



February 2020

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

GAO Highlights

Highlights of [GAO-20-299](#), a report to congressional committees

Why GAO Did This Study

Cyber threats to the nation's critical infrastructure (e.g., financial services and energy sectors) continue to increase and represent a significant national security challenge. To better address such threats, NIST developed, as called for by federal law, a voluntary framework of cybersecurity standards and procedures.

The *Cybersecurity Enhancement Act of 2014* included provisions for GAO to review aspects of the framework. The objectives of this review were to determine the extent to which (1) SSAs have developed methods to determine framework adoption and (2) implementation of the framework has led to improvements in the protection of critical infrastructure from cyber threats. GAO analyzed documentation, such as implementation guidance, plans, and survey instruments. GAO also conducted semi-structured interviews with 12 organizations, representing six infrastructure sectors, to understand the level of framework use and related improvements and challenges. GAO also interviewed agency and private sector officials.

What GAO Recommends

GAO is making ten recommendations—one to NIST on establishing time frames for completing selected programs—and nine to the SSAs to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. GAO continues to believe that all ten recommendations are warranted.

View [GAO-20-299](#). For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

February 2020

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

What GAO Found

Most of the nine agencies with a lead role in protecting the 16 critical infrastructure sectors, as established by federal policy and referred to as sector-specific agencies (SSAs), have not developed methods to determine the level and type of adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (framework), as GAO previously recommended. Specifically, two of the nine SSAs had developed methods and two others had begun taking steps to do so. The remaining five SSAs did not yet have methods to determine framework adoption. Most of the sectors (13 of 16), however, noted that they had taken steps to encourage and facilitate use of the framework, such as developing implementation guidance that links existing sector cybersecurity tools, standards, and approaches to the framework. In addition, all of the 12 selected organizations that GAO interviewed described either fully or partially using the framework. Nevertheless, implementing GAO's recommendations to the SSAs to determine the level and type of adoption remains essential to the success of protection efforts.

The 12 selected organizations using the framework reported varying levels of resulting improvements. Such improvements included identifying risks and implementing common standards and guidelines. However, the SSAs have not collected and reported sector-wide improvements. The SSAs and organizations identified impediments to doing so, including the (1) lack of precise measurements of improvement, (2) lack of a centralized information sharing mechanism, and (3) voluntary nature of the framework. NIST and the Department of Homeland Security (DHS) have initiatives to help address these impediments.

- **Precise measurements:** NIST is in the process of developing an information security measurement program that aims to provide the tools and guidance to support the development of information security measures that are aligned with an individual organization's objectives. However, NIST has not established a time frame for the completion of the measurement program.
- **Centralized sharing:** DHS identified its homeland security information network as a tool that was intended to be the primary system that could be used by all sectors to report on best practices, including sector-wide improvements and lessons learned from using the framework.
- **Voluntary nature:** In April 2019, NIST issued its *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, version 1.1, which included a tool for organizations to self-assess how effectively they manage cybersecurity risks and identify improvement opportunities.

While these initiatives are encouraging, the SSAs have not yet reported on sector-wide improvements. Until they do so, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructures from threats will be largely unknown.

Contents

Letter		1
	Background	4
	Most SSAs Have Not Developed Methods to Determine Framework Adoption	12
	Selected Organizations Reported Improvements but SSAs Have Not Collected and Reported Sector-Wide Improvements Resulting from Framework Use	20
	Conclusions	26
	Recommendations	27
	Agency Comments and Our Evaluation	28
Appendix I	Objectives, Scope, and Methodology	32
Appendix II	Comments from the Department of Agriculture	36
Appendix III	Comments from the Department of Commerce	37
Appendix IV	Comments from the Department of Defense	40
Appendix V	Comments from the Department of Energy	42
Appendix VI	Comments from the Department of Health and Human Services	45
Appendix VII	Comments from the Department of Homeland Security	47
Appendix VIII	Comments from the Department of the Treasury	50

Appendix IX	Comments from the Environmental Protection Agency	52
Appendix X	Comments from the General Services Administration	54
Appendix XI	GAO Contact and Staff Acknowledgments	55
Table	Table 1: Critical Infrastructure Sectors that Developed Cybersecurity Implementation Guidance to Facilitate Use of the Framework	17
Figures	Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies	6
	Figure 2: Number of Entities and Organizations that Identified the Five Impediments to Identifying Sector-wide Improvement as a Result of Using the Framework	22

Abbreviations

Agriculture	U.S. Department of Agriculture
ASPR	Assistant Secretary for Preparedness and Response
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
EPA	Environmental Protection Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	information technology
NIST	National Institute of Standards and Technology
SCC	Sector Coordinating Council
SSA	Sector Specific Agency

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



February 25, 2020

The Honorable Roger Wicker
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

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

The nation’s critical infrastructure provides the essential services—such as banking, water, and electricity— that underpin American society.¹ The infrastructure relies on electronic systems and data to support its missions. However, cyber threats to the critical infrastructure continue to increase and represent a significant national security challenge. In this regard, malicious actors have intruded and extracted highly sensitive materials from the networks of a number of government agencies and major critical infrastructure companies.

To address the cyber-based threats to the critical infrastructure, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013.² This order aimed to enhance the security and resilience of the nation’s critical infrastructure and maintain a

¹The term “critical infrastructure” as defined in the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act) refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

²The White House, Executive Order No. 13636 (Washington, D.C.: February 12, 2013), 78 Fed. Reg. 11737 (Feb. 19, 2013).

cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

Among other things, the order called for the Director of the National Institute of Standards and Technology (NIST) to lead the development of a voluntary, consensus-based cybersecurity framework that would comprise a set of industry standards and best practices to help organizations manage cybersecurity risks.³ In response, NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) in February 2014 to provide private sector organizations⁴ with principles and best practices of risk management to improve the security and resilience of their critical infrastructures.⁵ In addition, the *Cybersecurity Enhancement Act of 2014* (Cybersecurity Act) authorized NIST, among other things, to facilitate and support the development of a voluntary set of standards, best practices, and procedures to reduce cyber risks to critical infrastructures on an ongoing basis.⁶

The Cybersecurity Act also included a provision for us to review, in a series of reports, various aspects of the framework. The objectives of this review were to determine the extent to which (1) agencies with a lead role in critical infrastructure protection efforts, referred to as sector-specific agencies (SSA), have developed methods to determine the level and type of framework adoption and (2) implementation of the framework has led to improvements in the protection of critical infrastructure from cyber threats.

To address the first objective, we analyzed documentation, such as implementation guidance and survey instruments on framework adoption, that discussed actions federal and nonfederal entities have taken since

³The National Institute of Standards and Technology is a component within the Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science and standards and technology in ways that enhance economic security and improve the nation's quality of life.

⁴Private sector organizations are companies (both for-profit and nonprofit), businesses, or bodies such as those within a critical infrastructure sector that are free from direct governmental control.

⁵National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). Version 1.1 of the framework was issued April 16, 2018.

⁶Pub. L. No. 113-274, § 101, 128 Stat. 2971, 2972 (Dec. 18, 2014).

our report in 2018 to determine the level and type of adoption across their sectors.⁷ These entities included SSAs, NIST, Sector Coordinating Councils (SCC), which are made up of nonfederal organizations and serve as the voice of each sector and principal entryway for the government to collaborate with each sector, and Information Sharing and Analysis Centers (ISAC).⁸ We included SSAs and SCCs representing all of the 16 critical infrastructure sectors in our review.⁹ We also analyzed documentation from NIST and the Department of Homeland Security (DHS) and interviewed officials from entities—including SSAs, SCCs, NIST, and DHS—regarding their activities to assess the level and type of framework adoption by the entities within each sector.

In addition, we selected six critical infrastructure sectors identified in the 2018 *National Cyber Strategy of the United States of America* as having critical infrastructure with the greatest risk of being compromised.¹⁰ From these sectors, we asked SCCs, trade associations (e.g., the American Petroleum Institute), and ISACs to provide a list of small or medium and large organizations that were users of the framework. We then divided up the list of identified organizations by sector, and we randomly selected one large and one small or medium organization from each sector, resulting in a final list of 12 organizations. We conducted semi-structured interviews with officials from the selected organizations to understand the extent to which these organizations were using the framework.

To address the second objective, we collected and reviewed documentation, such as survey instruments and guides from federal and nonfederal entities (NIST, SSAs, SCCs, and ISACs) that discussed their efforts to measure sector-wide improvements. We compared these efforts to best practices, such as NIST Special Publication 800-55, to identify any measures the SSAs and SCCs had established to determine

⁷GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: Feb. 15, 2018).

⁸ISACs help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards by communicating critical information and maintaining sector-wide situational awareness.

⁹We did not include sector coordinating council representatives from the following three of 16 sectors due to non-responsiveness: critical manufacturing, dams, and information technology sectors.

¹⁰The six sectors were (1) communications, (2) financial services, (3) energy, (4) healthcare and public health, (5) information technology, and (6) transportation systems.

improvements as a result of using the framework.¹¹ In addition, we interviewed officials from the selected organizations to understand the extent to which they realized improvements in cybersecurity as a result of framework adoption. We also interviewed officials from NIST, SSAs, SCCs, and the selected organizations regarding the challenges in measuring improvements and any steps taken to address those challenges. Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from January 2019 to February 2020 in accordance with generally accepted government auditing standards.¹² 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

Our nation's critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of them would have a debilitating impact on our security, economic stability, public health or safety, or any combination of these factors. Critical infrastructure includes, among other things, banking and financial institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned and operated by the private sector.

Threats to the systems supporting our nation's critical infrastructures are evolving and growing. These systems are susceptible to unintentional and intentional threats, both cyber and physical. Unintentional, or nonadversarial, threat sources include equipment failures, software coding errors, or the accidental actions of employees. They also include

¹¹National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, SP 800-55, revision 1 (Gaithersburg, MD.: July 2008). This guide is to assist in the development, selection, and implementation of measurements for use at a system or program level. Such measures are to be used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of performance-related data.

¹²We submitted a draft of this report to the Senate Committee on Commerce, Science, and Transportation and the House Committee on Science, Space, and Technology to satisfy our statutory reporting mandate on December 18, 2019.

natural disasters and the failure of other critical infrastructures, since the sectors are often interdependent.

Intentional or adversarial threats can involve targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, and disgruntled employees. Adversaries can leverage common computer software programs to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, GAO first designated federal information security as a government-wide high-risk area in our biennial report to Congress in 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information. We continue to identify the protection of critical cyber infrastructure as a high-risk area, as shown in our March 2019 high-risk update.¹³

Federal Law and Policy Assign Responsibilities for the Protection of Critical Infrastructure Sectors

Because the private sector owns the majority of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. Toward this end, federal law and policy assign roles and responsibilities for agencies to assist the private sector in protecting critical infrastructure, including enhancing cybersecurity.

Presidential Policy Directive 21 establishes the SSAs in the public sector as the federal entities responsible for providing institutional knowledge and specialized expertise.¹⁴ The SSAs lead, facilitate, and support the security and resilience programs and associated activities of their designated critical infrastructure sectors.

The directive identified 16 critical infrastructure sectors and designated the nine associated SSAs, as shown in figure 1.

¹³GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: Mar. 6, 2019).

¹⁴The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: February 2013).

Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies



Sector-specific agency

Departments of Agriculture (USDA), Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Transportation (DOT), the Treasury, Environmental Protection Agency (EPA), and the General Services Administration (GSA)

Source: GAO analysis of Presidential Policy Directive-21 and Critical Infrastructure Protection GAO-18-211; Art Explosion (clip art) | GAO-20-299

Notes: The Department of Energy's sector-specific agency responsibilities are further codified in law by the *Fixing America's Surface Transportation Act* (FAST Act). The FAST Act contains provisions designed to protect and enhance the nation's electric power delivery infrastructure.

The government facilities sector is comprised of public sector members. The sector ensures continuity of functions for facilities owned and leased by various levels of government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

The following sectors have co-sector specific agencies: food and agriculture (USDA and HHS); government facilities (DHS and GSA); and transportation systems (DHS and DOT).

In addition, the directive required DHS to update the *National Infrastructure Protection Plan*¹⁵ to address the implementation of the directive.¹⁶ The directive called for the plan to include, among other things, the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure and a metrics and analysis process to be used to measure the nation's ability to manage and reduce risks to critical infrastructure. DHS, in response, updated the *National Infrastructure Protection Plan* in December 2013 in collaboration with public- and private-sector owners and operators and federal and nonfederal government representatives, including SSAs, from the critical infrastructure community. According to the 2013 plan, SSAs are to work with their private-sector counterparts to understand cyber risk and they are to develop and use metrics to evaluate the effectiveness of risk management efforts.

To work with the government, the SCCs were formed as self-organized, self-governing councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SSAs and the SCCs coordinate and collaborate in a voluntary fashion on issues pertaining to their respective critical infrastructure sector.

In addition to the directive, federal laws and policies have also established roles and responsibilities for federal agencies to work with industry to enhance the cybersecurity of the nation's critical

¹⁵The plan, originally developed in 2006, defines the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.

¹⁶Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). The *National Infrastructure Protection Plan* outlines how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resilience outcomes for their information systems.

infrastructures. These include the *Cybersecurity Enhancement Act of 2014* and Executive Order 13636.¹⁷

In February 2013, Executive Order 13636 outlined an action plan for improving critical infrastructure cybersecurity. Among other things, the executive order directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes. The executive order also directed SSAs, in consultation with DHS and other interested agencies, to coordinate with the SCCs to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.¹⁸

Further, in December 2014, the *Cybersecurity Enhancement Act of 2014* established requirements that are consistent with the executive order regarding NIST's development of a cybersecurity framework. According to this law, NIST's responsibilities in supporting the ongoing development of the cybersecurity framework included, among other things, identifying an approach that is flexible, repeatable, performance-based, and cost-effective. Additionally, the *Cybersecurity Act* requires NIST to coordinate with federal and nonfederal entities (e.g., SSAs, SCCs, and ISACs) to identify a prioritized, performance-based approach to include information security measures to help entities assess risk.

In May 2017, Executive Order 13800 directed federal agency heads to use the framework to manage cybersecurity risks. The executive order also required them to provide a risk management report to DHS and the Office of Management and Budget within 90 days of the date of the executive order. The risk management report calls for agencies to document the risk mitigation and acceptance choices including, for example, describing the agency's action plan to implement the framework.¹⁹

¹⁷Executive Order No. 13636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

¹⁸Executive Order No. 13636 states that other interested agencies include the Office of Management and Budget and owners and operators of critical infrastructure, among other things.

¹⁹The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order No. 13800 (Washington, D.C.: May 11, 2017), 82 Fed. Reg. 22391 (May 16, 2017).

NIST Established a Framework for Improving Critical Infrastructure Cybersecurity

In response to Executive Order 13636, NIST published, in February 2014, the *Framework for Improving Critical Infrastructure Cybersecurity*, a voluntary framework of cybersecurity standards and procedures for industry to adopt. According to NIST, as of February 2019, the framework had been downloaded more than a half million times since its initial publication in 2014. Additionally, it has been translated into Arabic, Japanese, Portuguese, and Spanish, and has been adopted by many foreign governments. The framework is composed of three main components: the framework core, the implementation tiers, and the profiles.

The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes. Through the use of the profile, the framework is intended to help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources.

The framework core is divided into four elements: functions, categories, subcategories, and informative references. Functions consist of five elements—(1) identify, (2) protect, (3) detect, (4) respond, and (5) recover. When considered together, these functions provide a strategic view of the life cycle of an organization’s management of cybersecurity risk. Categories are the subdivisions of a function into groups of cybersecurity outcomes tied to programmatic needs and particular activities (i.e. asset management).²⁰ Subcategories further divide a category into specific outcomes of technical and/or management activities (i.e. notifications from detection systems are investigated).²¹ Lastly, informative references are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes described and

²⁰Asset management is the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. They are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.

²¹Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

support one or more informative references (i.e. NIST Special Publication (SP) 800-53A).²²

Implementation tiers characterize an organization's approach to managing cybersecurity risks over a range of four tiers. The four tiers are partial, risk informed, repeatable, and adaptive. They reflect a progression from informal, reactive responses to approaches that are flexible and risk-informed.

Profiles enable organizations to establish a road map for reducing cybersecurity risks that is well aligned with organizational and sector goals, consider legal/regulatory requirements and industry best practices, and reflect risk management priorities. Organizations can use the framework profiles to describe the current state (the cybersecurity outcomes that are currently being achieved) or the desired target state (the outcomes needed to achieve the desired cybersecurity risk management goals) of specific cybersecurity activities.

GAO Has Previously Reported on the Development, Promotion, and Adoption of the Cybersecurity Framework

In December 2015, we issued our first report on the development and promotion of the framework in response to the 2014 *Cybersecurity Act*.²³ We reported that the framework met the requirements established in federal law that it be flexible, repeatable, performance-based, and cost-effective. We also reported that SSAs and NIST had promoted and supported adoption of the cybersecurity framework in the critical infrastructure sectors. For example, we reported that DHS had established the Critical Infrastructure Cyber Community Voluntary Program to encourage adoption of the framework and had undertaken multiple efforts as part of this program. These efforts included developing guidance and tools intended to help sector entities that use the framework. However, we noted that DHS had not developed metrics to measure the success of its activities and programs. Accordingly, we concluded that DHS could not determine if its efforts were effective in

²²National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, SP 800-53A*, revision 4 (Gaithersburg, MD.: December 2014). This document provides guidelines for building effective security and privacy assessment plans and procedures for assessing the effectiveness of security controls and privacy.

²³GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, [GAO-16-152](#) (Washington, D.C.: Dec. 17, 2015).

encouraging adoption of the framework. We recommended that the department develop metrics to assess the effectiveness of its framework promotion efforts. DHS agreed with the recommendation and subsequently took actions to implement it.

We also reported in December 2015 that SSAs had promoted the framework in their sectors by, for example, presenting the framework at meetings of sector stakeholders and holding other promotional events. In addition, all of the SSAs, except for DHS and the General Services Administration (GSA), as co-SSAs for the government facilities sector, made decisions, as required by Executive Order 13636, on whether to develop tailored framework implementation guidance for their sectors.

However, we noted that DHS and GSA had not set a time frame to determine, as required by Executive Order 13636, whether sector-specific implementation guidance was needed for the government facilities sector. We concluded that, by not doing so, DHS and GSA could be hindering the adoption of the framework in this sector. As a result, we recommended that DHS and GSA set a time frame to determine whether implementation guidance was needed for the government facilities sector. Both DHS and GSA agreed with our recommendations and subsequently took actions to implement them.

More recently, in February 2018, we issued our second report on the adoption of the framework. We reported that most of the 16 critical infrastructure sectors had taken action to facilitate adoption of the framework by entities within their sectors.²⁴ We also reported that 12 of the 16 critical infrastructure sectors had taken actions to review the framework and, if necessary, develop implementation guidance or supplemental materials that addressed how entities within their respective sectors can adopt the framework.

We also reported that none of the SSAs had measured the cybersecurity framework's implementation by entities within their 16 respective sectors. We noted that the nation's plan for national critical infrastructure protection efforts stated that federal and nonfederal sector partners (including SSAs) were to measure the effectiveness of risk management goals by identifying high-level outcomes and progress made toward

²⁴GAO, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: Feb. 15, 2018).

national goals and priorities, including securing critical infrastructure against cyber threats. However, we reported that none of the 16 coordinating councils reported having qualitative or quantitative measures of framework adoption because they generally did not collect specific information from entities about critical infrastructure protection activities.

Most SSAs Have Not Developed Methods to Determine Framework Adoption

As of November 2019, most of the SSAs had not developed methods to determine their level and type of cybersecurity framework adoption, as we previously recommended.²⁵ The SSAs and SCCs identified a number of impediments to developing a comprehensive understanding of the use of the framework, including the voluntary nature of the framework. However, most SSAs have taken steps to encourage and facilitate use of the framework. Further, the 12 selected organizations we interviewed reported either fully or partially using the cybersecurity framework.

Most Sector-Specific Agencies Had Not Determined the Level and Type of Framework Adoption

Best practices identified in the *National Infrastructure Protection Plan* recommend that entities, such as SSAs and SCCs, take steps to evaluate progress toward achieving their goals—in this case, to implement or adopt the cybersecurity framework. As we previously reported, until the SSAs had a more comprehensive understanding of the use of the cybersecurity framework by entities within the critical infrastructure sectors, they would be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation. As a result, we recommended that the SSAs take steps to consult with respective sector partner(s), such as the SCCs, DHS, and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by the entities across their respective sectors.²⁶

However, as of November 2019, most of the SSAs had not developed methods to determine the level and type of framework adoption. Specifically, only two of the nine SSAs—the Department of Defense (DOD) in collaboration with the defense industrial base sector and GSA in conjunction with DHS’s Federal Protective Service—had methods to

²⁵GAO-18-211.

²⁶Five SSAs agreed with the recommendations, while four others neither agreed nor disagreed.

determine the level and type of framework adoption across their respective sectors.

DOD, in coordination with the defense industrial base sector, had developed a process to monitor the level or extent to which all contracts (not including commercial off-the-shelf contracts) were or were not adhering to the cybersecurity requirements in DOD acquisition regulations. The regulations called for organizations to implement the security requirements in NIST SP 800-171, which is mapped to the functional areas of the cybersecurity framework.²⁷ By doing so, DOD is able to determine the level at which the sector organizations are implementing the framework and the type of framework adoption through mapping to the functional areas.

Additionally, the federal departments and agencies that form the government facilities sector had submitted their risk management reports to DHS and OMB that described agencies' action plans to implement the framework, as required under Executive Order 13800. The risk management assessments are included as part of OMB's FISMA Annual Report to Congress.²⁸ As a result, the reports could be used as a resource to inform the level and type of framework adoption.

In addition, two other SSAs had begun taking steps to develop methods to determine the level and type of framework adoption in their sectors. Specifically, in October 2019, DHS, in coordination with its information technology (IT) sector partner, administered a survey to all small and mid-sized IT sector organizations to gather information on, among other things, framework use and plans to report on the results in 2020. Further, officials in the Department of Transportation's (DOT) Office of Intelligence, Security, and Emergency Response, in coordination with its co-SSA (DHS), told us that they planned to develop and distribute a survey to the transportation systems sector to determine the level and

²⁷Department of Defense, *Safeguarding Covered Defense Information and Cyber Incident Reporting Scorecard (Fiscal Year 2019, Q2)*; National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, revision 1 (Gaithersburg, MD.: December 2016); and Department of Defense, Defense Federal Acquisition Regulation Supplement Clause (48 CFR § 252.240-7012), *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

²⁸Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress* (fiscal year 2018).

type of framework adoption. DOT officials stated that the draft survey was undergoing DHS legal review and that the completion of the review and subsequent OMB review would determine when the survey is approved for distribution.

The remaining five SSAs did not have efforts underway to determine the level and type of framework adoption: Department of Agriculture, Department of Energy, Department of Health and Human Services (HHS), Environmental Protection Agency (EPA), and Department of the Treasury. These SSAs identified impediments to determining framework adoption but also noted steps taken to encourage use of the framework within their respective sector.

- Department of Agriculture's Office of Homeland Security officials stated that their sector is diverse and includes over 500 sector members that can range from small farms that are family operated to large corporations that deal with selling food wholesale. The officials noted that the diversity makes it difficult to develop a method for determining the level and type of framework adoption across the sector that would apply to all their members.

The framework, however, is adaptive to provide a flexible and risk-based implementation. Accordingly, the framework can be used with a broad array of cybersecurity risk management processes. Agriculture officials added that the SCC frequently invites DHS to semi-annual meetings to present on both the threat to cybersecurity and resources available to support the needs of the sector.

- Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response officials stated that the voluntary nature of the framework made it difficult to determine the level and type of framework adoption.

However, the department published the *Cybersecurity Capability Maturity Model* in May 2012, with the most recent update (version 1.1) published in February 2014. The model focused on the implementation and management of cybersecurity practices, and was intended to be descriptive, rather than prescriptive, guidance that could be used by organizations of various types and sizes to strengthen their cybersecurity capabilities. The model was designed for organizations to use with a self-evaluation methodology and toolkit to measure and improve their cybersecurity programs and serve as an example for how to implement the framework. In February 2020, officials stated that they were in the process of updating the model

and will update the framework implementation guidance once the model has been updated.

- HHS's Assistant Secretary for Preparedness and Response (ASPR) officials stated that, since the use of the framework by the private sector is voluntary, organizations were free to choose any cybersecurity framework(s) that they believed to be most effective for their particular environment.

However, HHS, in collaboration with NIST, DHS, and the Joint Healthcare and Public Health Cybersecurity Working Group, released a cybersecurity publication (*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*) that contained 10 best practices in December 2018 for the healthcare and public health services sector based on the framework. This publication allowed stakeholders to identify how to use the framework with existing sector resources by raising awareness and providing vetted cybersecurity practices to enable the organizations to mitigate cybersecurity threats to the sector. In addition, officials from HHS's ASPR stated that the working group discussed the challenges associated with measuring the use and impact of the NIST framework, and approved the establishment of a task group in 2020 to further investigate the issue. ASPR officials added that some of the ideas discussed included the use of surveys and identification of a set of voluntary reporting indicators.

- EPA officials told us that the agency will coordinate with its SCC to identify appropriate means to collect and report information, such as a survey, to determine the level and type of framework adoption. They explained that, in the past, the water sector had expressed concerns with sharing sensitive cybersecurity information and in developing metrics to evaluate cybersecurity practices.

However, EPA officials stated that they have conducted training, webcasts, and outreach related to cybersecurity, including using the framework and tailoring its efforts to sector needs. According to EPA officials, the agency's goal in doing so was to ensure that sector organizations understood the importance of the framework.

- Department of the Treasury officials noted the size of the financial services sector as an impediment to determine framework adoption. Specifically, officials stated that, because of the large number of members, it is difficult to survey all 800,000 organizations to determine framework adoption.

However, officials stated that the department, in coordination with the Financial and Banking Information Infrastructure Committee, and in consultation with NIST, developed the Cybersecurity Lexicon in March 2018.²⁹ The lexicon addressed, among other things, common terminology for cyber terms used in the framework. Additionally, the financial services sector, in consultation with NIST, created the *Financial Services Sector Cybersecurity Profile* (profile) in October 2018, which mapped the framework core to existing regulations and guidance, such as the *Commodity Futures Trading Commission System Safeguards Testing Requirements*.³⁰ Officials stated that these efforts will facilitate the use of the framework.

While the five SSAs have ongoing initiatives, implementing our recommendations to gain a more comprehensive understanding of the framework's use by critical infrastructure sectors is essential to the success of protection efforts.³¹

Most SSAs Have Taken Steps to Facilitate Use of the Framework

Executive Order 13636 directs SSAs, in consultation with DHS and other agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and facilitate framework use. Most of the SSAs developed guidance to encourage and facilitate use of the framework. Specifically, SSAs for 13 of the 16 sectors had developed implementation guidance that included mapping the existing sector cybersecurity tools, standards, and approaches to the framework. For example, the implementation guidance for the healthcare and public health sector provides instruction on how to align a host of existing voluntary or required standards (such as those promulgated pursuant to the *Health*

²⁹The Financial and Banking Information Infrastructure Committee is a standing committee of the President's Critical Infrastructure Protection Board and is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system.

³⁰The *Commodity Futures Trading Commission System Safeguards Testing Requirements* is a set of testing requirements for all designated contract markets, swap execution facilities, and swap data repositories. The testing requirements specify and define the types of cybersecurity testing essential to fulfilling system safeguards testing.

³¹[GAO-18-211](#).

Insurance Portability and Accountability Act of 1996), guidelines, and practices to the framework core functions.³²

Table 1 describes the 13 sectors and the associated cybersecurity framework implementation guidance.

Table 1: Critical Infrastructure Sectors that Developed Cybersecurity Implementation Guidance to Facilitate Use of the Framework

Critical infrastructure sector	Description of the implementation guidance
Defense Industrial Base	The October 2019 Defense Industrial Base sector’s implementation guidance mapped the Defense Federal Acquisition Regulation Supplement Clause on contractor cybersecurity and NIST SP 800-171 to the framework.
Energy	Developed by the Department of Energy in January 2015, the sector’s implementation guidance included a mapping of the Department of Energy’s Cybersecurity Capability Maturity Model to the practices of the framework core and tiers.
Water and Wastewater Systems	Developed by the American Water Works Association in April 2014 and revised in 2019, the Water and Wastewater Systems sector’s implementation guidance included mapping the framework core to the association’s Cybersecurity Guidance and Assessment Tool and cyber provisions in <i>America’s Water Infrastructure Act of 2018</i> .
Healthcare and Public Health	The May 2016 Healthcare and Public Health sector’s implementation guidance mapped the security rule standards and implementation specifications of the <i>Health Insurance Portability and Accountability Act of 1996</i> to the framework.
Chemical	Developed in coordination with DHS and the American Chemistry Council in 2015, the Chemical sector’s implementation guidance mapped five existing cybersecurity tools, such as the Chemical Facilities Anti-Terrorism Standards, to the functions and categories of the framework.
Commercial Facilities	Developed in coordination with DHS in 2015, the Commercial Facilities sector’s implementation guidance included mapping the framework core to six existing cybersecurity tools and standards, such as DHS’s Cyber Security Evaluation Tool.
Communications	Developed in coordination with the Federal Communications Commission in March 2015, the Communications sector’s implementation guidance included mapping the framework across the five Communications sector industry segments: broadcast, cable, satellite, wireless, and wireline.

³²The *Health Insurance Portability and Accountability Act of 1996* required the Secretary of the Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what is commonly known as the *Health Insurance Portability and Accountability Act* (HIPAA) Security Rule. The Security Rule established national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule required appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Critical infrastructure sector	Description of the implementation guidance
Critical Manufacturing	Developed in coordination with DHS in 2015, the Critical Manufacturing sector's implementation guidance included mapping the framework core to six existing cybersecurity tools and standards, such as the Cyber Security Evaluation Tool and International Standards Organization guidance.
Dams	Developed in coordination with DHS in 2015, the Dams sector's implementation guidance included mapping the framework core to six existing cybersecurity tools and standards, such as the Dams Sector Analyst Tool.
Emergency Services	Developed in coordination with DHS in 2015, the Emergency Services sector's implementation guidance included mapping the framework core to seven existing cybersecurity tools and standards, such as the Emergency Services Cyber Risk assessment.
Nuclear Reactors, Materials, and Waste (Nuclear)	Developed in coordination with DHS in 2015, the Nuclear sector's implementation guidance included mapping the Nuclear sector's reactor cybersecurity program practices to the functions and categories of the framework.
Transportation Systems	Developed by the Transportation Systems sector stakeholders and government partners in June 2015, the Transportation System sector's implementation guide aligned sector goals to the functions and categories of the framework.
Financial Services	There is no formal sector-specific guidance; however, the Financial Services sector mapped the <i>Financial Services Sector Cybersecurity Profile</i> to the framework.

Source: GAO summary based on agency data | GAO-20-299

Notes: DOD acquisition officials and contractors doing business with DOD are required to follow the Defense Federal Acquisition Regulation Supplement clause, if applicable.

The Cybersecurity Capability Maturity Model helps organizations evaluate and potentially improve their cybersecurity practices. Appendix A of the Energy Sector Cybersecurity Framework Implementation Guidance provides a mapping of the model to the framework.

The Financial Services Sector Cybersecurity Profile was created for financial institutions of all sizes to use for cyber risk management assessment and a mechanism to comply with various regulatory frameworks and the NIST Cybersecurity Framework.

The remaining three sectors (government facilities, food and agriculture, and IT) had not developed implementation guidance. In this regard, DHS's Federal Protective Service officials stated that, in 2015, the co-SSAs of the government facilities sector (DHS and GSA) decided that implementation guidance was not needed based on a consensus within the government facilities sector. DHS's Federal Protective Service officials added that this decision was reevaluated in 2017 and they determined that the guide was still not needed.

Department of Agriculture officials from the Office of Homeland Security stated that the co-SSAs (Agriculture and HHS) and the SCC for the sector collectively decided that a single implementation guidance document was

not sufficient for addressing the needs of the diverse membership of the food and agriculture sector and that the creation of such a document was a low priority for the sector. These officials added that, due to the complexity of operations and large number of entities within the sector, the coordinating councils determined that it was more appropriate to refer sector members to DHS's Critical Infrastructure Cyber Community Voluntary Program.³³

DHS officials representing the SSA for the IT sector stated that the SSA and SCC jointly determined that creating formal implementation guidance within the sector was not necessary. They added that the IT sector continued to play an active role by participating in framework development and promotion across the sectors, to include the development of a small and midsize business cybersecurity survey that was issued in 2019.

In addition to the above efforts, NIST officials stated that they took steps to encourage framework adoption through three main mechanisms for federal and nonfederal entities and organizations that were interested in the framework: (1) conferences and speaking engagements, (2) requests for information to solicit ways in which organizations are using the framework to improve cybersecurity risk management and how best practices are being shared, and (3) industry and agency events, such as webcasts.

Selected Organizations Described Varying Levels of Use of the Framework

The 12 selected organizations reported either fully or partially using the cybersecurity framework.³⁴ Specifically, six organizations reported fully using the framework, whereas six others reported partially using the framework. For example, one organization that reported fully using the framework stated that the framework core, profiles, and tiers were implemented across all the components or business units in the organization. In contrast, one organization that reported partially using the framework stated that it used the framework profiles, but did not fully use the framework core and tiers. Two other of the organizations that reported partially using the framework stated that they considered themselves to be using the framework since they use International Organization for

³³DHS's Critical Infrastructure Cyber Community Voluntary Program encourages the adoption of the framework.

³⁴For the purposes of this report, we are defining "fully using" the framework as using all elements and "partially using" as using some, but not all, elements of the framework.

Standardization (ISO) 27001, an international standard that has elements that overlap with those in the framework.³⁵

Selected Organizations Reported Improvements but SSAs Have Not Collected and Reported Sector-Wide Improvements Resulting from Framework Use

The 12 selected organizations using the framework reported varying levels of improvements. Such improvements included identifying risks and implementing common standards and guidelines. However, the SSAs have not collected and reported sector-wide improvements as a result of framework use. The SSAs, SCCs, ISACs, and the selected organizations identified impediments to collecting and reporting such improvements, including developing precise measurements of improvement, the voluntary nature of the framework, and lack of a centralized information sharing mechanism. NIST and DHS have identified initiatives to help address these impediments.

Selected Organizations Described Varying Levels of Improvements from Using the Framework

The 12 selected organizations reported varying levels of improvements as a result of using the framework. Specifically, four of the 12 reported great improvement, six reported some improvement, and two reported little improvement.³⁶ Examples of each category are described below:

- Great improvement: One organization stated that the framework allowed it to determine the current state (the cybersecurity outcomes that are currently being achieved) and the desired target state (the outcomes needed to achieve the desired cybersecurity risk management goals). The organization stated that identifying the

³⁵The ISO 27001 standard provides requirements for an information security management system.

³⁶In response to a structured question on the extent organizations experienced improvements from using the NIST Cybersecurity Framework, the organizations selected answers from the following options (a) great improvement, which refers to a significant impact on a selected organization (e.g., allowing for increased funding in cybersecurity or reduction of cybersecurity risk that an organization would not have received if the framework did not exist); (b) some improvement, which refers to a moderate impact on a selected organization (e.g., organization received benefits from using the framework, but the outcomes could have been achieved without use of the framework); (c) little improvement, which refers to a minimal impact on a selected organization; (d) none, which refers to a selected organization not having experienced any improvements; and (e) no basis to judge, which refers to a selected organization not having any direct experience with determining improvements as a result of using the framework.

current and target states enabled the organization to identify risks and implement common policies, standards, and guidelines across their organization. Officials of the organization also stated that the common language provided by the framework made it easier to communicate within the organization when discussing budgets for cybersecurity that resulted in budget increases.

- Some improvement: One organization explained that the framework is accepted across organizations and that modeling its capabilities against the framework provided assurance that it covered the critical aspects of security. However, the organization noted that, if the framework did not exist, it would have used another framework to protect its critical infrastructure and facilitate decision making.
- Little improvement: One organization noted that it already had a very robust risk management process through the use of international standards before using the framework. As a result, the organization stated that use of the framework resulted in little improvements. Another organization that reported little improvements stated that use of the framework helped the organization, but there were no specific improvements that it could identify in protecting its critical infrastructure as a result of using the framework.

Initiatives Available to Help Address Impediments to Collecting and Reporting on Sector-Wide Improvements

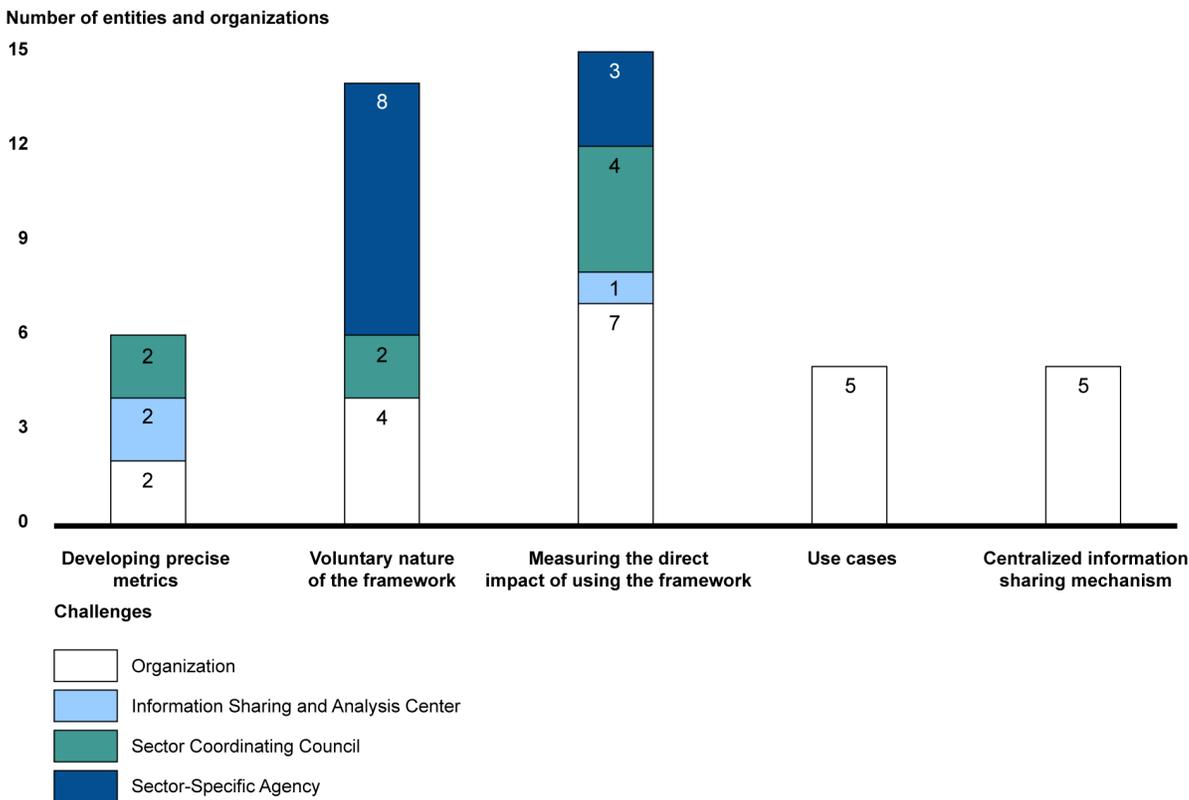
NIST Special Publication 800-55 guidance on performance measurement states that agency heads are responsible for actively demonstrating support for developing information security measures and facilitating performance improvements in their information security programs, which is to include a periodic analysis of data to determine lessons learned.³⁷ Additionally, the *National Infrastructure Protection Plan* directed SSAs and their federal and nonfederal sector partners (including SCCs) to measure the effectiveness of risk management goals by identifying high-level outcomes to facilitate the evaluation of progress toward national goals and priorities, including securing critical infrastructure from cybersecurity threats.

The SSAs are not collecting and reporting on improvements in the protection of critical infrastructure as a result of using the framework across the sectors. The SSAs, SCCs, ISACs, and organizations reported a number of impediments to identifying sector-wide improvements, including developing precise measurements of improvement, the

³⁷National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, SP 800-55, revision 1 (Gaithersburg, MD.: July 2008).

voluntary nature of the framework, difficulty in measuring the direct impact of using the framework, lack of use cases, and lack of a centralized information sharing mechanism. Figure 2 depicts the number of entities and organizations that identified these five impediments, and is followed by a discussion of each challenge.

Figure 2: Number of Entities and Organizations that Identified the Five Impediments to Identifying Sector-wide Improvement as a Result of Using the Framework



Source: GAO summary based on entity and selected organization data. | GAO-20-299

- Two SCCs, two ISACs, and two organizations identified the difficulty of having precise measurements of improvements as a result of using the framework. SCC officials from the communications and healthcare and public health sectors stated that authoritative and precise measurements of improvements are difficult to determine in a consistent and non-subjective manner. For example, the SCC officials for the healthcare and public health sector stated that they were not aware of a direct or precise form of sector-wide measurements to define success in mitigating cybersecurity risk using the framework

within the sector. These officials added that future efforts could include methodologies to track sector-wide improvements based on the framework structure or other cybersecurity guidance.

However, officials from NIST's Information Technology Laboratory stated that they were in the early stages of initiating an information security measurement program to facilitate identifying improvements sector-wide. Officials stated that the program aims to provide foundation tools and guidance to support the development of information security measures that are aligned with an individual organization's objectives. The officials stated that they had not established a time frame for the completion of the measurement program. They added that, once the program is developed, the SSAs are expected to be able to customize the program and work with their respective sector organizations to determine sector-wide improvements based on their unique objectives.

- Eight SSAs, two SCCs, and four organizations stated that the voluntary nature of using the framework made it difficult to identify sector-wide improvements. Officials stated that private sector framework adoption was voluntary and, therefore, there were no specific reporting requirements to provide information on improvements. For example, DOT officials from the Office of Intelligence, Security, and Emergency Response stated that, while the department and its co-SSA (DHS) intended to develop a survey to determine sector-wide improvements, consolidating voluntarily shared information will not reflect the depth and breadth of sector stakeholders, as organizations that share information will not collectively represent a sector.

In April 2019, NIST issued the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, version 1.1, which included a self-assessment tool that provided a mechanism for individual organizations to self-assess how effectively they manage cybersecurity risks in the context of broader enterprise risk management activities and identify improvement opportunities. In addition to the road map, NIST's framework included a section that encouraged organizations to incorporate measurements of their risks, which can be used to identify sector-wide improvements related to using the framework.

In addition, as previously mentioned, DHS, in partnership with its IT sector partners, administered a survey to the small and mid-sized IT sector organizations to gather information on, among other things,

framework adoption, challenges, and related improvements. While DHS did not plan to report on the results until 2020, the survey was intended to help the department in identifying improvements across the small and mid-sized IT sector organizations. The survey was administered to the small and mid-sized organizations within the IT sector. DHS officials stated that any small or mid-sized business across all critical infrastructure sectors could complete the survey and that the department had promoted the survey to all sectors.

Moreover, among all 16 sectors, only DOT and its co-SSA (DHS) had considered the applicability of a similar approach for their sector organizations. Specifically, DOT, in conjunction with DHS, plans to distribute a survey intended to cover framework adoption, challenges, and related improvements across the sector. DOT officials stated that the survey completion is contingent upon DHS's Transportation Security Administration's coordination of the review and approval process to meet *Paperwork Reduction Act* compliance requirements.³⁸

- Three SSAs, four SCCs, one ISAC, and seven organizations stated that identifying sector-wide improvements as a result of using the framework was difficult due to organizations struggling with determining the direct impact from framework use. For example, the Department of Energy officials from the Office of Cybersecurity, Energy Security, and Emergency Response stated that the sector cannot relate improvements to any one framework or model because the sector organizations are engaged in numerous concurrent public and private cybersecurity initiatives, each of which could impact cybersecurity to varying degrees. In addition, EPA officials from the Office of Groundwater and Drinking Water stated that most organizations will not be able to link improvements directly to the framework because EPA does not exclusively incorporate the framework into the agency's sector guidance. The officials added that existing industry standards and best practices are also recognized in the development of EPA cybersecurity guidance. Therefore, although an organization might experience improvements from using elements

³⁸The *Paperwork Reduction Act* was originally enacted into law in 1980 (Pub. L. No. 96-511, 94 Stat. 2812 (Dec. 11, 1980)). It was reauthorized in 1986 (Pub. L. No. 99-591, 100 Stat. 3341-335 (Oct. 30, 1986)) and was reauthorized a second time in 1995 (Pub. L. No. 104-13, 109 Stat. 163 (May 22, 1995)); codified at 44 U.S.C. §§ 3501 – 3521.

of the framework, it might not be readily apparent that those improvements came directly from the framework.

To provide the sector organizations with access to various framework resources, NIST updated its website to include sector-specific implementation guidance and case studies, as well as insights from organizations using the framework.

- Five organizations identified the lack of use cases as an impediment to determining improvements. For example, one organization stated that small and medium organizations struggled with identifying improvements from using the framework because of the lack of use cases (examples for how to determine or measure improvements as a result of using the framework). To address the challenge, the organization stated that it would be helpful if NIST, in collaboration with federal and nonfederal entities, would share and provide use cases or direction on common scenarios small and medium organizations faced and how these could be addressed through the framework.

NIST officials stated that they were in the early stages of developing a *cybersecurity framework starter profile* for small organizations. NIST officials stated that they did not have a time frame for completing the profile. However, they added that the profile will aim to identify common solutions to a specific challenge, such as threat surface or cybersecurity challenges in cloud computing, using a customized adaptation of the framework.

In addition, DHS created a small and midsize business road map for all critical infrastructure sectors in 2018.³⁹ The road map provided a guide for small and mid-sized businesses to use in enhancing their cybersecurity posture. The road map also included DHS's cybersecurity information sharing and collaboration program and secure information sharing portal. The purpose of the information sharing and collaboration program was to enable actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors. In addition, the secure information sharing portal served as a forum to share cybersecurity strategies and insights with the critical infrastructure sectors.

³⁹Department of Homeland Security, *Cybersecurity Resources Road Map: A Guide for Critical Infrastructure Small and Midsize Businesses* (Washington, D.C.: July 27, 2018).

-
- Five organizations identified the lack of a centralized information sharing mechanism as an impediment. For example, one organization stated that there is a challenge in sharing information among all critical infrastructure sectors in a more open and non-judgmental way. To address this challenge, the organization stated that it would be helpful to establish a centralized information sharing mechanism to share and exchange information in an anonymous manner. Another organization added that the challenge with determining improvements is that there is no centralized information sharing mechanism to obtain information. The organization added that it would be helpful to see how organizations compare with one another in terms of goals through this type of mechanism.

DHS, however, identified its homeland security information network as a tool that was intended to be the primary system used by entities to collaborate to protect critical infrastructure. Officials in DHS's Stakeholder Engagement and Cyber Infrastructure Resilience division stated that the information in its homeland security information network could be used by all sectors to report on best practices, including sector-wide improvements and lessons learned from using the framework.

Although NIST and DHS have identified initiatives to help address the impediments, the SSAs have not reported on sector-wide improvements. Until they do so, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructures from threats will be largely unknown.

Conclusions

Most of the SSAs have not determined the level and type of framework adoption, as we previously recommended. Most of the sectors, however, had efforts underway to encourage and facilitate use of the framework. Even with this progress, implementation of our recommendations is essential to the success of protection efforts.

While selected organizations reported varying levels of improvements, the SSAs have not collected and reported sector-wide improvements as a result of framework use. The SSAs and organizations identified impediments to collecting and reporting sector-wide improvements, including the lack of precise measurements of improvement, voluntary nature of the framework, and lack of a centralized information sharing mechanism. However, NIST and DHS have initiatives to help address these impediments. These included an information security measurement program, cybersecurity framework starter profile, information sharing

programs, self-assessment tools, and surveys to support SSAs in measuring and quantifying improvements in the protection of critical infrastructure as a result of using the framework. However, NIST has yet to establish time frames for completing the information security measurement program and starter profile. Moreover, the SSAs have yet to report on sector-wide improvements using the initiatives. Until they do so, the critical infrastructure sectors may not fully understand the value of the framework to better protect their critical infrastructures from cyber threats.

Recommendations

We are making the following 10 recommendations to NIST and the nine sector-specific agencies.

The Director of NIST should establish time frames for completing NIST's initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats. (Recommendation 1)

The Secretary of Agriculture, in coordination with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 2)

The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 3)

The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 4)

The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements

from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 5)

The Administrator of the General Services Administration, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 6)

The Secretary of Health and Human Services, in coordination with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 7)

The Secretary of Homeland Security should take steps to consult with respective sector partner(s), such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives. (Recommendation 8)

The Secretary of Transportation, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s) such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 9)

The Secretary of the Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 10)

Agency Comments and Our Evaluation

We received comments on a draft of this report from the ten agencies to which we made recommendations—the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury; and the Environmental Protection Agency and the General Services Administration. Among these agencies, eight agreed with the recommendations, one neither

agreed nor disagreed with the recommendation, and one partially agreed with the recommendation.

In written comments, the Department of Agriculture generally concurred with the recommendation in our report. The department's comments are reprinted in appendix II.

In written comments, the Department of Commerce concurred with the recommendation in our report. The department stated that the National Institute of Standards and Technology expects to document its cybersecurity measurement program scope, objectives, and approach by about June 2020 and publish two cybersecurity starter profiles by about September 2020. The department's comments are reprinted in appendix III.

In written comments, the Department of Defense concurred with the recommendation in our report and described ongoing steps to evaluate defense organizations' cybersecurity maturity levels. The department's comments are reprinted in appendix IV.

In written comments, the Department of Energy partially concurred with the recommendation in our report. The department stated that it will coordinate with the energy sector to develop an understanding of sector-wide improvements from use of the framework.

The department, however, stated that implementing our recommendation as written prescribes the SCC as a forum for coordination regarding the framework. Our recommendation is not intended to be prescriptive, but rather, to provide suggestions for consideration. Thus, we have revised the wording of the recommendation to emphasize coordination with other entities, as appropriate.

The department also stated that the recommendation implies that improvements from the use of the framework could accurately be attributed to a single initiative, which may be misleading. We do not agree. Our report identifies the challenge of determining the direct impact from framework use and notes that NIST's website provides the sector organizations with access to various framework resources, to include sector-specific implementation guidance and case studies, as well as insights from organizations using the framework. Hence, organizations can report on improvements from use of the framework using multiple initiatives.

Further, the department stated that suggesting government collection and reporting of information regarding adoption or improvements erodes the voluntary character of the framework. We do not agree with this statement. Our report recognizes the voluntary character of the framework but also notes that, without collecting and reporting such information, critical infrastructure sectors may not fully understand the benefits and value of the framework to better protect their critical infrastructures from cyber threats. The department's comments are reprinted in appendix V.

In written comments, the Department of Health and Human Services concurred with the recommendation in our report and stated that it would work with the appropriate entities to refine and communicate best practices to the sector. The department's comments are reprinted in appendix VI.

In written comments, the Department of Homeland Security concurred with the recommendation in our report. The department stated that, once it receives the results of the survey on framework adoption that it sent to small- and mid-sized IT sector partners, it will determine the feasibility of issuing similar surveys to other sectors. The department's comments are reprinted in appendix VII.

In written comments, the Department of the Treasury neither agreed nor disagreed with the recommendation in our report. The department stated that it will assess using the identified initiatives and their viability for collecting and reporting sector-wide improvements from use of the framework with input from the SCC and financial regulators. The department added, however, that it does not have the authority to compel financial institutions to respond to inquiries regarding the sector's use of the framework or resulting improvements. We acknowledge the lack of authority but believe that implementing the recommendation to gain a more comprehensive understanding of the framework's use by the critical infrastructure sector is essential to the success of protection efforts. The department's comments are reprinted in appendix VIII.

In written comments, the Environmental Protection Agency concurred with the recommendation in our report. The agency stated that it will coordinate with its SCC to investigate options to collect and report sector-wide improvements from use of the cybersecurity framework that are consistent with statutory requirements and the sector's willingness to participate. The agency's comments are reprinted in appendix IX.

In written comments, the General Services Administration concurred with the recommendation in our report and stated that it is working with the Department of Homeland Security to develop a plan to address the recommendation. The agency's comments are reprinted in appendix X.

In comments sent via e-mail, the Department of Transportation's Director of Audit Relations and Program Improvement stated that the department concurred with the recommendation in our report.

In addition to the aforementioned comments, we received technical comments from officials of the Departments of Agriculture, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury. We also received technical comments on the report from the Environmental Protection Agency and General Services Administration. We incorporated the technical comments in the report, where appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury; the Administrators of the Environmental Protection Agency and General Services Administration; and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6240 or at dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix XI.



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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the extent to which (1) agencies with lead roles in critical infrastructure protection efforts, referred to as sector-specific agencies (SSAs), have determined the level and type of *National Institute of Standards and Technology Cybersecurity Framework* (framework)¹ adoption and (2) implementation of the framework has led to improvements to the protection of critical infrastructure from cyber threats.²

To address the first objective, we analyzed documentation and evidence, such as implementation guidance and survey instruments that discussed actions federal and nonfederal entities have taken since our report in 2018 to develop methods to determine the level and type of adoption across their sectors, as we previously recommended.³ These entities included nine SSAs, 13 out of the 16 Sector Coordinating Councils (SCC)⁴ representing all 16 critical infrastructure sectors established in federal policy,⁵ the National Institute of Standards and Technology (NIST), and

¹National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity version 1.1*. (Gaithersburg, MD.: April 2018). The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

²We satisfied the requirement to assess the extent to which the framework has proved successful in protecting critical infrastructure from cyber threats by determining the extent to which implementation of the framework has led to improvements.

³GAO, *Critical Infrastructure Protection: Additional Actions Are Essential For Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: February 15, 2018).

⁴Sector Coordinating Councils are made up of nonfederal members and are to serve as the voice of each sector and principal entryway for the government to collaborate with each sector. We included Sector Coordinating Council representatives from the following 13 sectors: chemical; commercial facilities; communications; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. We did not include Sector Coordinating Council representatives from the following three sectors due to non-responsiveness: critical manufacturing, dams, and information technology sectors.

⁵Presidential Policy Directive 21 identifies 16 critical infrastructure sectors for which Sector Specific Agencies are responsible: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

Information Sharing and Analysis Centers (ISAC).⁶ We also analyzed documentation from the SSAs and SCCs, such as the Department of Energy's *Cybersecurity Capability Maturity Model* and the Department of the Treasury's *Financial Services Sector Cybersecurity Profile*. We compared these to best practices, such as the *National Infrastructure Protection Plan*⁷ and the *Standards for Internal Control in the Federal Government* to determine efforts to facilitate framework adoption across the sectors.⁸ We supplemented our review by interviewing officials from these entities to determine any actions taken to determine framework adoption.

In addition, we selected six critical infrastructure sectors identified in the 2018 *National Cyber Strategy of the United States of America* as having critical infrastructure with the greatest risk of being compromised. The six sectors were (1) communications, (2) financial services, (3) energy, (4) healthcare and public health, (5) information technology, and (6) transportation systems. We asked SCCs, trade associations (e.g., the American Petroleum Institute), and ISACs to provide a list of organizations that were users of the framework. We divided up the list of identified organizations by sector, and we randomly selected one large and one small or medium organization from each sector, resulting in a final list of 12 organizations.⁹ We then conducted semi-structured interviews with officials from the selected organizations to understand the extent to which these organizations were using the framework.

To address the second objective, we collected and reviewed documentation from NIST and the federal and nonfederal entities, such

⁶Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards by communicating critical information and maintaining sector-wide situational awareness.

⁷Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). The *National Infrastructure Protection Plan* outlines how government and private sector participants in the critical infrastructure community can work together to manage risks and achieve security and resilience outcomes for their information systems.

⁸GAO, *Standards for Internal Control in the Federal*, [GAO-14-704G](#) (Washington D.C.: September 2014). This publication, also known as the Green Book, provides guidelines for designing, implementing, and operating an effective internal control system.

⁹We randomly selected one small or medium organization and one large organization from each sector.

as NIST's framework and its April 2019 *Roadmap for Improving Critical Infrastructure Cybersecurity*,¹⁰ the Department of Homeland Security's *Information Technology Sector Small and Midsize Business Cybersecurity Survey* and 2018 *Cybersecurity Resources Road Map*,¹¹ and other SSA efforts to determine ongoing efforts to enable the identification and measurement of improvements as a result of using the framework. We compared these efforts to the *2014 Cybersecurity Act* and best practices, such as NIST Special Publication 800-55 on performance-based measures to determine the measures the SSAs and SCCs had taken to determine improvements from using the framework.¹²

In addition, we interviewed officials from the selected organizations to understand the extent to which they realized improvements as a result of framework adoption¹³ and the support the organizations received from federal and nonfederal entities.¹⁴ We also interviewed officials from other

¹⁰National Institute of Standards and Technology, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, MD.: April 2019). This road map describes next steps with the NIST Cybersecurity Framework and identifies key areas of development, alignment, and collaboration.

¹¹Department of Homeland Security, *Cybersecurity Resources Road Map: A Guide for Critical Infrastructure Small and Midsize Businesses* (Washington, DC: July 2018). This road map was intended to help critical infrastructure for small and midsize businesses identify useful cybersecurity resources to meet their needs.

¹²National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, SP 800-55, revision 1 (Gaithersburg, MD.: July 2008). This guide is to assist in the development, selection, and implementation of measurements for use at a system or program level. Such measures are to be used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of performance-related data.

¹³In response to a structured question on the extent organizations experienced improvements from using the NIST Cybersecurity Framework, the organizations selected answers from the following options: (a) great improvement, which refers to a significant impact on a selected organization; (b) some improvement, which refers to a moderate impact on a selected organization; (c) little improvement, which refers to a minimal impact on a selected organization; (d) none, which refers to a selected organization not having experienced any improvements; and (e) no basis to judge, which refers to a selected organization not having any direct experience with determining improvements as a result of using the framework.

¹⁴In response to a structured question on the support organizations received from NIST, ISACs, DHS, SSAs, and SCCs, the organizations selected answers from the following options: (a) very helpful, which refers to support that had a significant impact; (b) moderately helpful, which refers to support that had a small impact; (c) somewhat helpful, which refers to support that had a minimal impact; (d) not at all helpful, which refers to support as having no impact on the organization; and (e) no basis to judge, which refers to an organization having limited or no interactions with the entity.

federal and nonfederal entities, to include NIST, nine SSAs, 13 of the 16 SCCs, and six ISACs on efforts to measure improvements from use of the framework, and any related challenges.¹⁵

We conducted this performance audit from January 2019 to February 2020 in accordance with generally accepted government auditing standards.¹⁶ 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.

¹⁵In response to a structured question on the challenges organizations experienced with determining improvements from using the framework, the organizations selected from the following options: (a) no requirement for reporting, (b) organizations are not willing to share information with one another, (c) measurements would be too technical and scientific, (d) difficulty in measuring the direct impact of using the *NIST Cybersecurity Framework*, (e) lack of guidance on improvement measures, (f) lack of cybersecurity expertise, (g) lack of funding, (h) lack of a centralized information sharing mechanism among all critical infrastructure sectors, (i) lack of use cases to assist organizations in measuring improvements, (j) lack of leadership in in developing improvement measures as a result of using the framework, (k) other, and (l) organization has not experienced any challenges.

¹⁶We submitted a draft of this report to the Senate Committee on Commerce, Science, and Transportation and the House Committee on Science, Space, and Technology to satisfy our statutory reporting mandate on December 18, 2019.

Appendix II: Comments from the Department of Agriculture



United States
Department of
Agriculture

Office of Homeland
Security

1400 Independence
Avenue SW

Washington, DC
20250

TO: Neela Lakhmani
Assistant Director
Information Technology and Cybersecurity
Government Accountability Office

FROM: Jessica Fantinato
Acting Director
Office of Homeland Security

**JESSICA
FANTINATO**
Digitally signed by
JESSICA FANTINATO
Date: 2020.01.31
11:47:37 -0500

SUBJECT: Response to Report GAO 103316: Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements, (GAO-20-299).

Thank you for the opportunity to review the subject report and provide the U.S. Government Accountability Office (GAO) with the steps the U.S. Department of Agriculture (USDA) is taking to address the listed recommendation. The USDA generally concurs with the recommendation and requests that the contextual edits below be incorporated to add clarity.

To summarize, USDA requests the following edits:

1. Page 21, 2nd paragraph: "Department of Agriculture Officials from the Office of Homeland Security stated that the co-SSA's (Agriculture and HHS) and the SCC for the sector collectively decided that a single implementation guidance document was not sufficient for addressing the needs of the diverse membership of the Food and Agriculture sector and that the creation of such a document was a low priority for the sector. These officials added that they have not been able to find an example of guidance that would cover all uses of IT within the sector."

Suggest deleting the final sentence and adding the additional detail provided here: "Due to the complexity of the operations within the Food and Agriculture Sector, and the number of entities that comprise the Food and Agriculture Sector, the Food and Agriculture Sector GCC and SCC Leadership determined that it was more appropriate to refer members to DHS's Critical Infrastructure Cyber Community C³ Voluntary Program (<https://www.dhs.gov/ccubedvp>). Each of the 6 million entities within the Food and Agriculture Sector have a multitude of operations which may need to be assessed for cybersecurity vulnerabilities."

2. Page 30, paragraph 2 – should include the Secretary of HHS and be reworded to read "The Secretaries of Agriculture and HHS, as co-SSAs, should take steps, in coordination with their SCC...."

Again, thank you for the opportunity to review and comment on this report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

AN EQUAL OPPORTUNITY EMPLOYER

Appendix III: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

January 29, 2020

Mr. Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. D'Souza:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements* (GAO-20-299).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. We concur with the recommendation, and the National Institute of Standards and Technology expects to complete implementation by September 2020. We will provide additional details when we submit our action plan.

If you have any questions, please contact MaryAnn Mausser, Department of Commerce Audit Liaison, at (202) 482-8120.

Sincerely,


Wilbur Ross

Enclosure

Department of Commerce's Comments on

GAO Draft Report titled *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*

(GAO-20-299)

The Department of Commerce has reviewed the draft report, and we offer the following comments for GAO's consideration. Page numbers refer to page numbers in the report unless otherwise stated.

Comments on Recommendations

The Government Accountability Office (GAO) made one recommendation to the Department of Commerce in the report.

- **Recommendation 1:** The Director of NIST should establish time frames for completing its initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats.

Commerce Response: The Department of Commerce concurs with this recommendation.

Information Security Measurement Program:

GAO recommends NIST complete its information security measurement program to help organizations improve the protection of critical infrastructure from cyber threats. NIST's cybersecurity measurement program seeks to perform research that can lead to tools and approaches to help organizations align technical measures to determine effect on high-level organizational objectives. Our process builds on existing research and approaches, and will involve consultation with the research, business, and government sectors, including those already offering measures.

Examples of supportive NIST research activities, datasets, and tools already initiated include:

- Cybersecurity Risk Analytics (<https://csrc.nist.gov/Projects/Cybersecurity-Risk-Analytics>) – research and prototype methods and tools to enable predictive risk analytics and identify cyber risk trends.
- National Vulnerability Database (NVD; <https://nvd.nist.gov>) – the repository of standards-based vulnerability management data that enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
- Baldrige Cybersecurity Excellence Builder (<https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative>) – a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance.

Given the pace of change in the technology and cybersecurity landscape, cybersecurity measurement is, and will likely always be, an ongoing program. NIST will continue its focused work on cybersecurity measurement to align technical measures to determine effect on high-level organizational objectives, as well as to support decision making by senior executives and oversight by boards of directors. This program will build on existing research and approaches, and will involve consultation with the research, business, and government sectors, including those already offering measures.

To further establish its Cybersecurity Measurement program, NIST will document NIST Cybersecurity Measurement program scope, objectives, and approach, including inventory of existing measurement resources. Expected completion date June 2020.

The above document will be updated as appropriate based on ongoing NIST research aimed at understanding the continuously evolving challenges, insights, and gaps in cybersecurity measurement; and NIST will share these results with stakeholders through our documents, other work products, and outreach events.

Cybersecurity Framework Starter Profile:

GAO recommends NIST complete Cybersecurity Framework starter profiles to help small businesses and other organizations improve the protection of critical infrastructure from cyber threats. In 2019, NIST launched the freely and publicly available NIST Small Business Cybersecurity Corner to connect small businesses to consistent, clear, concise, and actionable resources to help them improve their cybersecurity. These resources are produced by federal agencies, including NIST and several primary contributors, as well non-profit organizations. NIST also promotes the importance and impact of cybersecurity to small businesses and others through social media, cybersecurity-focused blogs, and webinars, as well as participating in and speaking at many government and industry events focused on small business cybersecurity. NIST also aligns many of its cybersecurity standards, guidelines, and other resources to the Cybersecurity Framework to help organizations of all sizes improve their cybersecurity.

To further amplify small business awareness of cybersecurity, and of the Cybersecurity Framework, NIST will develop and publish two (2) Cybersecurity Framework starter profiles tailored toward risk management of business processes important to small business owners. Expected completion date September 2020.

NIST will also continue to develop an inventory and catalog of cybersecurity resources of relevance and value to small businesses through the NIST Small Business Cybersecurity Corner; and further promote awareness of the importance and impact of cybersecurity and resources that help address cybersecurity through public events and expanded use of social media in order to help mitigate the evolving threats.

Appendix IV: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

FEB 11 2020

Mr. Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. D'Souza:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-20-299, "Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements," dated December 18, 2019 (GAO Code 103316). The Department is in general agreement with the overall content of the draft audit report. Enclosed are detailed comments on the report recommendations.

The Department appreciates the opportunity to review the draft report. My point of contact for this matter is Mr. Kevin Dulany, Kevin.M.Dulany.civ@mail.mil, (571-372-4699).

Sincerely,

A handwritten signature in black ink, appearing to read "Dana Deasy".

Dana Deasy

Enclosure:
As stated

GAO DRAFT REPORT DATED DECEMBER 19, 2019
GAO-20-299 (GAO CODE 103316)

**“Critical Infrastructure Protection: Additional Actions Needed to Identify Framework
Adoption and Resulting Improvements”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should take steps, in coordination with its Sector Coordinating Council, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives.

DoD RESPONSE: Concur. In October 2019, DoD Defense Industrial Base (DIB) Cybersecurity Program published the voluntary “DIB Guide to Implementing the Cybersecurity Framework,” to assist organizations in evaluating current and desired cybersecurity maturity levels and assessing how their current activities align with DoD requirements. Currently, DoD has processes and resources in place to help determine the type of framework adoption across the DIB by conducting assessments on the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations” implemented through requirements in the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting.” The DFARS Clause requires defense contractors to implement NIST SP 800-171 security controls on their networks to protect covered defense information. The voluntary “DIB Guide to Implementing the Cybersecurity Framework” maps to the NIST SP 800-171 standards assisting defense contractors in identifying the level of cybersecurity maturity for their organization. DoD is also collaborating with NIST in the development of NIST SP 800-171B (Draft), “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets” as another framework that would require enhanced security requirements for DoD critical programs or high value assets focusing on countering the advanced persistent threat.

Appendix V: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

February 11, 2020

Ms. Neela Lakhmani
Assistant Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Lakhmani,

Thank you for providing a draft copy of the Government Accountability Office (GAO) report, "*Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements (GAO-20-299)*."

The Department of Energy (DOE) partially concurs with GAO's recommendation for DOE, but recommends the attached revision to make the recommendation more specific, achievable, and measurable. Implementation of the Department's revision will help increase understanding of the potential benefits of the National Institute of Standards and Technology Cybersecurity Framework while continuing to recognize the voluntary character of the framework. Also attached are two technical edits recommended by the Department.

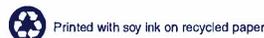
GAO should direct any questions to Mr. Fowad Muneer, Infrastructure Systems Analyst, at (202) 586-5961 or via email at fowad.muneer@hq.doe.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Karen S. Evans".

Karen S. Evans
Assistant Secretary
Cybersecurity, Energy Security and
Emergency

Enclosure



ENCLOSURE

GAO Draft Report
Critical Infrastructure Protection: Additional Actions Needed to Identify
Framework Adoption and Resulting Improvements (GAO-20-299)
Response to Report Recommendations

Recommendation 4: *The Secretary of Energy should take steps, in coordination with its SCC, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives.*

Management Response: Partially Concur.

The Department of Energy (DOE) will coordinate with the Energy Sector to develop an understanding of sector-wide improvements from use of the framework. DOE requests the recommendation to be revised to read:

The Department of Energy should take steps, in coordination with its sector stakeholders, to develop an understanding of sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives.

Implementing GAO's recommendation as written prescribes the Sector Coordinating Council (SCC) as a forum for coordination regarding the Framework. DOE should have the flexibility to consider other industry forums that might be more effective. Also, the recommendation implies that improvements could accurately be attributed to a single initiative; such direct attribution may be misleading. Suggesting government "collection" and "reporting" of information regarding adoption or improvements erodes the voluntary character of the Framework, which affects DOE efforts for adoption.

Estimated Completion Date: December 31, 2021.

The Department of Energy requests the above revision to Recommendation 4 so that the recommendation does not:

- Limit or prescribe the forums used for coordination. It is necessary for DOE to coordinate with Energy Sector organizations through a number of forums including, but not limited to, the SCCs.
- Imply that improvements could accurately be attributed to a single initiative. Energy Sector organizations are engaged in several concurrent public and private cybersecurity initiatives. Attribution of improvements directly to any one initiative may be misleading.
 - As an example, a utility may be engaged in incident response exercises, industry threat briefings, multi-year planning, the Cybersecurity Capability Maturity Model (C2M2), the National Institute of Standards and Technology Cybersecurity Framework, technology upgrades, and

other unspecified business confidential initiatives. If that organization then successfully thwarts a phishing campaign, attributing this as a direct improvement from one of these efforts may create a false picture of the performance of the framework and other efforts.

- The Cybersecurity Framework is a voluntary program. Private organizations have no requirement or incentive to share information about their cybersecurity programs. This impedes the collection and reporting of accurate information regarding adoption or improvements.

Appendix VI: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

JAN 21 2020

Vijay D'Souza
Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. D'Souza:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*" (GAO-20-299).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

A handwritten signature in blue ink, appearing to read "Sarah Arbes".

Sarah Arbes
Acting Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED — CRITICAL INFRASTRUCTURE PROTECTION:
ADDITIONAL ACTIONS NEEDED TO IDENTIFY FRAMEWORK ADOPTION AND
RESULTING IMPROVEMENTS (GAO-20-299)**

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 7

The Secretary of Health and Human Services Administration should take steps, in coordination with its SCC, to collect and report sector-wide improvements from the use of the framework across its critical infrastructure sector using existing initiatives.

HHS Response

HHS concurs with GAO's recommendation. HHS will continue to work in coordination with NIST and the SCC to refine and communicate best practices out to the sector. HHS notes that additional resources may be required to support efforts at the level recommended by GAO.

Appendix VII: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

February 6, 2020

Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-299, "CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements"

Dear Mr. D'Souza:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of years of effort by DHS, in its capacity as the Sector-Specific Agency (SSA) or co-SSA for nine of the nation's 16 critical infrastructure sectors, to promote and support adoption of the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (the framework). For example, DHS established the Critical Infrastructure Cyber Community Voluntary Program to encourage framework adoption and undertook multiple efforts as part of this program, such as working with Sector Coordinating Councils (SCCs) to develop framework implementation guidance and tools. DHS regularly discusses the framework and the benefits of framework adoption with sector partners at recurring sector meetings and individually. DHS remains committed to better understanding critical infrastructure sectors and how best to manage and mitigate cyber threats aligned against them.

The draft report contained ten recommendations, including one for DHS with which the Department concurs. Attached find our detailed response to the recommendation. DHS previously submitted technical comments under a separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,



JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: Management Response to Recommendation
Contained in GAO-20-299**

GAO recommended that the Secretary of Homeland Security:

Recommendation 8: Take steps, in coordination with its SCC, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives.

Response: Concur. DHS serves as the SSA or co-SSA for nine of the nation's 16 critical infrastructure sectors. Specifically:

- DHS's Cybersecurity and Infrastructure Security Agency (CISA) Sector Outreach and Programs Division serves as the SSA for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Reactors, Materials, and Waste sectors.
- CISA's Cybersecurity Security Division (CSD) serves as the SSA for the Communications and IT sectors.
- The Federal Protective Service serves as the co-SSA, with the General Services Administration, for the Government Facilities Sector.

CSD, in its SSA capacity and in close coordination with the IT Sector Coordinating Council, recently issued a survey to small and mid-sized IT sector partners to better understand framework adoption and use with the IT sector. Once the results of the survey are received, CISA will determine the feasibility of issuing similar surveys to other sectors, and the potential timelines for completing sector-specific survey modifications, issuing surveys, compiling responses, and developing white papers on the status of framework adoption for each sector.

Estimated Completion Date: December 31, 2021.

Appendix VIII: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 23, 2020

Vijay D'Souza
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. D'Souza:

Thank you for the opportunity to review the draft report entitled *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements* (the Report). This letter provides the official response of the Department of the Treasury.

The Report assesses the extent to which (1) sector-specific agencies, including Treasury, have developed methods to determine the level and type of adoption of the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure (the NIST Framework) and (2) implementation of the NIST Framework has led to improvements in the protection of critical infrastructure from cyber threats.

The Report recommends that Treasury take steps, in coordination with the Financial Services Sector Coordinating Council, to collect and report sector-wide improvements from the use of the NIST Framework across the financial services sector using existing initiatives. It also notes that NIST and the Department of Homeland Security have identified initiatives to help address impediments identified by multiple Sector Specific Agencies, including Treasury.

Treasury will assess using the identified initiatives and their viability for collecting and reporting sector-wide improvements from the use of the NIST Framework. In doing so, we will seek input from the Financial Services Sector Coordinating Council as well as financial regulators and take into consideration the limits on Treasury's authority. Notably, Treasury lacks the authority to compel financial institutions to respond to inquiries regarding the sector's use of the NIST Framework, or resulting improvements.

Thank you once again for the opportunity to review the Report. We look forward to continuing to work with your office in the future.

Sincerely,



David Lacquemont
Deputy Assistant Secretary
Cybersecurity and Critical Infrastructure Protection

Appendix IX: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

WASHINGTON, D.C. 20460

JAN 30 2020

OFFICE OF WATER

Mr. Alfredo Gomez
Natural Resources and Environment
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Gomez:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report, "Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements (GAO-20-299)".

The purpose of this letter is to provide the response of the Environmental Protection Agency (EPA) to the draft report's findings, conclusions, and recommendations.

GAO developed this report to fulfill a requirement under the Cybersecurity Enhancement Act of 2014 to assess periodically the extent to which critical infrastructure sectors have adopted the *Framework for Improving Critical Infrastructure Cybersecurity* (Framework). GAO's objectives for this report were to determine the extent to which (1) Sector Specific Agencies (SSA) have assessed the level and type of Framework adoption, and (2) Framework implementation has led to improvements in critical infrastructure protection from cyber threats.

To address these objectives, GAO analyzed documentation from 9 SSAs and 13 of 16 Sector Coordinating Councils (SCC), the National Institute of Standards and Technology (NIST), and Information Sharing and Analysis Centers (ISAC). GAO also interviewed officials from two critical infrastructure facilities in each of six critical infrastructure sectors. The EPA participated in these interviews as the SSA for the Water and Wastewater Systems (Water) sector under Presidential Policy Directive 21.

GAO Recommendation:

The Administrator of the EPA should take steps, in coordination with its SCC, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives.

EPA Response:

The EPA agrees with GAO's recommendation to the Agency and consequently will coordinate with the Water SCC to investigate options to collect and report sector-wide improvements from use of the cybersecurity framework across the water sector consistent with statutory requirements and the Sector's willingness to participate.

The EPA also has included an appendix to provide additional considerations to GAO with respect to the report's findings and statements.

In conclusion, the EPA is the sector specific agency for the Nation's 65,000+ water utilities and is responsible for cyber security coordination, interface, mitigation, and incident response. We fulfill our mission by working in tandem with our many government and industry partners. Through these collaborative efforts, the EPA has developed effective products and solutions to reduce risk and increase resilience to cyber threats.

To address further information and questions, please contact Dan Schmelling at schmelling.dan@epa.gov or 202-557-0683.

David Ross,



Assistant Administrator, EPA Office of Water

Enclosure: Memorandum titled "Response to Final Report, Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress, GAO-16-79" from Kenneth Kopocis, Deputy Assistant Administrator, EPA Office of Water, October 27, 2015.

cc: EPA GAO Liaison Team
Jennifer McLain
David Travers
Debbie Newberry
Dan Schmelling

Appendix X: Comments from the General Services Administration



The Administrator

January 22, 2020

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review the U.S. Government Accountability Office (GAO) draft report, *CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements* (GAO-20-299).

GAO made the following recommendation to GSA:

The Administrator of the General Services Administration should take steps, in coordination with the Department of Homeland Security, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives.

GSA agrees with the recommendation and is working with the Department of Homeland Security to develop a plan to address the issues. If you have any questions or concerns, please contact me at (202) 969-7277 or Jeffrey A. Post, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink that reads "Emily W. Murphy".

Emily W. Murphy
Administrator

cc: Mr. Vijay D'Souza, Director, Information Technology and Cybersecurity, GAO

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

Appendix XI: GAO Contact and Staff Acknowledgments

GAO Contact

Vijay A. D'Souza at (202) 512-6240 or Dsouzav@gao.gov

Staff Acknowledgments

In addition to the contact named above, Neelaxi Lakhmani (assistant director), Kendrick M. Johnson (analyst in charge), Christopher Businsky, Nancy Glover, Douglas Harris, Ceara Lance, Edward Malone, Gabriel Nelson, Harold Podell, and Dana Pon 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

