address shared cybersecurity challenges to their government partners.

Federal Agencies Provide Cyber Incident Response Capabilities

Certain federal entities, including DOD, DOE, HHS, DHS, and the Department of Transportation (DOT), have implemented programs and mechanisms to respond to cyber incidents. These include efforts to isolate and minimize damage, and coordinate the necessary actions to restore functionality. For example,

- DOD's Cyber Crime Center provides digital and multimedia forensic services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis for law enforcement and counterintelligence among other mission areas.[48]
- DOE's Office of Cybersecurity, Energy Security, and Emergency Response supports incident response for cyber incidents impacting or potentially impacting the energy sector, through the coordination of federal capabilities to provide relevant information, assess impacts, and remediate and mitigate the impact of energy disruptions.
- The HHS Office of the Assistant Secretary for Preparedness and Response leads and coordinates the preparedness and response related activities for major healthcare and public health sector cybersecurity incidents.
- DHS's CISA provides assistance, upon request, to entities that are potentially impacted when a cyber incident occurs, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents.

[48]See GAO-18-47, GAO-16-574, and GAO-16-332 for more information about DOD's planning and preparedness to provide support to civil authorities during a cyber incident.

- DOT's Federal Highway Administration developed a Transportation Cybersecurity Incident Response and Management framework to support information sharing in response to a cyber incident. The framework supports participation in Cyber Storm type exercises to assess the ability of transportation roadway entities to detect and respond to a cyberattack or vulnerability that spans devices or other sectors.[49]

Federal Entities Investigate Cyberattacks

Federal entities with law enforcement responsibilities, including the DOJ and the FBI, have established programs to investigate cyberattacks on critical infrastructure. For example,

- Within DOJ, the U.S. Attorney's Offices' Computer Hacking and Intellectual Property Network consists of specially trained federal prosecutors, who focus on computer crimes, and the Criminal Division's Computer Crime and Intellectual Property Section, which investigates and prosecutes cyber intrusions. Additionally, the U.S. Attorney's Office partners with DOJ's National Security Division and the FBI's Cyber Division to draw upon all available legal resources to investigate, disrupt, and deter malicious cyber activity that affects, involves, or relates to national security.
- The FBI's Cyber Division consists of specially trained cyber squads at FBI headquarters and in each of its 56 field offices, staffed with agents and analysts who protect against and investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

[49]Cyber Storm is DHS's biennial exercise series that provides the framework to strengthen cyber preparedness in the public and private sectors. According to DHS, Cyber Storm participants: (1) examine organizations' capability to prepare for, protect from, and respond to the potential effects of cyberattacks; (2) exercise strategic decision-making and interagency coordination of incident response(s) in accordance with national-level policy and procedures; (3) validate information-sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response, and recovery information; and (4) examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.

Federal Entities Support Cybersecurity-related Research and Development Efforts

Certain agencies, including DHS, the Department of State (State), DOT, and the National Science Foundation (NSF) have a role in coordinating federally sponsored research and development in support of infrastructure protection and funding cybersecurity research projects. For example,

- DHS's CISA sponsors numerous grants, projects, and activities intended to directly support cybersecurity workforce development, including the National Initiative for Cybersecurity Careers and Studies, a one-stop shop for information on cybersecurity careers and a portal for access to thousands of hours of cybersecurity training content.
- State's Bureau of Democracy, Human Rights, and Labor supports research programs along with innovative technologies, digital safety, and policy advocacy through the Office of Global Programs Overseas.
- DOT, through its Office of the Assistant Secretary for Research and Technology, sponsors research in intelligent transportation communications security technology, such as the Security Credential Management System for connected vehicles and over-the-air communications.
- NSF supports research on a variety of areas related to cybersecurity, including secured communications, and sponsors workshops and meetings of government, industry, and academia experts to discuss research challenges and opportunities in technologies to advance security. NSF also funds centers for cybersecurity education and projects focused on cybersecurity education and workforce development, such as the CyberCorps Scholarship for Service scholarship program.

The National Cyber Strategy and Implementation Plan Are Missing Desirable Characteristics and Clear Leadership

The administration's planned approach to managing the nation's cybersecurity is articulated through the *National Cyber Strategy* and the accompanying *Implementation Plan*.[50] When evaluated together, these documents addressed several of the desirable characteristics of national strategies, but did not fully address other characteristics. For example, although the White House specified the purpose and problem definition in the *National Cyber Strategy*, the NSC did not require executive branch entities to fully establish goals and timelines or identify resources needed to execute a number of the activities detailed in the *Implementation Plan*. Additionally, although the NSC defined priorities for how it is to engage with entities responsible for executing these activities, NSC has not made clear how it will implement oversight of prioritized activities while overseeing the execution of the plan.

The executive branch's leadership of the *National Cyber Strategy*'s implementation is unclear, even though an implementation plan was developed. Specifically, though the *Implementation Plan* describes a coordination structure to support the implementation of the strategy, the executive branch's process and entity responsible for ensuring that the strategy's goals are achieved has not been fully defined. Further, the *Implementation Plan* assigned cybersecurity-related activities to federal entities. However, neither the strategy nor the *Implementation Plan* articulate how the White House can hold these entities accountable for accomplishing their assigned activities.

The National Cyber Strategy and Implementation Plan are Missing Desirable Characteristics of a National Strategy

We previously identified a set of generally desirable characteristics to aid responsible parties in developing and implementing national strategies, to enhance such strategies' usefulness in resource and policy decisions,

[50]National Security Council, *National Cyber Strategy Implementation Plan* (Washington, D.C.: June 2019). The *Implementation Plan* was not published to the public, but any entity assigned a lead or supporting role within the plan received a digital copy of the plan.

and to better assure accountability.[51] The characteristics that we identified are:

- **Purpose, scope, and methodology.** Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
- **Organizational roles, responsibilities, and coordination.** Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.
- **Integration and implementation.** Addresses 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.
- **Problem definition and risk assessment.** Addresses the particular national problems and threats the strategy is directed toward and entails a risk assessment that includes an analysis of threats to, and vulnerabilities of, critical assets and operations.
- **Goals, subordinate objectives, activities, and performance measures.** Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities; milestones; performance measures; and a monitoring mechanism to gauge results.
- **Resources, investments, and risk management.** Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.

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 following three characteristics of a national strategy including the definition of the document's purpose, specification of organizational roles in implementing the strategy and integration with other strategy documents:

- **Purpose, scope, and methodology.** The *National Cyber Strategy* articulated the need for a new cyber strategy to respond to new threats and a new era of strategic competition based on new realities

[51]GAO-04-408T.

that reduces vulnerabilities, deters adversaries, and safeguards opportunities for the nation. Additionally, the strategy outlined its scope by organizing along the pillars (i.e., goals)[52] first identified in the 2017 *National Security Strategy* and Executive Order 13800 as the foundation for developing the *National Cyber Strategy*. Although neither document outlines the methodology used for its development, NSC staff provided an overview of how the *Implementation Plan* was developed. From September 2018 to June 2019, NSC met with entities across the federal government to determine the various activities required to support goals and priority actions outlined in the *National Cyber Strategy* and the specific entities with responsibilities for executing each activity.

- **Organizational roles, responsibilities, and coordination.** Although the *National Cyber Strategy* does not specify which federal entities are responsible for addressing each of the 42 priority actions outlined within the document, the *Implementation Plan* assigns explicit responsibility to lead and supporting entities. Specifically, the plan outlines 191 activities the executive branch is to fulfill in order to execute the 42 priority actions outlined in the strategy and assigns organizational roles, responsibilities, and coordination for all 191 activities in the plan. Each activity is assigned to a lead or co-lead entity as the primary federal entity responsible for executing each activity; and one or more supporting entities expected to support the execution of an activity.

The *Implementation Plan* identifies a mechanism for the entities to coordinate their efforts. Each of the activities is assigned a level, or tier, which pertains to the coordination efforts required to execute the activity and the extent the NSC is intended to be involved in its coordination. Specifically:

[52]The four pillars are (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability—in concert with allies and partners—to deter and, if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

- The NSC Cyber directorate[53] is responsible for coordinating the implementation of each tier 1 activity. Of the 191 activities, 35 are designated at tier 1.
- Each federal entity assigned to lead a tier 2 activity is responsible for coordinating with other supporting entities and with the NSC, which intended to maintain a "significant interest" in each effort.[54] Of the 191 activities, 53 are designated at tier 2.
- Each federal entity assigned to lead a tier 3 activity (the tier that most activities are designated) is responsible for coordinating activities with other supporting entities and reporting periodically to the NSC on progress toward accomplishing an activity's goals. Of the 191 activities, 103 are designated at tier 3.

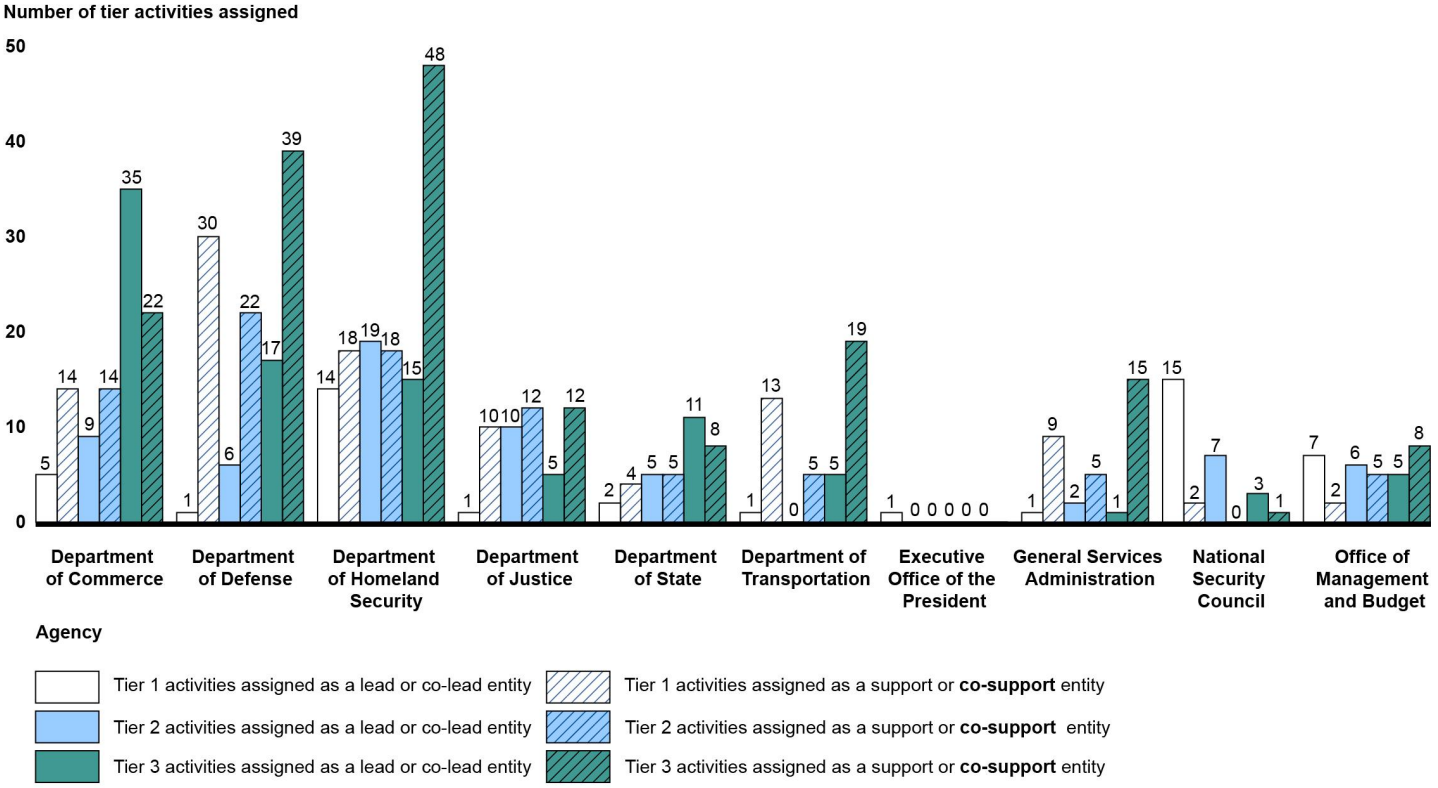
Entities are assigned responsibility for varying numbers of the tier 1, 2, and 3 activities. For example, DHS is assigned as a lead entity for 14 tier 1 activities, the NSC is assigned as a lead entity for 15, and State is assigned as a lead entity for two. Further, specific components within an entity are also assigned as a lead or support entity for various activities. Specifically, NIST, a component of the Department of Commerce, is assigned as a lead entity for 14 tier 3 activities. The NSC is tasked with maintaining direct oversight or "significant interest" in 88 of 191 tier 1 and 2 activities.

Figure 2 shows the number of tier 1, 2, and 3 activities for entities that are assigned as a lead or co-lead for a tier 1 activity. In addition, see appendix III for all entities' tier 1, 2, and 3 activities.

[53]The Cyber directorate is a functional entity within the NSC staff tasked with overseeing the implementation of the *National Cyber Strategy*. The directorate is led by the senior director and is made up of subject matter experts.

[54]NSC staff did not define the term "significant interest" or provide further details on required actions for activities where the NSC staff is tasked with such designation.

Figure 2: *National Cyber Strategy Implementation Plan* Tier 1, 2, and 3 Activities for Entities Assigned as Leads for Tier 1 Activities



Source: GAO analysis of *National Cyber Strategy Implementation Plan*. | GAO-20-629

Agency	Tier 1 co-lead	Tier 1 co-support	Tier 2 co-lead	Tier 2 co-sup- port	Tier 3 co-lead	Tier 3 co-support
Department of Commerce	5	14	9	14	35	22
Department of Defense	1	30	6	22	17	39
Department of Homeland Security	14	18	19	18	15	48
Department of Justice	1	10	10	12	5	12
Department of State	2	4	5	5	11	8
Department of Transportation	1	13	0	5	5	19
Executive Office of the President	1	0	0	0	0	0
General Services Administration	1	9	2	5	1	15
National Security Council	15	2	7	0	3	1
Office of Management and Budget	7	2	6	5	5	8

- **Integration and implementation.** In addition to the previously mentioned alignment with the *National Security Strategy*, the strategy documents demonstrate how they align to other strategies' goals, objectives, and activities. For example, actions such as improving the resilience of the internet and communications ecosystems, and promoting routine vulnerability assessments and mitigation within all Internet of Things products, are identified in both the *Implementation Plan* and Executive Order 13800.[55] The strategy documents also address how it relates to subordinate levels of government and their plans to implement the strategy. For example, some of the activities assigned to DOD in the *Implementation Plan* also were identified in the *DOD Cyber Strategy*. [56]

The *National Cyber Strategy* and the *Implementation Plan* did not fully address the three desirable characteristics of a national strategy related to risk assessment, performance measures, and resource investment:

- **Problem definition and risk assessment.** To its credit, the *National Cyber Strategy* highlights various cybersecurity challenges that public and private entities across the nation face, such as effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data, as well as detecting, responding to, and recovering from incidents. Additionally, the document identifies specific nation-state actors who have conducted cyberattacks, including economic espionage, against U.S. businesses and allies.

  However, none of the discussion of risk in the *National Cyber Strategy* is in the context of an assessment that included analysis of threats and vulnerabilities, as identified in the desirable characteristics. Further, although the *Implementation Plan* tasked entities with various risk assessment activities, such as those related to the federal supply chain and maritime infrastructure, it did not expand on the general references to risk identified in the *National Cyber Strategy*. Without a risk assessment, including an analysis of the threats to, and vulnerabilities of, critical assets and operations, the executive branch is unable to adequately make informed management decisions about

[55]Internet of Things 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.

[56]Department of Defense, *2018 Department of Defense Cyber Strategy* (2018).

resource allocations required to minimize risks and maximize returns on resources expended.

- **Goals, subordinate objectives, activities, and performance measures.** Although the *National Cyber Strategy and Implementation Plan* establish a structure intended to outline goals and performance measures, such measures are only outlined for 145 of the 191 activities. The *Implementation Plan* emphasizes that goals and timelines are discrete deliverable objectives or measures of performance for measuring an activity's success. In most cases, the *Implementation Plan* describes when specific tasks within activities are expected to be completed and may also state when an activity has been completed. However, other than periodic check-ins that NSC officials stated they conduct with officials from responsible entities, the NSC has not established a formal mechanism to track progress of the execution of activities in support of the goals outlined in the *National Cyber Strategy* and *Implementation Plan*.

  Moreover, the plan does not establish goals or timelines for 46 of the 191 activities. For example, the *Implementation Plan* did not document goals and timelines for DHS, NIST, and Treasury, among others, for activities related to developing global cyber incident response capability, developing standards and best practices for election infrastructure, and conducting Hamilton exercises, respectively.[57] Without identifying goals and performance measures for all activities, entities may not understand what they should try to achieve or the steps required to produce the desired results.

- **Resources, investments, and risk management.** The *National Cyber Strategy* lacks any information on the cost of implementation and the *Implementation Plan* only details information on needed resources for 31 of the 191 activities. For the remaining 160 activities, the *Implementation Plan* detailed that responsible entities were not required to submit resource information if they determined that the activity could be accomplished through the entities' existing budget. Neither of the documents include an analysis of the cost and resources needed to implement the entire strategy, as identified in the desirable characteristics. Without identifying resources for each activity in the plan, the NSC does not have sufficient insight into where responsible entities plan to target resource and investment allocation to balance risk reductions with costs. Consequently, the

[57]Hamilton exercises are one-day simulation events with public and private sector participants aimed at improving cyber threat response within the U.S. financial sector.

NSC is unable to fully articulate the true cost of the *National Cyber Strategy*'s implementation.

Despite the *National Cyber Strategy* and *Implementation Plan* addressing many aspects of the desirable characteristics of a national strategy, those elements not fully addressed make it unclear whether the actions taken in support of the strategy will be consistent with the requirements specified in documentation. For example, the lack of performance measures for all activities hinders NSC's ability to ensure accountability of entities tasked with executing the plan. Additionally, NSC staff stated that although the tier designation for each activity in the plan were derived from the priorities established in the *National Security Strategy* and *National Cyber Strategy*, each activity stands on its own. As such, the level of NSC's engagement (i.e., frequency of communication) may vary among entities and is driven by the requirements articulated by the entity responsible for the specific activity, regardless of the associated tier level. Furthermore, NSC staff did not provide an explanation for how they maintain "significant interest" for the 88 tier 1 and 2 activities, nor define what "significant interest" means.

NSC staff stated that the Cyber directorate receives updates from entities on progress or roadblocks encountered in completion of milestones in support of their respective activities. However, without a consistent approach to engaging with responsible entities or a comprehensive understanding of the resources required or means to evaluate performance of all 191 activities, the NSC will be challenged in ensuring that the *National Cyber Strategy* is executed as intended.

The White House's Leadership Role in Implementing the Strategy and Ensuring the Cybersecurity of the Nation is Unclear

We recently reported that when faced with threats of unprecedented scale, such as the COVID-19 pandemic, a whole-of-government response is required. Moreover, clearly defining roles and responsibilities for the wide range of federal departments and other key players becomes critically important in order to overcome such challenges.[58] We also have previously reported that the single most important element of successful

[58]GAO, *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts*, GAO-20-625 (Washington, D.C.: June 25, 2020).

government improvement initiatives—such as strategic efforts to address major challenges like ensuring the cybersecurity of the nation—is the demonstrated commitment of top leaders.[59] Federal standards for internal control in the federal government also emphasize the importance of maintaining leadership continuity in order to achieve agency objectives.[60] For these reasons, and others, we have highlighted the need to ensure that top leadership drives transformation and establishes dedicated teams to manage transformation processes.

We and other entities have reported on 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. Most recently:

- We reported in March 2019 that the *National Cyber Strategy* states that NSC staff are to coordinate with departments, agencies, and OMB to determine the resources needed to support the strategy's implementation. However, we stated it was unclear what official maintained overall responsibility for coordinating these efforts, especially in light of the elimination of the White House Cybersecurity Coordinator position in May 2018.
- The Solarium Commission's March 2020 report noted that numerous commissions, initiatives, and studies have recommended a more robust and institutionalized national-level mechanism for coordinating cybersecurity and associated emerging technology issues, and for overseeing the executive branch's development and implementation of an integrated national cybersecurity strategy. Accordingly, the Solarium Commission recommended the establishment of a National Cyber Director position, within the Executive Office of the President, who is Senate-confirmed and supported by the Office of the National Cyber Director. The Solarium Commission recommended that the official would serve as the President's principal advisor for cybersecurity and associated emerging technology issues; the lead for national-level coordination for cyber strategy, policy, and defensive cyber operations; and the chief U.S. representative and spokesperson on cybersecurity issues.

[59]GAO, *Government Performance: GPRA Modernization Act Provides Opportunities to Help Address Fiscal, Performance, and Management Challenges*, GAO-11-466T (Washington, D.C.: Mar. 16, 2011).

[60]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sep. 10, 2014).

The White House identified the NSC as the organization responsible for coordinating the implementation of the *National Cyber Strategy*. However, since the elimination of the position of the White House Cybersecurity Coordinator in May 2018, it has remained unclear what official within the executive branch ultimately maintains responsibility for not only coordinating execution of the *Implementation Plan*, but also holding federal agencies accountable for the nearly 200 activities moving forward.

We requested an explanation from the NSC as to which official or officials now maintain responsibility for the duties previously attributed to the Cyber Coordinator position. NSC staff stated the Cyber directorate and corresponding senior director, who reports to the Assistant to the President for National Security, now fulfill those duties, but did not provide a description of what those responsibilities include. Further, NSC staff stated that federal entities are responsible for determining the status of the activities that they lead or support, and for communicating the status of implementation to relevant NSC staff members. However, the *Implementation Plan* also states that a federal entity responsible for a specific activity can exclude itself from reporting this information if it determines that a respective activity is ongoing and has no discrete goals or measures of performance.

Without a clearly defined central leader to coordinate activities, as well as a process for monitoring performance on the *Implementation Plan* activities, the White House cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and, ultimately, overcome this urgent challenge.

Conclusions

Federal legislation, policies, guidance, and strategies, along with the *National Cyber Strategy* and *Implementation Plan*, establish roles and responsibilities for federal entities in supporting national cybersecurity, such as developing cybersecurity policies, guidance, and sharing information regarding actual or possible cyberattacks on the nation's critical infrastructure. In addition, multiple agencies carry out key activities supporting the nation's cybersecurity.

While the *National Cyber Strategy* and *Implementation Plan* address some of the characteristics of an effective national strategy, additional efforts are needed to fully incorporate risk assessment; performance measures; and resources, investments, and risk management into the

executive branch's cybersecurity strategy. Further, our previous reviews, as well as other studies, have highlighted the need for responsibility and accountability for leading and overseeing national cybersecurity policy to be elevated to the White House. Although NSC staff is tasked with the coordination of efforts to carry out the *National Cyber Strategy* and its accompanying *Implementation Plan*, there is a lack of clarity around how it plans on accomplishing this. Without effective and transparent leadership that includes a clearly defined leader, a defined management process, and a formal monitoring mechanism, the executive branch cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and ultimately overcome this urgent challenge.

Matter for Congressional Consideration

Congress should consider legislation to designate a leadership position in the White House with the commensurate authority—for example, over budgets and resources—to implement and encourage action in support of the nation's cyber critical infrastructure, including the implementation of the *National Cyber Strategy*. (Matter for Consideration 1)

Recommendation for Executive Action

We are making the following recommendation to the National Security Council:

The Chairman of the National Security Council, or his designee, should work with relevant federal entities to update strategy documents related to the nation's cybersecurity to better reflect desirable characteristics of a national strategy, to include:

- an assessment of cyber-related risk, based on an analysis of the threats to, and vulnerabilities of, critical assets and operations;
- measures of performance and formal mechanism to track progress of the execution of activities; and
- an analysis of the cost and resources needed to implement the *National Cyber Strategy*. (Recommendation 1)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the 23 entities included in our review. All of these entities provided responses, as further discussed.

In oral comments, NSC staff neither agreed nor disagreed with our recommendation. They did, however, provide comments regarding our discussion within the report on the elimination of the White House Cybersecurity Coordinator position in 2018. Specifically, NSC staff stated that the senior director of the NSC Cyber directorate now fulfills the duties that were previously assigned to the former White House Cybersecurity Coordinator.

However, the NSC staff did not provide additional details on what those responsibilities include and how they are executed. Therefore, as we previously stated, it remains unclear what official within the executive branch ultimately maintains responsibility for not only coordinating execution of the *Implementation Plan*, but also holding federal agencies accountable for the nearly 200 activities moving forward. Without a clearly defined leader, a defined management process, and a formal monitoring mechanism, the executive branch cannot ensure that entities are effectively executing their assigned activities intended to implement the nation's cybersecurity strategy.

Twelve entities (Department of Agriculture, DOE, DHS, DOJ, EPA, the Federal Communications Commission, NSF, the National Security Telecommunications Advisory Committee, ODNI, OMB, the Office of Science and Technology Policy, and the President's Council of Advisors on Science and Technology) provided technical comments, which we incorporated as appropriate. Further, we received emails from officials of the Central Intelligence Agency, the Departments of Commerce, Defense, Health and Human Services, State, Transportation, and Treasury, the Federal Chief Information Officers Council, the General Services Administration, and the National Science and Technology Council. In all of those emails, the officials stated that the entities had no comments on the draft report.

We are sending copies of this report to our Congressional addressees; the Chairman of the National Security Council; the Secretaries of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, State, Transportation, Treasury; the Attorney General

of the United States; the Directors of National Intelligence, the Central Intelligence Agency, the National Science Foundation, the Office of Science and Technology Policy, and the Office of Management and Budget; the Administrators of the General Services Administration and the Environmental Protection Agency; and the Chairs of the Chief Information Officers Council, Federal Communications Commission, National Security Telecommunications Advisory Committee, and the Presidential Advisory Committees within scope of this engagement. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions on the matters discussed in this report, please contact Nick Marinos at (202) 512-9342 or marinosn@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 IV.

Nick Marinos
Director, Information Technology and Cybersecurity

List of Requesters

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

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

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

The Honorable Mike Gallagher
House of Representatives

The Honorable James R. Langevin
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the roles and responsibilities of federal entities tasked with supporting the nation's cybersecurity, and (2) determine the extent to which the executive branch has developed a national strategy for cybersecurity and a plan to manage its implementation.

To address our first objective, we analyzed applicable policies, strategies, and laws to confirm the key federal entities with roles and responsibilities in supporting the nation's cybersecurity, as reported in our prior work, and to identify other relevant federal entities.[1] Presidential Policy Directive 21 (PPD-21) designates federal entities as sector-specific agencies and states that these agencies are to partner with critical infrastructure owners and operators to strengthen the security and resilience of the nation's critical infrastructure and, along with the 2013 *National Infrastructure Protection Plan*, identifies their roles and responsibilities within this mission.[2]

Based on our analysis of these documents, we identified 13 federal agencies to include in this review. Nine federal entities were selected based on their designation as sector-specific agencies in PPD-21: Departments of Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; the Environmental Protection Agency; the General Services Administration; and the United States Department of Agriculture. In addition, PPD-21 designates four other federal agencies with specialized or support functions related to critical infrastructure security and resilience such as the Departments of

[1]GAO, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems,* GAO-02-474 (Washington, D.C.: July 15, 2002).

[2]The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21 (Washington, D.C.: Feb. 12, 2013); Department of Homeland Security, *National Infrastructure Protection Plan, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

Commerce, Justice, and State; and the Federal Communications Commission.

We also analyzed recent cybersecurity policy and strategy documents issued by the White House, such as Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the 2017 *National Security Strategy*, and the Department of Homeland Security's May 2018 cybersecurity strategy.[3] Further, we reviewed our prior report on national cybersecurity.[4] From these documents, we identified an additional five federal entities to include the Central Intelligence Agency; the Office of Science and Technology Policy in the Executive Office of the President; and Presidential Advisory Committees including the National Science and Technology Council, the President's Council of Advisors on Science and Technology Policy, and the President's National Security Telecommunications Advisory Committee.

The *National Cyber Strategy* and *Implementation Plan* assigned cybersecurity-related activities to five additional federal entities: the Executive Office of the President, including the National Security Council (NSC) and the Office of Management and Budget; the Federal Chief Information Officers Council; the National Science Foundation; and the Office of the Director of National Intelligence that we included in our review.[5]

For the 23 entities identified to be within our scope, we interviewed relevant federal officials to confirm the key federal entities. In addition, we summarized cybersecurity-related roles and responsibilities for each federal entity based on the analysis we performed on the eight documents utilized in our selection analysis detailed above, as well as information from federal laws and publicly available agency information. We provided the summaries to each entity in order to confirm their

[3]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800, 82 Fed. Reg. 22391 (Washington, D.C.: May 11, 2017). The White House, *National Security Strategy* (Washington, D.C.: Dec. 2017). Department of Homeland Security, *U.S. Department of Homeland Security Cybersecurity Strategy* (May 15, 2018).

[4]GAO-02-474.

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

accuracy and to collect additional information about their roles and responsibilities and related activities.

To address the second objective, we reviewed the contents of the *National Cyber Strategy* and its associated *Implementation Plan* dated June 2019. We obtained the *Implementation Plan's* contents through observation at NSC's request to not submit a copy of the plan. From the observation, we transcribed, among other things, each activity's title and the lead and supporting federal agencies. We also transcribed sections from each element containing data related to the desirable characteristics of a national strategy developed from our prior GAO work, such as new resources and authorities, goals and timelines, and tier designation.[6] We did not transcribe all of the information contained within the *Implementation Plan*.

We then evaluated the *National Cyber Strategy* and the transcribed elements of the *Implementation Plan* to determine whether they collectively possessed the desirable characteristics of a national strategy developed from our prior work by identifying possible indicative statements in the documents. See table 1 for the indicative statements.

Table 1: National Strategy Characteristics, Definitions, and Indicative Statements Used to Evaluate the *National Cyber Strategy* and *Implementation Plan*

Characteristic	Definition	Indicative Statements
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	• "This plan was created to…" • "Purpose" statement • Executive summary
Problem definition and risk assessment	Addresses the particular national problems and threats the strategy is directed towards, and entails a risk assessment that includes an analysis of threats to, and vulnerabilities of, critical assets and operations.	• Risk assessment, including an analysis of threats and vulnerabilities • Issue areas
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	• Milestones for achieving goals • Performance measures for tracking progress • Reporting requirements • Life cycle/time frames • Standards

[6]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

Characteristic	Definition	Indicative Statements
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.	• Analysis of the cost of planned activities • Estimates of how activities will be funded in the future • Source and type of resources needed to carry out the goals and objectives • Assessment of the specific risks and resources needed to mitigate them
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	• Delegation of responsibilities • Oversight responsibilities • Clarity for individual agencies' response options to specific incidents • Coordination groups • "XX is responsible for…"/ "XX shall..." • "XX will do ___ by doing…"
Integration and implementation	Addresses 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.	• How strategy is linked to or superseded other documents and strategies • Describe progress made since previous strategy or plan • Why activities in this plan are prioritized differently than in other plans • Crosswalk(s)

Source: GAO. | GAO-20-629

In addition, to evaluate the executive branch's plan to manage the strategy's implementation, we provided to each federal entity identified in the first objective a list of all *Implementation Plan* activities for which they were assigned a lead or supporting role. We documented the federal agencies' responses indicating the extent to which they were aware of their assigned activities and examples of actions taken to fulfill them. We also interviewed NSC staff to understand the *Implementation Plan's* development process and the executive branch's approach and mechanisms to oversee the execution of *Implementation Plan* activities.

We conducted this performance audit from November 2018 to September 2020 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.

Appendix II: Key Federal Entities' Cybersecurity-related Roles and Responsibilities

Federal entities have a variety of roles and responsibilities for supporting the nation's cybersecurity, as defined in legislation, policies, strategies, and other guidance. Tables 2 through 20 present 23 key federal entities' cybersecurity-related roles and responsibilities with respect to developing policies, monitoring critical infrastructure protection efforts, sharing information, responding to cyber incidents, investigating cyberattacks, and conducting research.

Table 2: White House: Executive Offices of the President Cybersecurity-related Roles and Responsibilities

EOP components	Roles and responsibilities
National Security Council	Advises and assists the President on national security and foreign policies and for coordinating these policies among various government agencies. Coordinates with departments, agencies, and the Office of Management and Budget to determine the resources needed to support the *National Cyber Strategy's* implementation.
Office of Management and Budget: Office of the Federal Chief Information Officer	Promotes initiatives and develops guidance intended to strengthen federal cybersecurity. Provides oversight and accountability for federal cybersecurity programs. Oversees interagency cooperation between the Department of Homeland Security and civilian agencies regarding cybersecurity efforts.
Office of Science and Technology Policy	Advises the President and members within the EOP on scientific, engineering, and technological aspects of national security, homeland security, and the technological recovery and use of resources, among other things. Manages the Networking and Information Technology Research and Development Program that funds research and development in advanced information technologies in computing, networking, and software.

Source: GAO analysis of EOP documentation. | GAO-20-629

Note: EOP = Executive Office of the President

Table 3: White House: Presidential Advisory Committees' Cybersecurity-related Roles and Responsibilities

Committees	Roles and responsibilities
National Science and Technology Council	Serves as the principal means within the executive branch to coordinate science and technology policy across entities that make up the federal research and development enterprise.
	Establishes national goals for federal science and technology policy and investment.
	Prepares research and development strategies that are coordinated across federal agencies, aimed at accomplishing multiple national goals pertaining to science and technology policy and investment.
	Leads interagency science and technology policy coordination efforts.
President's Council of Advisors on Science and Technology	Provides the President with scientific and technical information that is needed to inform public policy relating to the economy, and national and homeland security, among other things.
	Solicits information and ideas from stakeholders, including the research community, the private sector, universities, national laboratories, State and local governments, and nonprofit organizations, on contemporary topics of critical importance to the nation in order to inform policymaking.
	Provides advice to the National Science and Technology Council in response to council requests.
President's National Security Telecommunications Advisory Committee	Studies topics including cybersecurity-related issues, as determined and approved by the Executive Office of the President in coordination with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.
	Provides industry-based analyses and recommendations to the President and the executive branch regarding policy enhancements to national security and emergency preparedness telecommunications concerns, including how they relate to cybersecurity.

Source: GAO analysis of Advisory Committees' documentation. | GAO-20-629

Table 4: Central Intelligence Agency Cybersecurity-related Roles and Responsibilities

CIA components	Roles and responsibilities
Central Intelligence Agency	Provides cyber expertise in collaboration with other federal agencies for analysis and warning, information sharing, vulnerability reduction, mitigation, and critical infrastructure information systems' incident recovery activities.

Source: GAO analysis of CIA documentation. | GAO-20-629

Note: CIA = Central Intelligence Agency

Table 5: Department of Commerce Cybersecurity-related Roles and Responsibilities

DOC components	Roles and responsibilities
National Institute of Standards and Technology	Conducts research, and develops and deploys information security standards, guidance, best practices, and technology to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services.
National Telecommunications and Information Administration	Promotes U.S. national security interests in telecommunications domestically and abroad. Works to detect spoofing and build a safer online environment for users through increased internet security. Develops policies on issues related to the internet economy, including online privacy, copyright protection, cybersecurity, and the global free flow of information online. Convenes industry and other experts to find consensus around shared solutions to cybersecurity marketplace challenges.

Source: GAO analysis of DOC documentation. | GAO-20-629

Note: DOC = Department of Commerce

Table 6: Department of Defense Cybersecurity-related Roles and Responsibilities

DOD components	Roles and responsibilities
Chairman of the Joint Chiefs of Staff	Advises the President and Secretary of Defense on operational policies, responsibilities, and programs. Assists the Secretary of Defense in implementing operational responses to cyber threats and ensures cyberspace plans and operations are compatible with other military plans and operations.[a]
Defense Information Systems Agency	Develops, implements, and manages cybersecurity for the department's network and works with other components to secure DOD systems.
DOD Chief Information Officer	Oversees and coordinates information assurance and computer network defense across DOD. Oversees the DIB Cybersecurity Program, including those related to DOD Cyber Crime Center activities. Develops and coordinates additional policy guidance.
DOD Components	Ensures that IT under DOD component heads' (e.g., Secretaries of the Air Force, Army, and Navy) purview complies with DOD Instruction 8500.01.[b]
DOD Cyber Crime Center	Provides digital and multimedia forensic services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the DOD mission areas of: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, counterterrorism, and safety inquiries. Shares cyber threat information from the Defense Industrial Base across the government as one of six designated Federal Cyber Centers.[c] Provides mitigation and remediation strategies as well as analyst-to-analyst exchanges to protect DOD information on contractor networks or information systems.
Geographic Combatant Commands	Directs and manages Command, Control, Communications, Computers, and Intelligence Environment. Protects and secures identified combatant commands constructed networks and Mission Relevant Terrain-Cyber within their area of operations assigned by USCYBERCOM.

DOD components	Roles and responsibilities
	Coordinates Cyberspace Effects Operations.
National Guard Bureau	Operates as channel of communication and conducts multi-directional information sharing on multiple networks between DOD mission partners, Chief National Guard Bureau and the 54 states and territories.
National Security Agency	Protects national security systems, including networks that contain classified information, or that are critical to military and intelligence missions. Provides foreign Signals Intelligence[d] to the nation's policymakers, including all departments of the Executive Branch, and military forces.
Office of the Under Secretary of Defense for Acquisition and Sustainment	Develops, updates, and implements policy and processes into the DOD acquisition process for improved protection of DOD information transiting or residing on unclassified DIB information systems.
Office of the Under Secretary of Defense for Policy	Serves as the principal staff assistant to the Secretary of Defense on the risk management of defense critical infrastructure. Manages the assigned sector-specific agency responsibilities for the national DIB sector. *Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, and the Deputy Assistant Secretary of Defense for Cyber Policy* Develops, coordinates, and oversees policy associated with protection of DOD's policy implementation of the Defense Critical Infrastructure Program, Homeland Security Presidential Directive 7, and the National Infrastructure Protection Plan. Coordinates assigned sector-specific agency responsibilities pertaining to DIB cybersecurity activities with the Under Secretary of Defense for Acquisition and Sustainment, and the DOD Chief Information Officer, as appropriate, in accordance with the DHS National Infrastructure Protection Plan and the DOD and DHS DIB Critical Infrastructure and Key Resources Sector-Specific Plan. Represents the Secretary of Defense in interagency cybersecurity policy matters and leads DOD coordination of cybersecurity plans, activities, and support with DHS, other federal agencies, and international partners.
Principal Cyber Advisor	Serves as principal advisor to the Secretary of Defense on cyber-related activities, including policy and operational considerations, resources, personnel, acquisition, and technology. Oversees implementation of the *DOD Cyber Strategy* and other relevant policy and planning documents to help achieve DOD's cyber mission, goals, and objectives.
U.S. Cyber Command	Coordinates cyberspace planning and operations in collaboration with domestic and international partners. Coordinates with the DOD Chief Information Officer, National Security Agency, Department of Homeland Security, Federal Bureau of Investigation, sector-specific agencies, and critical infrastructure partners to share threat information, conduct collaborative analyses of vulnerabilities and threats, and mitigate those risks. Leads coordination efforts for cyberspace operations when infrastructure protection requirements affect more than one defense sector.

Source: GAO analysis of DOD documentation. | GAO-20-629

Note: DOD = Department of Defense; IT = information technology; USCYBERCOM = U.S. Cyber Command

[a]Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (June 8, 2018).

[b]Department of Defense, *Cybersecurity*, Instruction 8500.01 (Mar. 14, 2014, incorporating Change 1, Oct. 7, 2019).

[c]The six federal cyber centers include the Department of Defense's Cyber Crime Center and U.S. Cyber Command Joint Operations Center, the Department of Homeland Security's National Cybersecurity and Communications Integration Center, the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, the National Security Agency's Cybersecurity Threat Operations Center, and the Office of the Director of National Intelligence's Intelligence Community—Security Coordination Center. The four primary centers of cyber threat analysis excellence include the Central Intelligence Agency, the Defense Intelligence Agency, the Department of Homeland Security, and the Federal Bureau of Investigation

[d]Signals Intelligence (SIGINT) is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a window for the nation into foreign adversaries' capabilities, actions, and intensions.

Table 7: Department of Energy Cybersecurity-related Roles and Responsibilities

DOE components	Roles and responsibilities
National Laboratories	Conducts projects and activities aimed at protecting energy sector cybersecurity.
Office of Cybersecurity, Energy Security, and Emergency Response	Performs DOE's sector-specific agency responsibilities for the energy sector, which comprises the electricity subsector, and the oil and natural gas subsector.
	Provides situational awareness and subject matter expertise to help facilitate the restoration of energy systems following a cyber-incident.
	Works with public and private sector entities to accelerate the research, development, and demonstration of next-generation cyber-resilient energy delivery systems and components.

Source: GAO analysis of DOE documentation. | GAO-20-629

Note: DOE = Department of Energy

Table 8: Department of Health and Human Services Cybersecurity-related Roles and Responsibilities

HHS components	Roles and responsibilities
Office of the Assistant Secretary for Preparedness and Response	Performs HHS's sector-specific agency responsibilities for the healthcare and public health sector.
	Coordinates and collaborates with DHS and other relevant federal agencies, with critical infrastructure owners and with State, Local, Tribal, and Territorial entities, as appropriate, to implement DHS Cybersecurity and Infrastructure Security Agency requirements and presidential directives.
	Works with the private sector and Federal State, Local, Tribal, and Territorial entities to manage the overall HPH cyber risks and to strengthen the security and resilience of the HPH critical infrastructure and enhance sharing of cyber risks and threat information.
	Leads and coordinates the preparedness and response related activities for major sector wide cybersecurity incidents.
Food and Drug Administration	Develops regulatory decisions about the information security of medical devices in collaboration with the Assistant Secretary for Preparedness.
	Performs HHS's sector-specific agency responsibilities for the food and agriculture sector, in conjunction with the United States Department of Agriculture.

HHS components	Roles and responsibilities
Office of the Chief Information Officer	Fulfills HHS's implementation of the *Cybersecurity Act of 2015*, which calls for the establishment of a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks. Fulfills the implementation of the *Cybersecurity Information Sharing Act of 2015*, which calls for federal entities to develop and issue procedures to facilitate timely sharing of cyber threat indicators.
Office for Civil Rights	Enforces the information security regulations of healthcare and services in coordination with the Assistant Secretary for Preparedness as outlined in law, specifically the *Health Insurance Portability and Accountability Act* and the *Health Information Technology and Economic and Clinical Health Act of 2009*.

Source: GAO analysis of HHS documentation. | GAO-20-629

Note: DHS = Department of Homeland Security; HHS = Health and Human Services; HPH = Healthcare and Public Health

Table 9: Department of Homeland Security Cybersecurity-related Roles and Responsibilities

DHS components	Roles and responsibilities
Cybersecurity and Infrastructure Security Agency	*National Risk Management Center* Collaborates with public and private stakeholders to identify, analyze, prioritize, and manage strategic risks to the nation's critical infrastructure. Uses its supply chain risk management task force to work with government and industry partners to ensure that supply chain risk management is integrated into efforts in CISA and DHS. Works to ensure the physical security and cybersecurity of voter registration data bases, IT infrastructure used to count, audit, and display results as well as polling places and storage facilities. *Cybersecurity Division* Supports the security of federal information and information systems (i.e., .gov environment) through threat detection and analysis and information sharing functions. Helps critical infrastructure businesses make better decisions about where to put resources to enhance cybersecurity before an event occurs to disrupt it and to improve recovery in case such an event occurs. Develops processes to ensure the timely production of unclassified reports of cyber threats to the United States that identify a specific targeted entity. Coordinates with the Secretary of Defense to establish procedures to expand the Enhanced Cybersecurity Services program, a voluntary information sharing program that provides classified cyber threat and technical information to all critical infrastructure sectors. Jointly with Secretary of Commerce led an open and transparent process to identify and promote action by appropriate parties to improve the resilience of the internet and communications systems and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). *Emergency Communications Division* Provides planning, resources, and training to support and enhance operable and interoperable emergency communications for first responders and support implementation of the National Emergency Communications Plan and development of Statewide Communication Interoperability Plans.

DHS components	Roles and responsibilities
	Infrastructure Security Division Provides strategic guidance, promotes a national unity of effort, and coordinates the overall federal effort to promote the security and resilience of critical infrastructure. Fulfills other evaluation, coordination, and reporting responsibilities related to the national infrastructure and cybersecurity. Examines the sufficiency of existing federal policies and practices to promote awareness of cybersecurity risk management practices by critical infrastructure entities. Carries out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States. Uses its supply chain risk management task force to work with government and industry partners to ensure that supply chain risk management is integrated into efforts in CISA and DHS. Works to ensure the physical security and cybersecurity of voter registration databases, including the IT infrastructure used to count, audit, and display results as well as polling places and storage facilities. *Integrated Operations Division* Ensures that all CISA's externally facing activities are coordinating, collaborating, and communicating across divisions to allow for seamless support and fast response to critical needs. Provides a single reporting channel to give leadership end-to-end operational visibility for physical, cyber, and emergency communications activities. *Stakeholder Engagement Division* Fulfills sector-specific agency function—implementing activities to enhance security—for the chemical, commercial facilities, communications, critical manufacturing, dams, emergency services, information technology, and nuclear reactors, materials, and waste sectors.
Federal Emergency Management Agency	Provides anonymous cybersecurity gap analyses to help state, local, tribal, and territorial partners inventory their cybersecurity capabilities and identify existing gaps. Provides organizations with centralized cybersecurity best practices and guidance on their cybersecurity capabilities through the National Cyber Resilient Architecture. Developed multi-tier training to help organizations better understand the importance of cybersecurity.
Transportation Security Administration	Manages the Pipeline Cybersecurity Initiative with CISA/National Risk Management Center and uses its technical cybersecurity capabilities to identify and mitigate cyber vulnerabilities to the oil and natural gas pipeline systems. This initiative enables pipeline owners and operators to identify and mitigate potential vulnerabilities through direct engagement with the federal government. Co-leads with the Coast Guard in DHS and with the Department of Transportation as the sector-specific agencies for the transportation systems sector. Co-leads an Aviation Cybersecurity Initiative Working Group on Airports with the Federal Aviation Administration, collaborating with government and transportation industry partners to reduce cybersecurity risks and improve cyber resilience in the aviation ecosystem, specifically in the airport environment.

DHS components	Roles and responsibilities
U.S. Coast Guard	Co-leads with TSA in DHS and with the Department of Transportation as the sector-specific agencies for the transportation systems sector, specifically to help protect public and private maritime infrastructure owners and operators from cyber threats. Charged with preventing and responding to transportation security incidents that take place in the maritime domain.
U.S. Immigration and Customs Enforcement	Delivers computer-based technical services to support domestic and international investigations into cross-border crime and support to combat cybercrime and training to federal, state, local, and international law enforcement agencies. Develops and coordinates investigations of immigration and customs violations for which the internet is used to commit financial fraud, money laundering, identity and benefit fraud, the sale and distribution of narcotics and other controlled substances, arms trafficking, and the export of controlled commodities.
U.S. Secret Service	Identifies and mitigates risks from malicious cyber actors to protected persons, facilities, and events. Investigates cybercrimes and develops counter measures against cyber threats to financial and payment systems including through financial and electronic crime taskforces with other law enforcement agencies.

Source: GAO analysis of DHS documentation. | GAO-20-629

Note: CISA = Cybersecurity and Infrastructure Security Agency; DHS = Department of Homeland Security; IT = Information Technology; TSA = Transportation Security Administration

Table 10: Department of Justice Cybersecurity-related Roles and Responsibilities

DOJ components	Roles and responsibilities
Criminal Division	*Computer Crime and Intellectual Property Section* Implements DOJ national strategies to combat computer and intellectual property crimes worldwide by working with other DOJ components and government agencies, the private sector, academic institutions, and foreign counterparts, among others.
	Prosecutes violations of federal law involving cyber intrusions and cyberattacks. *Office of International Affairs* Leverages extradition treaties, mutual legal assistance treaties, and other available legal methods to support U.S. investigations and prosecutions of cybercriminals
Drug Enforcement Agency	Develops and maintains equipment, capabilities, and tools to support investigations and assists with technical operations.
Federal Bureau of Investigation	Has primary investigative authority for all computer network intrusions relating to threats to national security, including cases involving espionage, foreign counterintelligence, and information protected against unauthorized disclosure for reasons of national defense or foreign relations. Notifies and disseminates pertinent information to victims in a timely manner to the extent to which such notification does not interfere with ongoing law enforcement investigations or law enforcement/intelligence community operations, or expose sources, methods, or technologies.
INTERPOL Washington	Advances the cybercrime investigations of U.S. law enforcement by establishing and maintaining relationships with the heads of other countries, sharing information through a secure communications platform to assist cybercrime investigations.

DOJ components	Roles and responsibilities
National Security Division	*Counterintelligence and Export Control Section*
	Implements DOJ national strategies to investigate and prosecute cases affecting national security, including espionage, counterproliferation, export control, embargo, neutrality, atomic energy, and foreign agent registration, and state sponsored cybercrimes, and serves as the DOJ's primary liaison with the United States Intelligence Community.
	Prosecutes violations of federal law involving cyber intrusions and cyberattacks by nation-state intelligence and military services and their proxies.
	Counterterrorism Section
	Implements DOJ national strategies to investigate and prosecute cases affecting national security, including domestic and international terrorism, terrorism financing, and material support to terrorist organization.
	Prosecutes violations of federal law involving terrorist use of the internet and cyberattacks by members of terrorist organization.

Source: GAO analysis of DOJ documentation. | GAO-20-629

Note: DOJ = Department of Justice; INTERPOL = International Criminal Police Organization

Table 11: Department of State Cybersecurity-related Roles and Responsibilities

State's components	Roles and responsibilities
Bureau of Counterterrorism	Engages in diplomatic efforts to counter violent extremism and use of the internet by terrorists, and to boost critical infrastructure security and resilience.
Bureau of Democracy, Human Rights, and Labor	Leads diplomatic engagement on internet freedom issues.
Bureau of Economic and Business Affairs	Leads diplomatic engagement on digital economy issues.
	Coordinates the Digital Connectivity and Cybersecurity Partnership.
	Provides developing country officials training on Information Communications Technology regulations and deployments.
	Leads international campaign on 5G security.
Bureau of Intelligence and Research	Performs intelligence analysis and operational coordination.
Bureau of International Narcotics and Law Enforcement Affairs	Leads diplomatic efforts on combatting cybercrime, including international engagement and negotiations on cybercrime, and cybercrime capacity building.
Bureau of International Organization Affairs	Engages with international organizations involved in cyber issues.
Office of the Coordinator for Cyber Issues	Coordinates cyber diplomacy efforts to ensure State coordination on cyber issues.
	Leads cyber diplomacy efforts with international partners to further global cyber stability.
Office of the Legal Advisor	Advises on all legal issues—domestic and international—arising in the course of the State's work. This includes assisting agency principals and policy officers in formulating and implementing U.S. foreign policies (including policies related to cybersecurity and internet freedom), and promoting the adherence to, and development of, international law and its institutions.
Regional Bureaus	Coordinates regional approaches to implement the *National Cyber Strategy* through engagement with host countries, in coordination with the Office of the Coordinator for Cyber Issues.

Source: GAO analysis of State documentation. | GAO-20-629

Note: State = Department of State

Table 12: Department of Transportation Cybersecurity-related Roles and Responsibilities

DOT components	Roles and responsibilities
Federal Aviation Administration	Sustains and improves cybersecurity in the aviation ecosystem through relationships with external partners in government and industry.
Federal Highway Administration	Develops and deploys innovative practices and technologies to improve the safety and performance of the transportation system. Researches the safety, mobility, and economic benefits of automation; the impacts of automation on infrastructure, commercial drivers, and other road users; the cybersecurity of those systems; and better access for people with disabilities, public safety, and first responders.
Maritime Administration	Works to strengthen the maritime transportation system (landside infrastructure, the shipbuilding and repair industry, and labor) to meet national economic and national security needs.
National Highway Traffic Safety Administration	Works to save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement.
Office of the Assistant Secretary for Research and Technology	Works to improve the nation's transportation system by anticipating emerging issues and advancing technical, operational, and institutional innovations.
Office of Intelligence, Security and Emergency Response	Ensures development, coordination, and execution of plans and procedures for DOT to balance transportation security requirements with the safety, mobility, and economic needs of the nation through effective intelligence, security, preparedness, and emergency response programs.

Source: GAO analysis of DOT documentation. | GAO-20-629

Note: DOT = Department of Transportation

Table 13: Department of the Treasury Cybersecurity-related Roles and Responsibilities

Treasury components	Roles and responsibilities
Office of Cybersecurity and Critical Infrastructure Protection	Performs Treasury's sector-specific agency responsibilities for the financial services sector including collaborating with financial services sector companies, federal and state regulators, the Financial and Banking Information Infrastructure Committee, and the Financial Services-Information Sharing and Analysis Center regarding public policy proposals and implementation plans that strengthen the cybersecurity and resilience of the sector. Collaborates with the Departments of Energy and Homeland Security on cybersecurity issues and incident response planning.
Office of Intelligence and Analysis	Provides current and strategic intelligence analysis and support to the department, interagency, and the financial services sector through the Office of Cybersecurity and Critical Infrastructure Protection on malicious cyber activities against the sector and its critical financial infrastructure, Office of Foreign Asset Control cyber sanctions, as well as developments in the illicit use of financial technology.

Source: GAO analysis of Treasury documentation. | GAO-20-629

Note: Treasury = Department of the Treasury

Table 14: Environmental Protection Agency Cybersecurity-related Roles and Responsibilities

EPA components	Roles and responsibilities
Office of Homeland Security	Coordinates with the Office of the Director of National Intelligence and Intelligence Community agencies to facilitate information sharing, increase threat awareness, and leverage intelligence analysis support to alert organizations of potential or actual infrastructure cyberattacks.
Office of Research and Development	Conducts research to improve water utilities' abilities to prepare for, and respond to, all hazardous incidents that threaten public health.
Office of Water	Performs EPA's sector-specific agency responsibilities for the water and wastewater systems sector, in conjunction with the Department of Homeland Security's Federal Protective Service.

Source: GAO analysis of EPA documentation. | GAO-20-629

Note: EPA = Environmental Protection Agency

Table 15: Federal Chief Information Officers Council Cybersecurity-related Roles and Responsibilities

Federal CIO Council components	Roles and responsibilities
Federal Chief Information Officers Council	Leverages FISMA quarterly reporting and agency cybersecurity budget enhancements to meet the key federal cybersecurity priorities across the enterprise including increasing cyber threat awareness, standardizing cyber and IT capabilities, and driving agency accountability.

Source: GAO analysis of Federal Chief Information Officers Council documentation. | GAO-20-629

Note: CIO = Chief Information Officer; FISMA = Federal Information Security Modernization Act; IT = Information Technology

Table 16: Federal Communications Commission Cybersecurity-related Roles and Responsibilities

FCC components	Roles and responsibilities
Communications Security, Reliability and Interoperability Council	Provides recommendations to the FCC to help ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety. Focuses on a range of public safety and homeland security-related communications matters, including, but not limited to: (1) the reliability and security of communications systems and infrastructure, particularly mobile systems; (2) 911, Enhanced 911, and Next Generation 911; and (3) emergency alerting.
International Bureau	Consults with Executive Branch agencies for feedback on national security, law enforcement, foreign policy, or trade policy risks to communications networks. Reviews applications from domestic and foreign entities seeking authority to provide international telecommunications services in the United States. Executes the President's authority to grant, deny, or condition applications for authority to build and operate international undersea telecommunications cables. Considers petitions to allow holders of wireless licenses to accept substantial foreign ownership (over 25%).
Public Safety and Homeland Security Bureau	*Cybersecurity and Communications Reliability Division* Works with the communications industry and other related organizations to develop and implement improvements to the reliability and security of the U.S. communications infrastructure.

FCC components	Roles and responsibilities
	Provides legal, engineering, and other technical advice and expertise to the Bureau and the Commission regarding public safety and homeland security issues that may affect the reliability, resilience and security of communications networks. Coordinates with federal agency and industry partners on outreach and information sharing about network threats and network security best practices. Administers FCC's information collection requirements for communications reliability related to: network outage reporting system, disaster information reporting system, and 911 reliability certification. *Operations and Emergency Management Division* Maintains FCC preparedness to respond to major communications incidents and coordinates incident management activities. **Policy and Licensing Division** Reviews and maintains systems security and integrity plans submitted by all telecommunications carriers pursuant to the *Communications Assistance for Law Enforcement Act*.[a]
Wireline Competition Bureau	Leads the development and implementation of policies with respect to the Universal Service Fund, which includes consideration of national and network security. Administers FCC's policy pursuant to section 222,[b] which governs telecommunications carriers' responsibilities to protect proprietary information about customers.
Wireless Telecommunications Bureau	Leads the development and implementation of policies with respect to 5G and FCC's 5G FAST Plan, which is a comprehensive strategy to facilitate America's superiority in 5G technology.

Source: GAO analysis of FCC documentation. | GAO-20-629

Note: FCC = Federal Communications Commission

[a]*Communications Assistance for Law Enforcement Act*, Pub. L. No. 103-414, 108 Stat. 4279 (codified, as amended, at 47 U.S.C. §§ 1001-1010).

[b]Section 222 of the *Telecommunications Act of 1996*, Pub. L. 104-104, is codified in 47 U.S.C. § 222. It requires telecommunications carriers to protect the privacy and confidentiality of proprietary/personal information of customers and other carriers.

Table 17: General Services Administration Cybersecurity-related Roles and Responsibilities

GSA components	Roles and responsibilities
Federal Acquisition Service–Office of Information Technology Category	Provides federal agencies with access to information technology and cybersecurity products and services through various types of contracts.
Office of Government-wide Policy	Manages the Federal Identity, Credential, and Access Management program, which provides the tools, policies, and systems that allow federal agencies to manage, monitor, and secure access to protected electronic and physical resources.
Office of Mission Assurance	Performs GSA's sector-specific agency responsibilities for the government facilities sector, in conjunction with the Department of Homeland Security's Federal Protective Service.

Source: GAO analysis of GSA documentation. | GAO-20-629

Note: GSA = General Services Administration

Table 18: National Science Foundation Cybersecurity-related Roles and Responsibilities

NSF components	Roles and responsibilities
Computer and Information Science and Engineering	*Division of Computing and Communication Foundations* Develops and directs funding programs that support research and education on mathematical, scientific, and technological foundations of computing, information, and communications. *Division of Computer and Network Systems* Supports research and education activities that invent new computing and networking technologies and explore new ways to make use of existing technologies. Supports the computing infrastructure that is required for experimental computer science and coordinates cross-divisional activities that foster the integration of research, education, and workforce. *Division of Information and Intelligent Systems* Studies the inter-related roles of people, computers, and information by supporting research and education activities that: (1) develop new knowledge about the role of people in the design and use of information technology; (2) increase the capability to create, manage, and understand data and information in circumstances ranging from personal computers to globally-distributed systems; and (3) advance the understanding of how computational systems can exhibit the hallmarks of intelligence. *Office of Advanced Cyberinfrastructure* Supports and coordinates the development, acquisition, and provision of state-of-the-art cyberinfrastructure resources, tools, and services essential to the advancement and transformation of science and engineering. Supports forward-looking research and education to expand the future capabilities of cyberinfrastructure specific to science and engineering.
Education and Human Resources	Supports the growth and improvement of cybersecurity education programs at community colleges through the Advanced Technological Education program. Builds the technician-level workforce in cybersecurity by growing and enhancing associate degree programs and certificate programs. Develops cybersecurity program and cybersecurity workforce. Builds education capacity and innovate cybersecurity education. Supports individual research projects related to cybersecurity education for K-12 students.
Engineering	Supports the integration of computation, data analysis and interdisciplinary research partnerships and perspectives for the advancement of knowledge in all of its core programs. Funds research to enable advances in a variety of areas, including resilient and sustainable civil infrastructure and distributed infrastructure networks. Supports fundamental research in Electrical, Communications and Cyber Systems core programs and special initiatives such as smart grid, technology for trustworthy and secure systems, cyber-physical systems, hardware security, and analog security. Supports projects in emerging cybersecurity areas. Supports programs to accelerate NSF-funded and federally funded fundamental research into market opportunities, and fosters public-private partnerships to advance technological innovation.

NSF components	Roles and responsibilities
Mathematical and Physical Sciences	Supports both disciplinary and interdisciplinary activities and partner with other NSF directorates in order to effectively encourage research across the scientific disciplines
	Addresses scientific questions, educates the future advanced high-tech workforce, and promotes discoveries to meet the needs of the Nation.

Source: GAO analysis of NSF documentation. | GAO-20-629

Note: NSF = National Science Foundation

Table 19: Office of the Director of National Intelligence Cybersecurity-related Roles and Responsibilities

ODNI components	Roles and responsibilities
Cyber Threat Intelligence Integration Center	Serves as a center for government partners to coordinate with and receive contextualized threat intelligence.
	Coordinates government response to significant cyber events in collaboration with the Federal Bureau of Investigation and the Department of Homeland Security.
Intelligence Community Chief Information Officer	Oversees IC information security policies and practices for IC national security systems.
	Develops and oversees implementation of policies, principles, standards, and guidelines on information security.
	Oversees IC element's compliance with the Federal Information Security Modernization Act.
Intelligence Community—Security Coordination Center	Serves as the Federal Cyber Center responsible for integrated defense of the intelligence community's information environment on behalf of the Director of National Intelligence and the IC chief information officer.
National Aviation Intelligence—Integration Office	Ensures the mitigation of cyber threats to the aviation sector.
National Counterintelligence and Security Center	Provides strategic policy guidance to lower the risk associated with supply chains.
	Ensures the proper integration of counterintelligence and computer network defense across the IC.
	Creates reports on foreign intelligence threats to U.S. critical infrastructure.
National Intelligence Manager for Cyber	Serves as the principal adviser for the IC and provides strategic oversight of cyber threat intelligence activities and issues across relevant regions, countries, and issues that may have a role in cybersecurity.
National Intelligence Manager for Space and Technical Intelligence	Implements the National Strategy for Space and pursues additional protection across national, military, civil, and commercial space sectors to meet space and cyber strategy objectives.
National Intelligence Officer for Cyber	Serves on the National Intelligence Council, the IC's center for long-term strategic analysis, and provides judgments and assessments on long-term national security issues.
National Maritime Intelligence—Integration Office	Ensures cyber threats to maritime infrastructure—vessels, ports, and related offshore sectors—are mitigated.

Source: GAO analysis of ODNI documentation. | GAO-20-629

Note: IC = Intelligence Community; ODNI = Office of the Director of National Intelligence

Table 20: United States Department of Agriculture Cybersecurity-related Roles and Responsibilities

USDA components	Roles and responsibilities
Office of Homeland Security	Performs USDA's sector-specific agency responsibilities for the food and agriculture sector, in conjunction with the U.S. Department of Health and Human Services, Food and Drug Administration.

Source: GAO analysis of USDA documentation. | GAO-20-629

Note: USDA = United States Department of Agriculture

Appendix III: National Cyber Strategy Implementation Plan Activity Responsibilities

Table 21: Entities' Assigned Tier 1, 2, and 3 Activities in the *National Cyber Strategy Implementation Plan*

Entity	Number of Tier 1[a] activities entity is assigned as a lead or co-lead entity	Number of Tier 1 activities entity is assigned as a support or co-support entity	Number of Tier 2[b] activities entity is assigned as a lead or co-lead entity	Number of Tier 2 activities entity is assigned as a support or co-support entity	Number of Tier 3[c] activities entity is assigned as a lead or co-lead entity	Number of Tier 3 activities entity is assigned as a support or co-support entity
Central Intelligence Agency	-	1	-	1	-	1
Department of Commerce (DOC)	1	8	3	9	11	7
DOC – International Trade Administration	-	-	-	-	2	-
DOC – National Institute of Standards and Technology	3	2	5	4	14	14
DOC – National Oceanic and Atmospheric Administration		1	-	-	-	-
DOC – National Telecommunications and Information Administration	1	3	1	-	8	1
DOC – U.S. Patent and Trademark Office	-	-	-	1	-	-
Department of Defense (DOD)	1	19	3	13	9	26
DOD – National Security Agency	-	11	3	9	8	13
Department of Energy (DOE)	-	8	2	5	7	14
DOE – Federal Energy Regulatory Commission	-	-	-	1	-	-
DOE – National Laboratories	-	-	1	-	-	2
Department of Health and Human Services (HHS)	-	6	-	3	5	12
HHS – Food and Drug Administration	-	-	-	-	1	1

Entity	Number of Tier 1[a] activities entity is assigned as a lead or co-lead entity	Number of Tier 1 activities entity is assigned as a support or co-support entity	Number of Tier 2[b] activities entity is assigned as a lead or co-lead entity	Number of Tier 2 activities entity is assigned as a support or co-support entity	Number of Tier 3[c] activities entity is assigned as a lead or co-lead entity	Number of Tier 3 activities entity is assigned as a support or co-support entity
Department of Homeland Security (DHS)	12	18	18	18	13	45
DHS – Cybersecurity and Infrastructure Security Agency	-	-	-	-	-	2
DHS – Transportation Security Administration	-	-	-	-	1	-
DHS – U.S. Coast Guard	2	-	1	-	1	-
DHS – U.S. Secret Service	-	-	-	-	-	1
Department of Justice (DOJ)	1	5	7	6	2	4
DOJ – Federal Bureau of Investigation	-	5	3	6	3	8
Department of State	2	4	5	5	11	8
Department of Transportation (DOT)	1	13	-	5	1	16
DOT – Federal Highway Administration	-	-	-	-	1	2
DOT – Intelligent Transportation System – Joint Program Office	-	-	-	-	3	-
DOT – National Highway Safety Administration	-	-	-	-	-	1
Department of the Treasury	-	7	-	4	6	14
Environmental Protection Agency	-	6	-	2	1	11
Executive Office of the President	1	-	-	-	-	-
Federal Chief Information Officers Council	-	-	-	-	-	1
Federal Communications Commission	-	4	-	2	2	1
General Services Administration	1	9	2	5	1	15
National Science Foundation	-	1	-	1	3	5
National Science and Technology Council	-	-	1	1	-	-
National Security Council	15	2	7	-	3	1

Entity	Number of Tier 1[a] activities entity is assigned as a lead or co-lead entity	Number of Tier 1 activities entity is assigned as a support or co-support entity	Number of Tier 2[b] activities entity is assigned as a lead or co-lead entity	Number of Tier 2 activities entity is assigned as a support or co-support entity	Number of Tier 3[c] activities entity is assigned as a lead or co-lead entity	Number of Tier 3 activities entity is assigned as a support or co-support entity
Office of the Director of National Intelligence (ODNI)	-	6	2	3	2	7
ODNI – National Maritime Intelligence-Integration Office	-	1	-	2	-	-
Office of Management and Budget	7	2	6	5	5	8
Office of Science and Technology Policy	-	1	-	2	3	-
United States Department of Agriculture	-	6	-	2	1	11

Source: National Security Council, *National Cyber Strategy Implementation Plan* (Washington, D.C.: June 2019). | GAO-20-629

[a]Tier 1: Activities that the National Security Council (NSC) Cyber directorate will use the Cyber Policy Coordinate Committee (PCC) to coordinate implementation of or may require endorsement from the Deputies Committee, chaired by the Deputy National Security Advisor, to implement. PCCs are responsible for the management of the development and implementation of national security policies by multiple executive departments and agencies. PCCs are to provide policy analysis for consideration by the more senior committees of the nation security systems and ensure timely responses to the President's decisions.

[b]Tier 2: Activities that departments and agencies will implement with significant interest from the Cyber directorate and that may require Cyber PCC coordination to implement.

[c]Tier 3: Activities that departments and agencies will implement with periodic reporting to the Cyber directorate on their progress toward accomplishing the objectives.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kush K. Malhotra (Assistant Director), Kenneth A. Johnson (Analyst-in-Charge), Bradley W. Becker, Anna Bennett, Christina Bixby, David Blanding, Jr., Chris Businsky, Michael W. Gilmore, Hoyt Lacy, Priscilla Smith, and Paige Teigen made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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