



February 2022

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Assess Adoption of Cybersecurity Guidance

Accessible Version

GAO Highlight

Highlights of [GAO-22-105103](#), a report to congressional committees

Why GAO Did This Study

The nation's 16 critical infrastructure sectors provide essential services such as banking, electricity, and gas and oil distribution. However, increasing cyber threats—like the May 2021 ransomware cyberattack on an American oil pipeline system that led to regional gas shortages—represent a significant national security challenge. To better protect against cyber threats, NIST facilitated, as required by federal law, the development of a voluntary framework of cybersecurity standards and procedures for sectors to use.

The *Cybersecurity Enhancement Act of 2014* included provisions for GAO to review aspects of the framework. GAO's report addresses the extent to which SRMAs have (1) determined framework adoption by entities within their respective sectors and (2) identified improvements resulting from sector-wide use. GAO analyzed documentation, such as requests for information, polls, and survey instruments. It also conducted interviews with agency officials from each SRMA and NIST.

What GAO Recommends

In prior reports, GAO recommended that the nine SRMAs (1) develop methods for determining the level and type of framework adoption by entities across their respective sectors and (2) collect and report sector-wide improvements. Most agencies have not yet implemented these recommendations.

View [GAO-22-105103](#). For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

February 2022

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Assess Adoption of Cybersecurity Guidance

What GAO Found

Federal agencies with a lead role to assist and protect one or more of the nation's 16 critical infrastructures are referred to as sector risk management agencies (SRMAs). The SRMAs for three of the 16 have determined the extent of their sector's adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (framework). In doing so, lead agencies took actions such as developing sector surveys and conducting technical assessments mapped to framework elements. SRMAs for four sectors have taken initial steps to determine adoption (see figure). However, lead agencies for nine sectors have not taken steps to determine framework adoption.

Status of Framework Adoption by Critical Infrastructure Sector



Source: GAO analysis based on agency data. | GAO-22-105103

Regarding improvements resulting from sector-wide use, five of the 16 critical infrastructure sectors' SRMAs have identified or taken steps to identify sector-wide improvements from framework use, as GAO previously recommended. For example, the Environmental Protection Agency identified an approximately 32 percent overall increase in the use of framework-recommended cybersecurity controls among the 146 water utilities that requested and received voluntary technical assessments. In addition, SRMAs for the government facilities sector identified improvements in cybersecurity performance metrics and information standardization resulting from federal agencies' use of the framework. However, SRMAs for the remaining 11 sectors did not identify improvements and were not able to describe potential successes from their sectors' use of the framework.

SRMAs reported various challenges to determining framework adoption and identifying sector-wide improvements. For example, they noted limitations in knowledge and skills to implement the framework, the voluntary nature of the framework, other priorities that may take precedence over framework adoption, and the difficulty of developing precise measurements of improvement were challenges to measuring adoption and improvements. To help address challenges, NIST launched an information security measurement program in September 2020 and the Department of Homeland Security has an information network that enables sectors to share best practices. Implementing GAO's prior recommendations on framework adoption and improvements are key factors that can lead to sectors pursuing further protection against cybersecurity threats.

Contents

GAO Highlight	2
Why GAO Did This Study	2
What GAO Recommends	2
What GAO Found	2
Letter	1
Background	6
SRMAs Had Not Determined Framework Adoption for Most Sectors; Measurement Challenges Persist	17
Most SRMAs Have Not Identified Framework-Driven Improvements	29
Agency Comments	42
Appendix I: GAO Contact and Staff Acknowledgments	45
GAO Contact	45
Staff Acknowledgments	45
Tables	
Table 1: Examples of Cybersecurity Improvements Resulting from the Government Facilities Sector's Use of the National Institute of Standards and Technology's Cybersecurity Framework	32
Table 2: Extent to Which Sector Risk Management Agencies (SRMA) Identified Challenges to Measuring Framework Improvement	38
Figures	
Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies	9
Figure 2: Extent to Which Sector Risk Management Agencies Took Steps to Determine Critical Infrastructure Sectors' Adoption of the National Institute of Standards and Technology's Cybersecurity Framework	18
Figure 3: Critical Infrastructure Sectors That Businesses Reported Belonging to in the Department of Homeland Security's Information Technology Sector Survey	23
Figure 4: Extent to Which Sector Risk Management Agencies Took Steps to Identify Improvements Resulting from	

Abbreviations

ASPR	Assistant Secretary for Preparedness and Response
C2M2	Cybersecurity Capability Maturity Model
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EPA	Environmental Protection Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SCC	Sector Coordinating Council
SRMA	sector risk management agency
USDA	U.S. Department of Agriculture

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 9, 2021

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

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

The nation's 16 critical infrastructure sectors provide the essential services—such as banking, electricity, and oil and gas distribution—that underpin American society.¹ These sectors rely on electronic systems and data to support their missions.

However, cyber threats to the infrastructure continue to increase and represent a significant national security challenge. Specifically, malicious actors have intruded and extracted information from, and disrupted the networks of, both government agencies and major critical infrastructure companies. Recent incidents—such as the ransomware attack on the Colonial pipeline and attacks targeting health care and essential services during the Coronavirus Disease 2019 (COVID-19) pandemic—illustrate

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; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.

the pressing need to strengthen federal and critical infrastructure cybersecurity.²

To address the cyber-based threats to critical infrastructure, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013.³ This order aimed to enhance the security and resilience of the nation's critical infrastructures and maintain a 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 include a set of industry standards and best practices to help organizations manage cybersecurity risks.⁴ In response, NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) in February 2014.

NIST intended for the framework to provide private sector organizations⁵ with principles and best practices for risk management, in order to

²On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. See GAO, [Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness \(infographic\)](#), (Washington, D.C.: May 18, 2021). In May 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released a joint alert with the United Kingdom's National Cyber Security Centre regarding advanced persistent threat groups exploiting COVID-19 to target health care and essential services. The alert warned that advanced persistent threat groups were frequently targeting organizations in order to collect bulk personal information, intellectual property, and intelligence that aligns with national priorities. See GAO, *HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, [GAO-21-403](#) (Washington, D.C.: June 28, 2021).

³The White House, Executive Order No. 13636 (Washington, D.C.: Feb. 12, 2013), 78 Fed. Reg. 11737 (Feb. 19, 2013).

⁴NIST is a component within the Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the nation's quality of life.

⁵Private 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.

improve the security and resilience of the nation's critical infrastructure.⁶ NIST's role was established in statute by the *Cybersecurity Enhancement Act of 2014 (Cybersecurity Act)*, which required the agency to, among other things, facilitate and support the development of a voluntary set of standards, best practices, and procedures to reduce cyber risks to critical infrastructure on an ongoing basis.⁷

The *Cybersecurity Act* included a provision for us to conduct a series of reviews and report on various aspects of the framework. We reported on the framework in 2015, 2017, and 2019.⁸ In our December 2017 report, we noted that sector risk management agencies (SRMAs)⁹ did not have qualitative or quantitative measures of framework adoption because they generally did not collect specific information from entities about critical infrastructure protection activities. We recommended that the SRMAs take steps to develop methods for determining the level and type of framework adoption by entities across their respective critical infrastructure sectors.¹⁰

In addition, in December 2019, we reported that NIST had planned initiatives—such as its information security measurement program and the framework starter profile—that could help SRMAs overcome impediments and measure improvements from framework use. We recommended that NIST establish time frames for completing its initiatives. We also noted that none of the SRMAs had collected and reported sector-wide improvements from use of the framework by entities

⁶National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). Version 1.1 of the framework was issued Apr. 16, 2018.

⁷Pub. L. No. 113-274, § 101(a)(2), 128 Stat. 2971, 2972 (Dec. 18, 2014).

⁸GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, [GAO-16-152](#) (Washington, D.C.: Dec. 17, 2015); *Critical Infrastructure Protection: Additional Actions Are Essential For Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: Feb. 15, 2018); and *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, [GAO-20-299](#) (Washington, D.C.: Feb. 25, 2020).

⁹SRMAs lead, facilitate, and support, the security and resilience programs and associated activities of their designated critical infrastructure sector.

¹⁰For the purposes of this report, "level" of adoption refers to the number or proportion of entities within each sector that have adopted the framework. "Type" of framework adoption refers to the manner in which the framework has been used or adopted by sector entities.

within their 16 respective sectors and recommended that the SRMAs do so.

Our specific objectives for this review were to determine the extent to which SRMAs have taken steps to (1) determine framework adoption by entities within their respective sectors and (2) identify sector-wide improvements from framework use across their critical infrastructure sectors.

For both objectives, we obtained and reviewed information on the actions of the nine SRMAs that lead, facilitate, and support the security and resilience programs and associated activities of their designated critical infrastructure sectors.¹¹ They are the 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).

Five of the nine SRMAs—DHS, DOT, GSA, HHS, and USDA—also function as co-SRMAs, in which they work collaboratively to support a particular sector. Specifically, as co-SRMAs, HHS and USDA lead the food and agriculture sector; GSA and DHS lead the government facilities sector; and DHS and DOT lead the transportation systems sector. In instances where co-SRMAs demonstrated evidence of actions taken to address our recommendations, we acknowledged the actions that these agencies took individually or in collaboration.

To address the first objective, we obtained and reviewed documentation, such as survey instruments that the nine SRMAs used and requests for information that they distributed to sector members, to gather information regarding the sectors' adoption of the framework. We also reviewed documentation, such as NIST's cybersecurity case studies on encryption and business security standards, social engineering and phishing, and data breaches. In addition, we obtained and reviewed the Department of Energy's *Cybersecurity Capability Maturity Model* and EPA's

¹¹The nine SRMAs in our review comprise all of the 16 critical infrastructure sectors.

cybersecurity assessments from its Technical Assistance Provider Initiative.¹²

Using the above documentation, we identified and evaluated any actions that the nine SRMAs had taken that addressed our prior recommendations related to determining framework adoption. Specifically, we assessed whether they had determined framework adoption, taken steps but had not yet determined framework adoption, or had not taken steps to determine framework adoption for their respective sectors.

We supplemented our analysis by interviewing officials from NIST and the SRMAs. We did so to confirm our understanding of the steps taken to determine framework adoption and to identify any challenges the SRMAs had encountered in their efforts.

To address the second objective, we collected and reviewed documentation from NIST, such as its framework, its April 2019 *Roadmap for Improving Critical Infrastructure Cybersecurity*,¹³ case studies of success in using the framework, and planned updates to NIST's performance measurement guide.¹⁴ We also reviewed documentation from the nine SRMAs, such as technical assessments and results from polls that they conducted regarding sector entities' observations of improvements from using the framework. In addition, we obtained and reviewed DHS's Information Technology Sector Small and Midsize

¹²EPA's Technical Assistance Provider Initiative provides technical assessments, on a voluntary basis, of water and wastewater utilities' implementation of cybersecurity safeguards that are consistent with the framework.

¹³National 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 framework and identifies key areas of development, alignment, and collaboration.

¹⁴National 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.

Business Cybersecurity Survey and 2018 Cybersecurity Resources Road Map.¹⁵

Using this documentation, we identified actions that NIST and the nine SRMAs had taken to address our prior recommendations related to measuring improvements from sectors' use of the framework. In doing so, we determined whether NIST had established time frames for its initiatives, and whether the SRMAs had identified improvements, taken steps but had not yet identified improvements, or had not taken steps to identify improvements resulting from the use of the framework for their respective sectors.

We supplemented our analyses by interviewing officials from NIST and the SRMAs to confirm our understanding of the steps taken to complete initiatives and determine improvements from use of the framework. We also sought to identify any challenges that SRMAs had encountered in their efforts. This included asking SRMAs and NIST to confirm challenges that we previously reported on that were still relevant.¹⁶ We then asked the SRMAs and NIST to identify any additional challenges.

We conducted this performance audit from January 2021 to February 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

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

¹⁵Department of Homeland Security, *Cybersecurity Resources Road Map: A Guide for Critical Infrastructure, Small and Midsize Businesses* (Washington, D.C.: July 2018). This road map was intended to help critical infrastructure for small and midsize businesses identify useful cybersecurity resources to meet their needs.

¹⁶[GAO-20-299](#).

production and transmission facilities, most of which are owned and operated by the private sector.

Threats to the systems supporting our nation's critical infrastructure 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 natural disasters and the failure of other critical infrastructure, 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. For example, adversaries can leverage common computer software programs to deliver a threat by embedding exploits within software files. These files can be activated when a user opens a file within its corresponding program, similar to what was done in the SolarWinds attacks.¹⁷

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we 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 2021 high-risk update on major cybersecurity challenges.¹⁸

¹⁷The SolarWinds attacks were a campaign of cyberattacks by the Russian Foreign Intelligence Service. In February 2020, the service injected trojanized (hidden) code into a file included in SolarWinds' software updates. SolarWinds released the updates to customers, exposing them to the hidden code that allowed the Russian Foreign Intelligence Service a "backdoor," or program that gave them remote access to any computers that had downloaded the software. SolarWinds estimates that nearly 18,000 customers were affected. See GAO, [SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response \(infographic\)](#), (Washington, D.C.: Apr. 22, 2021) and [Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents](#), [GAO-22-104746](#) (Washington, D.C.: Jan. 13, 2022).

¹⁸GAO, [High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges](#), [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

Since 2010, we have made nearly 80 recommendations in public reports to enhance infrastructure cybersecurity, including measuring the adoption of the NIST framework. However, as of November 2021, a majority of these recommendations (nearly 50) had not been implemented.

Law, Orders, and Directives Assign Responsibilities for 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, a presidential directive assigns roles and responsibilities for federal agencies to assist the private sector in protecting critical infrastructure, including enhancing cybersecurity.

Presidential Policy Directive 21, issued in February 2013, established sector specific agencies as the federal entities responsible for providing institutional knowledge and specialized expertise for enhancing and protecting the cybersecurity of critical infrastructure.¹⁹ Since then, the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* has updated the name for these agencies, stating that the term "sector risk management agency" holds the meaning previously given to the term "sector specific agency."²⁰ The act also amended the *Homeland Security Act of 2002* by adding a section on SRMAs and their responsibilities.

As leads for facilitating and supporting the security and resilience programs and associated activities of their designated critical infrastructure sectors, SRMAs' specific responsibilities include assessing sector risk, facilitating sector coordination and information sharing, and contributing to incident management and emergency preparedness. The Presidential Policy Directive 21 identified 16 critical infrastructure sectors and designated the nine associated SRMAs, which were referenced in the 2021 NDAA. As shown in figure 1, SRMAs are responsible for at least one sector each. HHS and DHS work with multiple sectors.

¹⁹The White House, Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

²⁰Pub. L. No. 116-283, § 9002(a)(7), 134 Stat. 3388, 4768 (2021).

Figure 1: Critical Infrastructure Sectors and Related Sector Risk Management Agencies



Sector risk management 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 DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-22-105103

Notes: The Department of Energy's sector risk management agency responsibilities are codified in law by the *Fixing America's Surface Transportation Act (FAST Act)*. Pub. L. No. 114-94, § 61003(c), 129 Stat. 1312, 1779 (2015). The FAST Act contains provisions designed to protect and enhance the nation's electric power delivery infrastructure.

Presidential Policy Directive 21 required DHS to update the *National Infrastructure Protection Plan*²¹ to address the implementation of the directive.²² 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; it also called for a metrics and analysis process to be used to measure the nation's ability to manage and reduce risks to critical infrastructure.

In response, DHS updated the *National Infrastructure Protection Plan* in December 2013. It did so in collaboration with public and private sector owners and operators and federal and nonfederal government representatives, including SRMAs, from the critical infrastructure community. According to the 2013 plan, SRMAs 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, including the SRMAs, sector coordinating councils (SCC) 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 SRMAs and the SCCs coordinate and collaborate in a voluntary fashion on issues pertaining to their respective critical infrastructure sectors.

Executive Orders and Federal Law for the Protection of Critical Infrastructure Sectors

In addition to Presidential Policy Directive 21, federal law and executive orders have also established roles and responsibilities for federal agencies to work with industry to enhance the cybersecurity of the nation's critical infrastructure. These include Executive Order 13636,²³ the

²¹The 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.

²²Department 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.

²³Executive Order No. 13636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

Cybersecurity Enhancement Act of 2014, Executive Order 13800,²⁴ and the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*.²⁵

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 SRMAs, in consultation with DHS and other interested agencies, to coordinate with the SCCs to review the framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.²⁶

Further, in December 2014, the *Cybersecurity Enhancement Act of 2014* established requirements regarding NIST's development of a cybersecurity framework. According to this law, NIST's responsibilities in supporting the ongoing development of the framework include, 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., SRMAs, SCCs, and information sharing and analysis centers²⁷) to identify a prioritized, performance-based approach to include information security measures to help entities assess risk.

In May 2017, Executive Order 13800 was issued for federal agency heads, including members of the government facilities sector, to manage cybersecurity risks. Specifically, the executive order directed federal agency heads to use the framework to manage cybersecurity risks. The executive order also required agencies/agency heads to provide a risk

²⁴The 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).

²⁵The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (Washington, D.C.: Jul. 28, 2021).

²⁶Executive 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.

²⁷Information sharing and analysis centers are sector-based organizations with the purpose of maximizing information flow between private critical infrastructure entities and the government in order to better protect entities from cyber and physical security threats.

management report to DHS and the Office of Management and Budget (OMB) within 90 days of the date of the executive order. The risk management report was to document the agency's risk mitigation and acceptance choices including, for example, describing the agency's action plan to implement the framework.

Besides managing cyber risks, in July 2021, the White House issued a memorandum that required DHS to issue sector-specific critical infrastructure cybersecurity performance goals within 1 year of the date of the memorandum's publication.²⁸ The performance goals are expected to serve as guidance for each SRMA in evaluating sectors' cybersecurity practices.

DHS Directives and Initiative for Enhancing the Cybersecurity of Critical Infrastructure

In addition to the previously mentioned executive orders and federal law, DHS also issued several directives and established an initiative to further define roles and responsibilities that are aimed at enhancing the cybersecurity of critical infrastructure. For example, the department introduced two security directives that require owners and operators of agency-designated critical pipelines that transport hazardous liquids and natural gas to implement certain protections against cyber intrusions.²⁹ Among other things, the directives require the critical pipeline owners and operators to identify cybersecurity coordinators, report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), test the effectiveness of existing practices, develop contingency plans, and implement mitigations for cyber-related risks.

In December 2021, DHS's Transportation Security Administration announced that it had established two additional security directives and issued additional requirements that aimed to strengthen cybersecurity

²⁸The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (Washington, D.C.: Jul. 28, 2021).

²⁹Transportation Security Administration, *Security Directive Pipeline-2021-01*, accessed Dec. 6, 2021, <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators> and *Security Directive Pipeline-2021-02A*, accessed Dec. 6, 2021, <https://www.tsa.gov/news/press/releases/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline>.

across the transportation sector.³⁰ Specifically, the agency issued two security directives for freight rail and public transportation and passenger rail that require owners and operators of those rail systems to take several steps to enhance cyber protections. These owners and operators are to designate a cybersecurity coordinator, report incidents to CISA within 24 hours, develop and implement incident response plans, and complete a cybersecurity vulnerability assessment.

According to the Transportation Security Administration's press release, the agency also recently updated requirements for its aviation security programs. Specifically, the Transportation Security Administration stated that it requires airport and airline operators to implement a cybersecurity coordinator and report incidents to CISA within 24 hours.

DHS has also recently established an initiative to further enhance the nation's critical infrastructure cybersecurity. In August 2021, CISA created the Joint Cyber Defense Collaborative. According to CISA, the collaborative brings partners together to unify defensive actions and drive down risk in advance of cyber incidents. Partners include federal, state, local, territorial, and tribal governments; and the public and private sectors. Additionally, CISA officials stated that collaboration between these partners is designed to strengthen the nation's cyber defenses—including protections against cyberattacks targeting critical infrastructure—through planning, preparation, and information sharing.

NIST Established a Framework for Improving Critical Infrastructure Cybersecurity

In response to Executive Order 13636, in February 2014, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity*, a voluntary framework of cybersecurity standards and procedures for industry to adopt. According to NIST, the framework had been downloaded approximately 1.6 million times as of October 2021. Additionally, it has been translated into Arabic, Bulgarian, Indonesian, Japanese, Polish, Portuguese, and Spanish, and has been adopted by many foreign governments.

³⁰Transportation Security Administration, *Security Directive-1580-21-01* and *Security Directive-1582-21-02*, accessed Dec. 6, 2021, <https://www.tsa.gov/news/press/releases/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation>.

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 framework core, organizations can better communicate cybersecurity practices between teams using simple, nontechnical language.

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.

Each function is broken down into categories, which are groups of cybersecurity outcomes tied to programmatic needs and particular activities (e.g., asset management). There are 23 categories for the five functions.

Subcategories further divide a category into specific outcomes of technical and/or management activities (e.g., for the category of anomalies and events, the activity is that detected events are analyzed to understand attack targets and methods).³¹ There are 108 subcategories for the 23 categories.

Lastly, informative references are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes described. They support one or more of the subcategories (e.g., NIST Special Publication 800-53).³²

Implementation tiers characterize an organization’s approach to managing cybersecurity risks over a range of four tiers. The four tiers are

³¹Intrusion 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.

³²National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations, SP 800-53*, revision 4 (Gaithersburg, MD.: April 2013). This document provides guidelines for establishing controls for systems and organizations.

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 road maps for reducing cybersecurity risks that are 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.

NIST officials stated that they planned to begin the process of updating the framework by issuing a call to stakeholders for input on areas for improvement. According to NIST, the updates may include areas such as addressing and advancing cybersecurity measurement challenges and solutions.

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

In December 2015, we reported that the NIST framework met the requirements established in federal law that it be flexible, repeatable, performance-based, and cost-effective. We also reported that SRMAs and NIST had promoted and supported adoption of the framework in the critical infrastructure sectors.

However, we noted that DHS had not developed metrics to measure the success of its activities and programs. Accordingly, 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 SRMAs had promoted the framework in their sectors and most had 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 whether sector-specific implementation guidance was needed for the government facilities 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.

In February 2018, we found that most of the 16 critical infrastructure sectors had taken action to facilitate adoption of the framework by entities within their sectors.³³ Specifically, 12 critical infrastructure sectors had taken actions to review the framework and, if necessary, had developed implementation guidance or supplemental materials that addressed how entities within their respective sectors could adopt the framework.

We also noted that none of the 16 sector coordinating councils had reported having qualitative or quantitative measures of framework adoption because they generally did not collect specific information from entities about critical infrastructure protection activities. As a result, we recommended that the nine SRMAs develop methods for determining the level and type of framework adoption by entities across their respective sectors. Among these SRMAs, five (DOD, HHS, DHS, DOT, and GSA) agreed with our recommendations, and four (USDA, DOE, Treasury, and EPA) neither agreed nor disagreed with the recommendations.

More recently, in February 2020, we pointed out that most of the SRMAs still had not developed methods to determine the level and type of framework adoption.³⁴ We also reported that SRMAs for 13 of the 16 critical infrastructure sectors had taken steps to encourage and facilitate the use of the framework, such as developing implementation guidance that links existing sector cybersecurity tools, standards, and approaches to the framework. However, the SRMAs had not collected and reported sector-wide improvements due to various impediments, such as the lack of precise measurements on improvements. We noted that NIST and DHS had existing and planned initiatives that could help SRMAs overcome impediments and measure improvements from framework use.

We recommended that the nine SRMAs take steps to consult with respective sector partner(s), such as the SCCs, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across their critical infrastructure sectors using existing initiatives. We also recommended that NIST establish time frames for completing initiatives to enable the identification of sector-wide improvements from using the framework. Eight SRMAs and NIST agreed

³³[GAO-18-211](#).

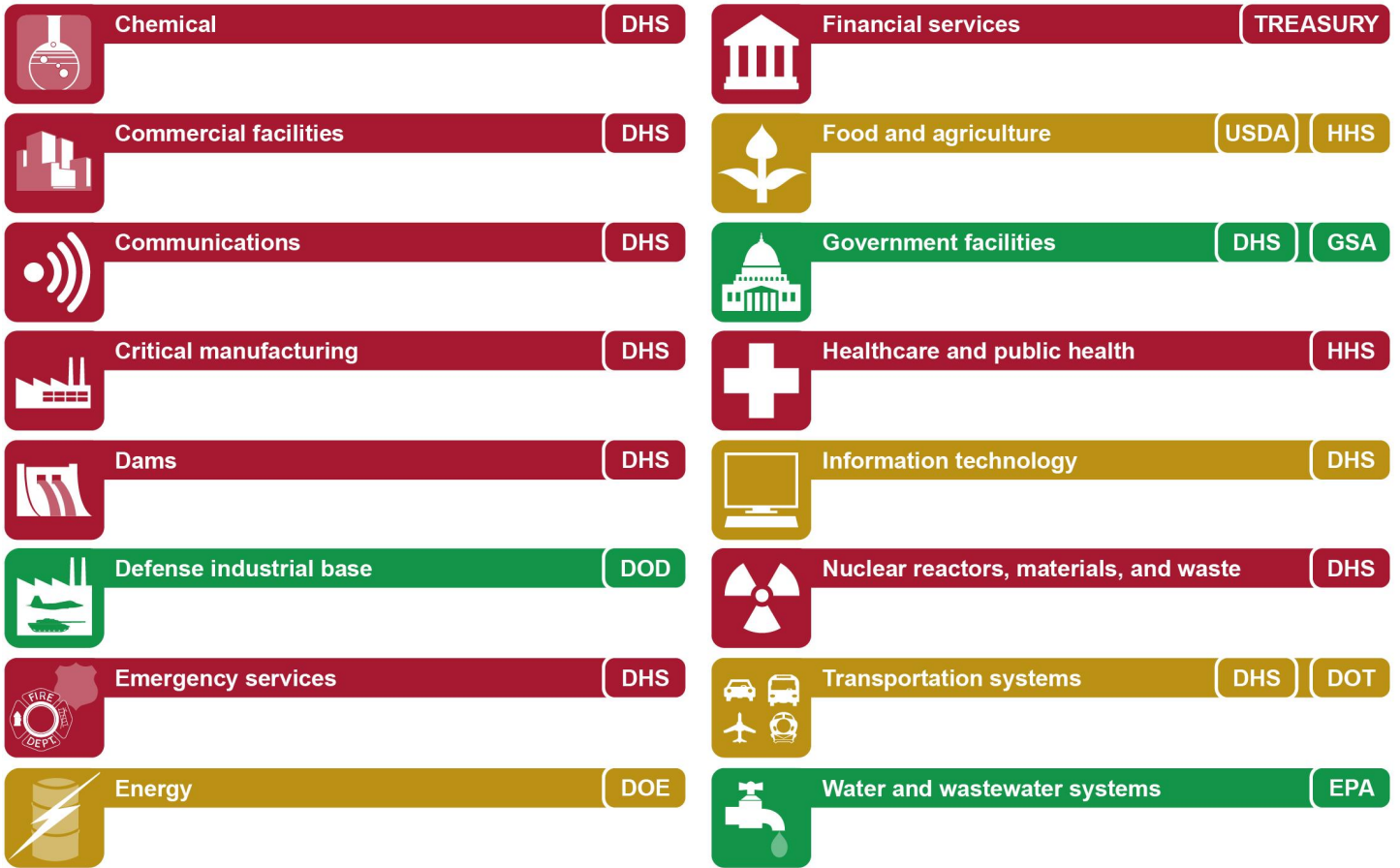
³⁴[GAO-20-299](#).

with the recommendations, while one SRMA neither agreed nor disagreed and one partially agreed.

SRMAs Had Not Determined Framework Adoption for Most Sectors; Measurement Challenges Persist

Best practices identified in the *National Infrastructure Protection Plan* recommend that entities, such as SRMAs and SCCs, take steps to evaluate progress toward achieving their goals—in this case, to implement or adopt the framework. As of November 2021, the SRMAs or co-SRMAs for three of the 16 critical infrastructure sectors had determined framework adoption among certain entities within their respective sectors. The SRMAs or co-SRMAs for four of the 16 sectors had taken initial steps, but had not yet determined framework adoption. The other nine sectors had not taken steps to determine framework adoption (see figure 2).

Figure 2: Extent to Which Sector Risk Management Agencies Took Steps to Determine Critical Infrastructure Sectors' Adoption of the National Institute of Standards and Technology's Cybersecurity Framework



- Have not taken steps to determine adoption
- Have taken steps to determine adoption
- Determined adoption

Sector risk management 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 agency data, Presidential Policy Directive-21, and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-22-105103

Note: Five of the nine SRMAs—DHS, DOT, GSA, HHS, and USDA—are co-SRMAs for one or more sectors that lead, facilitate, and support the security and resilience programs and associated activities of their designated critical infrastructure sector. The food and agriculture (USDA, HHS), government facilities (DHS, GSA), and transportation systems (DHS, DOT) sectors are led by co-SRMAs.

SRMAs for Three Sectors Determined Framework Adoption

In February 2020, we reported that DOD, in collaboration with the defense industrial base sector, took steps to determine framework adoption across the sector.³⁵ Specifically, we noted that DOD had developed a process, through its cyber incident reporting scorecard, to monitor the level or extent to which contracts (not including commercial off-the-shelf contracts) were or were not adhering to the cybersecurity requirements in DOD acquisition regulations.³⁶ DOD regulation³⁷ calls for contractors to implement, for their covered information systems, the security requirements in NIST Special Publication 800-171,³⁸ which DOD mapped to the functional areas of the framework. We found that by doing so, DOD was 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. As of June 2020, DOD determined that approximately 95 percent of contracts (not including commercial off-the-shelf contracts) included a clause from DOD regulation that required implementation of security requirements from NIST Special Publication 800-171.³⁹

In the same February 2020 report, we noted that GSA, in coordination with DHS's Federal Protective Service as the co-SRMA, took steps to

³⁵[GAO-20-299](#).

³⁶DOD, *Safeguarding Covered Defense Information and Cyber Incident Reporting Scorecard (Fiscal Year 2020, Q3)*.

³⁷DOD, *Defense Federal Acquisition Regulation Supplement (48 CFR § 252.204-7012)*.

³⁸NIST, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, Special Publication 800-171, revision 1 (Gaithersburg, MD.: December 2016).

³⁹In July 2019, DOD's Inspector General reported that the department was not always consistently tracking and monitoring organizations' implementation of the acquisition regulations. See DOD, *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*, DODIG-2019-105 (Washington, D.C.: July 23, 2019). In addition, we recently issued a report assessing DOD's implementation of its Cybersecurity Maturity Model Certification, which includes a process for verifying that a company has implemented sufficient safeguards consistent with NIST Special Publication 800-171 to protect DOD's sensitive unclassified information as a condition of contract award. GAO, *Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework*, [GAO-22-104679](#) (Washington, D.C.: Dec. 8, 2021).

determine framework adoption for the government facilities sector. We noted that the federal departments and agencies that form the government facilities sector had submitted their risk management reports to DHS and OMB, which 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.⁴⁰ As a result, GSA and DHS, in collaboration with OMB, were able to use the reports as a resource to inform their understanding of framework adoption by sector entities. As of May 2018, OMB and DHS determined that 71 of the 96 agencies assessed were at risk or high risk due, in part, to their lack of adoption of the framework's elements.

In addition, EPA had taken steps to determine framework adoption for the water and wastewater systems sector through its Technical Assistance Provider Initiative. Through this initiative, the agency conducted, on a voluntary basis, technical assessments of water and wastewater utilities and determined whether and how these utilities used the framework. As of October 2021, EPA determined that 146 out of 264 water and wastewater utilities that were eligible for the voluntary assessments had adopted the framework and obtained metrics on the utilities' implementation of the framework's security controls. Officials in EPA's Office of Ground Water and Drinking Water stated that they expect the data on framework adoption and usage from this initiative to continue to evolve as EPA assesses more utilities and obtains additional data.⁴¹

SRMAs for Four Sectors Had Taken Initial Steps, but Had Not Yet Determined Framework Adoption

DOE, DHS, DOT and its co-SRMA, DHS; and USDA and its co-SRMA, HHS, had taken initial steps to determine framework adoption for the energy, information technology, transportation systems, and food and agriculture sectors, respectively. Specifically:

⁴⁰Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress* (fiscal year 2020).

⁴¹The EPA assessment dashboard displays cybersecurity assessment data collected from water and wastewater utilities through the Technical Assistant Provider Initiative. The database organizes the utilities' responses by framework function and tracks their progress over time.

- DOE took initial steps to determine framework adoption for the energy sector by tracking requests for a sector-based cybersecurity toolkit, assessing polling data, and obtaining anecdotal reports on framework use from sector entities.
- **Toolkit requests.** As of May 2021, DOE's Office of Cybersecurity, Energy Security, and Emergency Response reported that 1,940 organizations had downloaded 2,253 Cybersecurity Capability Maturity Model (C2M2) toolkits.⁴² The toolkit included the C2M2, version 1.1, which is mapped to the framework in the Energy Sector Cybersecurity Framework Implementation Guidance. DOE released the most recent version of the C2M2 (version 2.0) in July 2021 and the agency is currently updating the mapping of the model to the framework.
- **Polling data.** According to officials in DOE's Office of Cybersecurity, Energy Security, and Emergency Response, the agency submitted a poll to 145 cybersecurity experts from 77 companies across the energy sector with questions about their use of the framework and the C2M2. The results indicated that 59 percent of respondents reported implementing both the C2M2 and the framework, 23 percent implemented C2M2 only, and 12 percent implemented the framework only.
- **Anecdotal reports.** Officials in DOE's Office of Cybersecurity, Energy Security, and Emergency Response noted that they received anecdotal reports that indicate energy sector organizations have used the C2M2 to evaluate their cybersecurity capabilities and prioritize improvements.

While DOE had initiated the above efforts to measure adoption, those efforts did not provide sufficient information for the agency to determine the framework adoption throughout the energy sector. For instance, while downloads of toolkits can provide an indicator of potential adoption because the C2M2 model is integrated with controls from the framework, they may not directly result in framework adoption. Thus, the download numbers did not provide sufficient information about adoption. In addition, while the polling data that DOE collected is a good starting point for determining adoption, the agency noted that it is exploring strategies, such as leveraging data

⁴²The Cybersecurity Capability Maturity Model is a DOE program that enables organizations to voluntarily measure the maturity of their cybersecurity capabilities in a consistent manner. No assessment data is collected by the department.

from trade associations and conducting additional feedback sessions with other groups, to obtain broader information across the sector.

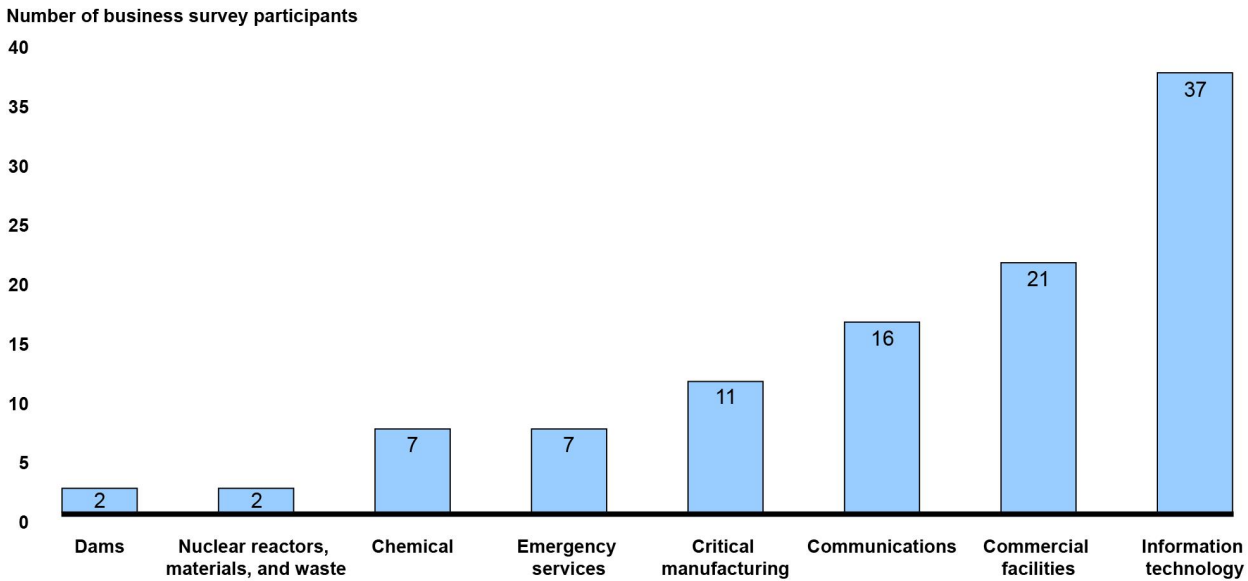
Officials from DOE's Office of Cybersecurity, Energy Security, and Emergency Response acknowledged that additional efforts are needed to determine adoption for the energy sector and are considering several additional steps. For example, DOE documented a *Concept of Operations for NIST Cybersecurity Framework Alignment, Measurement, and Reporting in the Energy Sector* that identified potential qualitative and quantitative measurements of framework adoption, as well as steps to collect additional information.

Potential steps for collecting more information about the sector's framework adoption included, among other things, engaging with NIST to ensure continued alignment of the C2M2 to the framework, learning new approaches to measuring adoption, and holding a user community workshop for organizations in the sector that adopted the framework or C2M2. DOE officials also stated that they were in the process of engaging with national laboratories to develop a report on sector usage of the framework, C2M2, and other derivative frameworks that were aligned to the NIST framework. If the agency implements its planned steps effectively, DOE could be better positioned to determine framework adoption among entities within its sector.

- DHS's CISA, in coordination with its information technology SCC, took initial steps to determine adoption by administering a survey to the information technology sector's small- and medium-sized business community from October through December 2019 to gather information on, among other things, framework use. One hundred businesses responded to the survey. CISA reported that a total of 63 of the 100 businesses used the framework alone or in conjunction with other frameworks, standards, and practices. Additionally, according to CISA officials, the businesses that responded to the survey self-identified that they were part of the information technology sector and one or more of the other seven sectors for which DHS is the SRMA.⁴³ Figure 3 identifies the sectors that businesses reported belonging to in DHS's survey.

⁴³DHS is the SRMA for eight sectors: chemical; commercial facilities; communications; critical manufacturing; dams; emergency services; information technology; and nuclear reactors, materials, and waste. DHS is the co-SRMA for the government facilities sector and the transportation systems sector.

Figure 3: Critical Infrastructure Sectors That Businesses Reported Belonging to in the Department of Homeland Security’s Information Technology Sector Survey



Source: GAO analyses of Department of Homeland Security’s 2019 information technology small and medium sized business survey. | GAO-22-105103

Accessible Data Table for Figure 3

DHS	Number of business survey participants
Dams	2
Nuclear	2
Chemical	7
Emergency services	7
Critical manufacturing	11
Communications	16
Commercial facilities	21
Information technology	37

Although the survey gathered information regarding the level and type of adoption from organizations that responded, there was not enough information for CISA to determine framework adoption across all of its sectors. For instance, each of the eight sectors for which DHS is the SRMA include thousands of businesses; yet none of the sectors had more than 40 respondents. As of September 2021, CISA did not have plans for conducting additional surveys or other steps to determine framework adoption among its sectors.

- DOT, in coordination with its co-SRMA (DHS's Transportation Security Administration), took initial steps to determine framework adoption by developing and distributing a survey to the sector from March to June of 2021. According to officials from DOT's Office of Intelligence, Security, and Emergency Response, the survey was distributed to 10 transportation systems SCC leads, along with dozens of federal sector stakeholders. DOT officials stated that the survey received a total of 857 responses as of mid-June 2021. The survey collected information on awareness and usage of the framework and the subsector of the responding organization. Further, the survey gathered information on the extent to which the organization had implemented the five core functions of the framework.

However, as of November 2021, the agencies had not yet determined framework adoption for the sector because they had not completed the analysis of the survey responses. According to officials from DOT's Office of Intelligence, Security, and Emergency Response and DHS's Transportation Security Administration, the co-SRMAs are still analyzing the results of the survey and expect to complete its analysis by the end of March 2022. Once the agencies have completed their analysis of the responses, DOT and DHS may be in a position to determine framework adoption among entities within the sector, as we have recommended.

- USDA, in coordination with HHS as the co-SRMA and its sector partners, took initial steps to determine framework adoption for the food and agriculture sector by distributing a request for information to sector members. The request for information was included in the food and agriculture sector's annual report for fiscal year 2020 to collect information on accomplishments, activities, and programs that show progress towards sector goals.

Officials from USDA's Office of Homeland Security stated that the agencies distributed the request for information to approximately 350 representatives of organizations in the food and agriculture sector and government coordinating council. Organizations included federal, state, local, tribal, and territorial governments; academia; and the private sector.

While USDA and HHS requested information on agencies' use of the framework, officials from USDA's Office of Homeland Security noted that this effort did not generate enough responses to be useful. As a result, USDA and HHS were not able to determine adoption across the sector.

As of October 2021, officials from USDA's Office of Homeland Security did not have additional plans for determining framework adoption among sector entities. However, according to agency officials, the department is in the process of preparing a request for information for the fiscal year 2021 Sector Annual Report and may include a question about framework adoption.

SRMAs for the Remaining Nine Sectors Had Not Taken Steps to Determine Framework Adoption

The SRMAs—HHS, Treasury, and DHS—for the healthcare and public health; financial services; chemical; commercial facilities; communications; critical manufacturing; dams; emergency services; and nuclear reactors, materials, and waste sectors had not taken steps to determine framework adoption within their respective sectors. Despite the absence of efforts to determine framework adoption among the sectors, these agencies did take steps to encourage use of the framework. For example:

- HHS took steps to encourage use of the framework through the development of health industry resources, updating implementation guidance, mapping tools to the framework, and implementing best practices.
 - **Health industry cybersecurity practices.** HHS officials from the Office of the Assistant Secretary for Preparedness and Response stated that the department organized a joint government and private-sector cybersecurity working group, under which a task group developed the Health Industry Cybersecurity Practices.⁴⁴ This publication raised awareness and encouraged use of the framework because it introduced terms and concepts from the framework, and leveraged the framework to establish the recommended health industry practices.
 - **Implementation guidance.** According to HHS officials from the Office of the Assistant Secretary for Preparedness and Response,

⁴⁴HHS, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (Dec. 2018). Pursuant to the collaborative process required by the *Cybersecurity Act of 2015*, HHS created a task force to develop a document listing a common set of voluntary, consensus-based, industry-led guidelines, practices, methodologies, procedures, and processes for sector entities to improve their cybersecurity posture. Pub. L. No. 114-113, div. N, §405(d), 129 Stat. 2935, 2983 (2015).

another task group is in the process of updating the *Healthcare and Public Health Sector Cybersecurity Implementation Guide* and is expected to release it in February 2022.⁴⁵ The guide is intended to increase awareness and use of the framework and its related tools, and to guide implementation.

- **Mapped tools.** HHS officials from the Office of the Assistant Secretary for Preparedness and Response also stated that the agency has two tools mapped to the framework. Specifically, the aforementioned Healthcare Industry Cybersecurity Practices and the Office of the Assistant Secretary for Preparedness and Response's Risk Identification and Site Criticality toolkits are mapped to the framework. By mapping the toolkits to the framework, sector entities are more likely to be aware of and use the framework when implementing these tools.
- **Best practices.** In November 2021, HHS officials from the Office of the Assistant Secretary for Preparedness and Response stated that the agency plans to form a task group in 2022 to discuss how to obtain an understanding of framework use across the sector, pending resource availability. HHS officials also stated that they will be reviewing actions of other SRMAs to better assess framework adoption.
- Officials in Treasury's Office of Cybersecurity and Critical Infrastructure Protection stated that the financial services SCC developed a cybersecurity profile for the sector that is based on the framework. Among other things, the profile maps the framework's five core functions to existing regulations and guidance for financial services entities.

According to Treasury officials, the authors of the financial services sector's cybersecurity profile continue to engage with regulators to seek their recognition or adoption of the profile, even though adoption of the profile is not a requirement. Officials in Treasury's Office of Cybersecurity and Critical Infrastructure Protection stated that they believed that financial services entities focus on implementing what

⁴⁵The Risk Management Sub-Working Group was formally launched under the Critical Infrastructure Partnership Advisory Council under the Joint Healthcare and Public Health Cybersecurity Working Group in late 2015 to produce the *Healthcare Sector Cybersecurity Framework Implementation Guide*; Department of Health and Human Services, *Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide* (May 2016).

regulators require, so increasing the regulators' recognition and adoption of the framework could lead to greater use.

Despite Treasury's actions to promote the use of the framework, officials stated that they do not have the authority to compel sector members to respond to inquiries regarding adoption and, therefore, cannot track implementation of the framework. Although the lack of authority is challenging, 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.

- DHS's CISA took steps to encourage use of the framework through updates to NIST's cybersecurity implementation guides. CISA updated NIST's guides for the chemical; commercial facilities; critical manufacturing; dams; emergency services; and nuclear reactors, materials, and waste sectors. Updates to the guides included, among other things, a self-assessment tool to help organizations better understand the effectiveness of cybersecurity risk management efforts and additional explanation of the relationship between the framework's implementation tiers and profiles. These guides can be used to increase overall cybersecurity awareness and understanding of the framework.

Challenges Persist in Measuring Framework Adoption

Several SRMAs could not yet determine framework adoption, in part, due to various challenges that persist. We previously reported that SRMAs faced four challenges in determining framework adoption:⁴⁶

- Officials from DHS and 10 SCCs stated that entities may have limitations in committing necessary resources toward framework adoption.
- Officials from DHS, NIST, and five SCCs noted that entities may not have the necessary knowledge and skills to effectively implement the framework.
- Officials from eight SCCs cited that entities may face regulatory and industry requirements that inhibit adopting the framework.

⁴⁶[GAO-18-211](#).

- Officials from seven SCCs stated that entities may face other priorities that take precedence over cyber-related risk management or adopting the framework.

In addition to the aforementioned challenges, we previously noted that, given the voluntary nature of the framework, sector entities are not required to adopt it or to report on framework adoption efforts. Further, several SRMAs noted that these challenges continue to persist.

For example, officials from DHS identified that all of the previously reported challenges are still valid, and noted that the lack of subject matter expert resources is a particular concern among sectors. Officials from EPA cited that lack of cybersecurity knowledge among utilities continues to be a barrier to the sector's adoption of the framework. In addition, officials from Treasury identified that, unless financial regulators require adoption of the framework, sector entities are unlikely to implement it. Also, officials from HHS stated that other priorities, such as the COVID-19 response and managing response planning and recovery from an increase in ransomware attacks, have stretched resources thin and shifted the focus away from determining adoption of the framework.

We acknowledge that challenges to determining framework adoption exist and there can be different reasons why sector entities may not adopt the framework. Despite these challenges, as previously mentioned, several SRMAs have successfully determined framework adoption for their sectors or are taking steps to do so. For example, while committing resources toward framework adoption can be difficult, especially for smaller organizations, EPA has supported utilities by providing voluntary technical assessments that assess aspects of the framework that utilities have adopted. In addition, while the framework is voluntary, DOT and DHS's Transportation Security Administration managed to distribute a survey and gather responses from hundreds of entities, which the agencies may eventually be able to use to inform framework adoption across the sector.

It will be important for SRMAs to take additional steps or continue existing efforts to determine framework adoption within their respective sectors. Implementing our prior recommendations will help SRMAs gain a more comprehensive understanding of critical infrastructure sectors' adoption of the framework, which is essential to the success of protection efforts and determining where to focus limited resources on cyber risk mitigation.

Most SRMAs Have Not Identified Framework-Driven Improvements

SRMAs have made limited progress towards identifying improvements from sectors' framework use. As of November 2021, SRMAs for five of 16 critical infrastructure sectors had identified or taken initial steps to identify sector-wide improvements from use of the framework, as we previously recommended. The SRMAs for the remaining 11 sectors had not taken steps to identify sector-wide improvements. SRMAs noted several challenges that persist in measuring improvements, including the voluntary nature of the framework. NIST and DHS have developed initiatives that may help address some of the challenges.

SRMAs Have Made Limited Progress towards Identifying Improvements from Sectors' Framework Use

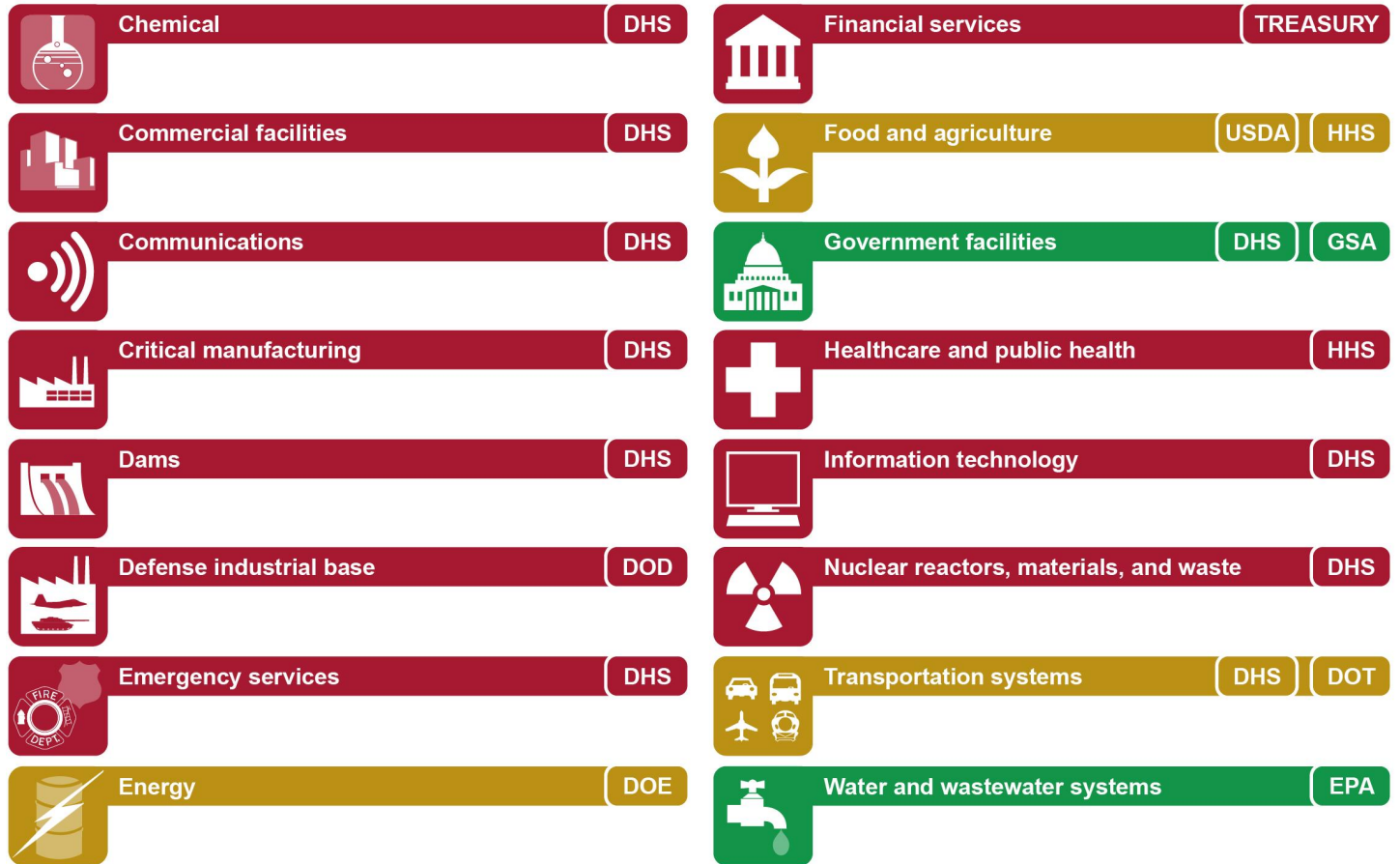
NIST Special Publication 800-55 guidance on performance measurement states that agency heads are responsible for actively demonstrating support for developing information security measures and facilitating performance improvements in their information security programs, which is to include a periodic analysis of data to determine lessons learned.⁴⁷ Additionally, the *National Infrastructure Protection Plan* directed SRMAs 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.

As of November 2021, SRMAs for five of the 16 critical infrastructure sectors had identified or taken initial steps to identify sector-wide improvements from use of the framework across their critical infrastructure sectors; the SRMAs for the 11 remaining sectors had not done so.⁴⁸ Figure 4 identifies the extent to which SRMAs had identified improvements for their respective sectors.

⁴⁷National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, SP 800-55, revision 1 (Gaithersburg, MD.: July 2008).

⁴⁸Although we identified that DHS, in coordination with its co-SRMA (GSA), collected and reported improvements for government facilities sector's use of the framework, DHS had not done so for eight sectors for which it is the sole SRMA.

Figure 4: Extent to Which Sector Risk Management Agencies Took Steps to Identify Improvements Resulting from Critical Infrastructure Sectors' Use of the National Institute of Standards and Technology's Cybersecurity Framework



- Have not taken steps to identify improvements
- Have taken steps to identify improvements
- Identified improvements

Sector risk management 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 agency data, Presidential Policy Directive-21, and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-22-105103

Note: Five of the nine SRMAs—DHS, DOT, GSA, HHS, and USDA—are co-SRMAs for one or more sectors that lead, facilitate, and support the security and resilience programs and associated activities of their designated critical infrastructure sectors. The food and agriculture (USDA and HHS), government facilities (DHS and GSA), and transportation systems (DHS and DOT) sectors have co-SRMAs.

SRMAs for Two Sectors Identified Improvements from Sectors' Use of the Framework

EPA identified improvements to the water and wastewater sector through its assessment initiative. Specifically, as mentioned previously, EPA launched a voluntary Technical Assistance Provider Initiative to provide cybersecurity assistance and create cybersecurity action plans for sector members. As part of the initiative, EPA's Office of Groundwater and Drinking Water developed metrics based on the framework, which it used to identify improvements resulting, in part, from use of the framework. As of October 2021, 146 utilities had completed both an initial assessment and two follow-up assessments. EPA captured the entities' progress in an assessment dashboard.

The data on improvements and progress made included growth that the entities have collectively made in each of the five functional areas of the NIST framework, as well as more specific cybersecurity activities, such as developing a list of cybersecurity best practices and conducting cybersecurity training. For example, during the initial assessment, entities reported implementing 38 percent of the activities that covered the five functional areas of the framework. After two follow-up assessments, the entities reported that they increased their implementation to 50 percent of the framework's cybersecurity activities. This represented an approximately 32 percent increase in the number of protections against cyber risks, and an overall improvement in the sector entities' cybersecurity from use of the framework.

In addition, GSA, in coordination with its co-SRMA, DHS's Federal Protective Service, identified improvements to the government facilities sector from the sector's use of the framework. Through Executive Order 13800, federal agencies that make up the government facilities sector were directed to provide a risk management report to OMB and DHS, where agencies were assessed against the five functional areas of the framework. After receiving risk management reports from sector organizations, OMB identified four areas where agencies needed to improve their cybersecurity programs in its May 2018 *Federal Cybersecurity Risk Determination Report and Action Plan*.

GSA, working with DHS and OMB, identified that agencies in the government facilities sector had taken several steps that resulted in improvements in these four areas. The following table lists examples of improvements that GSA, DHS, and OMB identified.

Table 1: Examples of Cybersecurity Improvements Resulting from the Government Facilities Sector’s Use of the National Institute of Standards and Technology’s Cybersecurity Framework

Cybersecurity program improvement areas	Examples of improvements identified by the General Services Administration (GSA), Department of Homeland Security (DHS), and Office of Management and Budget (OMB)
Cybersecurity threat awareness	Officials from GSA, DHS, and OMB stated that the Office of the Director of National Intelligence published the Cyber Threat Framework to increase cybersecurity threat awareness.
Information technology and cybersecurity standardization	DHS’s Continuous Diagnostics and Mitigation program helped address information technology and cybersecurity standardization by providing tools and services that collect and display standardized information to improve cybersecurity posture.
Security operations center consolidation	DHS’s Cybersecurity and Infrastructure Security Agency delivered core capability standards that are used to group services for future consolidation of security operation centers.
Agency accountability	OMB noted that the <i>Federal Information Security Modernization Act of 2014’s</i> Chief Information Officer Reporting Metrics helped to increase agency accountability by enabling OMB to measure agencies’ security capabilities against the National Institute of Standards and Technology framework.

Source: GAO analysis of agency data. | GAO-22-105103

Note: Officials from GSA and DHS that represent the government facilities sector noted that the framework’s core criteria has contributed to overall success, as it is used as the foundation for cybersecurity evaluative criteria and helps establish a common language for understanding and mitigating cyber risk for sector entities.

NIST officials and officials from the SRMAs responsible for the water and wastewater sector (EPA) and government facilities sector (GSA and DHS) shared their overall assessments of the extent to which the framework has been successful in protecting critical infrastructure from cyber threats. For example:

- NIST officials stated that the framework generally has helped organizations manage risk, identify assets, and respond to and recover from cyber incidents. NIST’s website also has a page on “Success Stories” that shows 11 examples of organizations using the framework to improve cybersecurity. The page includes examples of organizations in academia, critical infrastructure, workforce training, and other areas.
- Officials from EPA’s Office of Groundwater and Drinking Water noted that some subsets of their sector had been successful in using the framework to examine the comprehensiveness of their cybersecurity posture.

SRMAs for Three Sectors Took Initial Steps, but Had Not Yet Identified Improvements from Framework Use

DOE; DOT and its co-SRMA, DHS; and USDA and its co-SRMA, HHS, took initial steps to identify improvements across the energy, transportation systems, and food and agriculture sectors, but had not yet identified improvements for various reasons.

- As discussed earlier, DOE took initial steps to gather information from energy sector members regarding the framework and C2M2 implementation and impact. According to officials from the department's Office of Cybersecurity, Energy Security, and Emergency Response, of the 57 sector members who responded to questions about framework use, 12 members reported making improvements in foundational cybersecurity practices from use of the framework, seven reported making improvements in cyber incident response, and 11 reported making improvements in cyber risk management.

However, officials from DOE's Office of Cybersecurity, Energy Security, and Emergency Response believed that the agency needed to obtain additional information to identify sector-wide improvements. To facilitate this effort, DOE developed an action plan for additional steps the agency could take to measure improvements. For instance, the action plan identified steps DOE could take to gather broader feedback, such as through trade associations and sector owners and operators.

The action plan also identified potential quantitative and qualitative measurements to assess both implementation and results from either C2M2 or framework usage. Once established, these measurements may include, for example, the percentage of reporting organizations that improved cybersecurity practices based on C2M2 or framework assessment results, the percentage of organizations that repeated C2M2 or framework assessments over time, decisions organizations would like the C2M2 or framework to inform, and general feedback on experiences implementing the C2M2 or framework.

Officials from DOE's Office of Cybersecurity, Energy Security, and Emergency Response also noted that they are developing the National Rural Electric Cooperative Association's Rural Cooperative Cybersecurity Capabilities program to further improve cybersecurity for small- and mid-sized entities in the sector. The program is intended to enable sector entities to track and improve upon their

cybersecurity postures through self-assessments mapped to the framework. Once the department fully executes its action plan, DOE may be in the position to collect and report sector-wide improvements across its sector from framework use.

- As mentioned previously, DOT, in coordination with its co-SRMA DHS's Transportation Security Administration, sent out a survey to the transportation systems sector.⁴⁹ In addition to questions regarding adoption, the survey also asked questions regarding whether the framework provided value to the sector organization in five categories: (1) determining areas for improvement and developing plans to achieve improvements, (2) managing or fulfilling cybersecurity requirements, (3) understanding or managing cybersecurity risk, (4) reducing risk, and (5) prioritizing the relative importance of cybersecurity requirements or activities. An open-ended question was also included in the survey for entities to provide additional information about improvements from their use of the framework.

According to officials from DOT's Office of Intelligence, Security, and Emergency Response and DHS's Transportation Security Administration, the co-SRMAs are still analyzing the results of the survey and expect to complete its analysis by the end of March 2022. Once the agencies have collected and analyzed the responses, DOT and DHS may be in a position to collect and report improvements from use of the framework among entities within the transportation sector.

- As previously mentioned, USDA's Office of Homeland Security, in coordination with its co-SRMA, HHS's Food and Drug Administration, distributed a voluntary request for information to the food and agriculture sector.⁵⁰ The request for information asked sector members about improvements from use of the framework. Due to the low response rate, USDA and HHS could not collect and report improvements based on this request for information. As of October 2021, officials from USDA's Office of Homeland Security did not have additional plans for collecting and reporting improvements from the use of the framework; however, according to agency officials, the department is in the process of preparing a request for information for

⁴⁹DOT sent this voluntary survey to the transportation systems sector to gather data on framework use, in order to better tailor education and outreach activities to help mitigate the risk associated with cyber-related threats.

⁵⁰USDA and HHS are co-SRMAs for the food and agriculture sector.

the fiscal year 2021 Sector Annual Report and may repeat the request for framework data.

SRMAs for the Remaining 11 Sectors Did Not Identify Improvements from Framework Use

DHS, DOD, HHS, and Treasury, the SRMAs for the remaining 11 sectors,⁵¹ did not have efforts underway to identify sector-wide improvements from use of the framework.⁵² However, DOD, HHS, and Treasury took steps to encourage improvement in cybersecurity through use of the framework.

- DOD promoted its Defense Industrial Base Guide to Implementing the Cybersecurity Framework to encourage framework usage and provide resources to entities within the sector.⁵³ The department also reported that it used its Defense Industrial Base Cybersecurity Assessment Center process to assess contractor implementation of NIST SP 800-171, which the department mapped to the framework. However, the department had not yet determined whether the Defense Industrial Base Cybersecurity Assessment Center process or other approaches could be used to measure improvements across the sector. According to officials in DOD's Office of the Chief Information Officer, the department has focused on ensuring that appropriate cybersecurity requirements are mandated (through regulatory means) and are followed by entities within the sector.
- HHS officials noted that 192 health care and public health entities within the sector are participating in CISA's cybersecurity assessments and vulnerability scanning to identify cyber

⁵¹The remaining sectors are the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; financial services, health care and public health; information technology; and nuclear reactors, materials, and waste.

⁵²Although we identified that DHS, in coordination with its co-SRMA GSA, collected and reported improvements for government facilities sector's use of the framework, DHS had not done so for eight sectors for which it is the sole SRMA.

⁵³The Defense Industrial Base Guide to Implementing the Cybersecurity Framework supports DOD's responsibility to protect critical infrastructure by assisting organizations in implementing processes outlined in the framework. Organizations of all sizes and cybersecurity abilities can use the guide to manage their own levels of cybersecurity risk.

vulnerabilities and risks.⁵⁴ Aggregated assessment results showed the percentage of entities that had experienced certain vulnerabilities, such as running an unsupported operating system or risky service on an internet-accessible host. Officials from HHS's Office of the Assistant Secretary for Preparedness and Response noted that if the assessments were done periodically and entities were asked about their framework usage ahead of time, assessments could be used to determine improvements from framework use. HHS officials noted that they are having conversations with CISA about the possibility of incorporating questions regarding framework use into these assessments, but there is no time frame for when this might occur.

In addition, according to officials in HHS's Office of the Assistant Secretary for Preparedness and Response, the agency plans to update the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide.⁵⁵ Among other things, the agency intends to include a section on measurement and progress tracking by providing a method of comparing current cybersecurity profiles to target cybersecurity profiles that meet framework standards.⁵⁶ Officials from the Office of the Assistant Secretary for Preparedness and Response stated that, following these steps, HHS intends to consider how best to collect and report sector-wide improvements.

- Officials in Treasury's Office of Cybersecurity and Critical Infrastructure Protection stated that the financial services SCC developed a cybersecurity profile, which mapped the framework to other existing sector regulations and guidance.⁵⁷ According to officials from the agency's Office of Cybersecurity and Critical Infrastructure

⁵⁴CISA offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a cyber framework. These assessments are available at no cost to the organizations choosing to use them.

⁵⁵The Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide assists organizations in understanding and using the framework. The guide points organizations within the sector to the framework in order to improve critical infrastructure protection. It also includes an approach to implement the framework, including methods on how to track progress.

⁵⁶GAO, *Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*, [GAO-21-403](#) (Washington, D.C.: June 28, 2021).

⁵⁷The financial services SCC created the Financial Services Sector Cybersecurity Profile for financial institutions of all sizes to use for cyber risk management assessments and to provide a mechanism to comply with various regulatory frameworks and the NIST framework.

Protection, Treasury does not currently have the authority or processes to collect and report sector-wide improvements on a regular basis. It is important that Treasury implements our previous recommendation to collect and report sector-wide improvements to fully understand the value of the framework and to better protect critical infrastructure from cyber threats.

The SRMAs have not identified or taken initial steps to identify sector-wide improvements from use of the framework because of a lack of information. Specifically, when asked about the overall success from their sector's use of the framework, most SRMAs were unable to address the question.

We acknowledge that it can be difficult to identify an overall assessment of the framework's success, particularly when an SRMA is relying on sector entities to voluntarily provide relevant information. Nonetheless, the National Infrastructure Protection Plan directs SRMAs and their federal and nonfederal sector partners (including SCCs) to measure the effectiveness of efforts to secure critical infrastructure from cybersecurity threats.

Challenges Persist in Measuring Framework Improvements

The SRMAs reported five challenges in identifying sector-wide improvements related to their use of the framework: (1) the voluntary nature of the framework, (2) measuring the direct impact of using the framework, (3) developing precise measurements of improvement, (4) a lack of a centralized information sharing mechanism, and (5) a lack of cybersecurity culture and capacity. The first four of these challenges have persisted since our prior report, while the last one is a newly identified challenge.⁵⁸ The following table identifies the extent to which SRMAs identified the five challenges to measuring framework improvement.

⁵⁸[GAO-20-299](#).

Table 2: Extent to Which Sector Risk Management Agencies (SRMA) Identified Challenges to Measuring Framework Improvement

Challenges that SRMAs identified	Number of SRMAs that identified challenge	Examples
Challenge 1: Voluntary nature of the framework	8 of 9	Officials from the Departments of Defense, Energy (DOE), Homeland Security (DHS), Transportation (DOT), the Treasury (Treasury), Health and Human Services (HHS), and Agriculture (USDA); and the General Services Administration (GSA) stated that they could not get useful information on improvements resulting from use of the framework, as entities were not mandated to provide such information due to the voluntary nature of the framework. HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) officials also stated that there was a lack of incentives to report information due to the voluntary nature of the framework.
Challenge 2: Difficulty in measuring the direct impact of using the framework	5 of 9	Officials from DOE's Office of Cybersecurity, Energy Security, and Emergency Response stated that if a tool implemented according to framework standards prevented a cyber incident, the organization would not know if the credit goes to the framework or the tool. Officials from HHS's ASPR office and DOT's Office of Intelligence, Security, and Emergency Response also stated that it can be a challenge to link measures of success specifically to the framework.
Challenge 3: Developing precise measurements of improvement	3 of 9	Officials from HHS's ASPR noted that the different sizes and activities of organizations within their sector complicates the development of metrics and improvement parameters. Officials from USDA's Office of Homeland Security and DHS's Cybersecurity and Infrastructure Security Agency also acknowledged the challenge of developing precise measurements.
Challenge 4: No centralized information sharing mechanism	3 of 9	HHS's ASPR officials noted that the process for reporting improvements was a challenge overall due to the lack of a centralized information sharing mechanism.
Challenge 5: Lack of cybersecurity culture and capacity	3 of 9	GSA noted that the government facilities sector struggles with resource challenges and finds the framework overwhelming to implement in addition to other requirements. Officials from the Environmental Protection Agency's Office of Groundwater and Drinking Water stated that the sector itself is in the beginning of cybersecurity adoption. For instance, officials noted that many utilities have not yet integrated cybersecurity into their daily operations and maintenance, and thus had not created a cybersecurity culture. Therefore, many entities were unaware of National Institute of Standards and Technology's tools.

Source: GAO analysis of agency information. | GAO-22-105103

NIST and DHS Developed Initiatives That May Help Address Challenges

NIST and DHS have developed initiatives that may help SRMAs address some of the challenges in measuring improvements from sector entities' use of the framework. For example:

- **NIST's information security measurement program.** NIST launched its Measurements for Information Security program and

associated website in September 2020.⁵⁹ The website included links to tools, guidance, and other resources for organizations to better manage cybersecurity risk. With the establishment of this program and website, NIST can help address the challenge of developing precise measurements of improvement and measuring the direct impact of using the framework.

- **NIST's small business case studies.** In addition, NIST worked with the National Cybersecurity Alliance to publish five small business cybersecurity case studies. According to NIST officials, small businesses wanted examples of the framework applied to case studies in lieu of creating starter profiles that NIST was previously considering.⁶⁰ The case studies served as demonstrations of improvements from use of the framework. Specifically, the case studies include actions that are aligned to the framework, including lessons learned and resources that small businesses could use to handle common cybersecurity issues and realize improvements from use of the framework. For example, issues included automated teller machine skimming, keylogging, malware, and bank fraud; encryption and business security standards; social engineering and phishing; and data breaches. The case studies could potentially help address the challenge that SRMAs identified regarding the lack of use cases.
- **NIST's guidance on information security performance measurement.** NIST also made progress revising guidance for measuring cybersecurity effectiveness. Specifically, NIST issued a pre-draft public call⁶¹ for comments from September 2020 to December 2020 on Special Publication 800-55 Revision 2, *Performance Measurement Guide for Information Security*.⁶² NIST also plans to issue a draft of the guide that will be open for public comment in fiscal year 2022, but does not yet have a time frame for when the final publication will be released. This guide could help

⁵⁹National Institute of Standards and Technology, *Measurements for Information Security*, September 15, 2020, accessed Aug. 9, 2021, <https://www.nist.gov/cybersecurity-measurement>.

⁶⁰According to NIST, starter profiles 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.

⁶¹The pre-draft public call period allows the public to provide comments to the agency for consideration in preparing the final draft of the document.

⁶²NIST Special Publication 800-55 assists entities with the development and implementation of an information security measurement program. The goal is to provide a system that allows entities to connect better infrastructure protection to various information system and program security controls.

entities that are struggling to develop measurements related to the framework.

Moreover, we previously reported that DHS had various initiatives that could help to address challenges in collecting and reporting sector-wide improvements. For example:

- **DHS's road map for small and midsize businesses.** DHS created a small and midsize business road map to serve as a guide to cybersecurity enhancement for all critical infrastructure sectors in 2018. Included in the road map was the department's cybersecurity information sharing and collaboration program and secure information sharing portal. The information sharing portal could be used by entities to share cybersecurity strategies and insights, serving as a potential solution to the centralized information sharing mechanism challenge by creating an accessible space for all entities to share and review cybersecurity information.
- **DHS's information network for sharing best practices.** Officials from DHS's Stakeholder and Engagement and Cyber Infrastructure Resilience division also noted that its Homeland Security Information Network could serve as a tool for entities to share and report on best practices, including sector-wide improvements and lessons learned from using the framework.⁶³ By providing another environment for entities to discuss and learn cybersecurity practices, this could help address the challenge that SRMAs identified regarding centralized information sharing.

SRMAs Had Mixed Views of NIST and DHS Initiatives

SRMAs provided mixed views on using the NIST and DHS initiatives to address the challenges in measuring successes from framework use within their sectors.

- DOE's Office of Cybersecurity, Energy Security, and Emergency Response officials noted that the initiatives did not provide specific approaches to collect information on framework use or improvements. For example, DOE officials stated they met with NIST and were informed that the Measurements for Information Security Program

⁶³The Homeland Security Information Network serves as a system for government and its private sector partners to share sensitive information with each other, on topics such as operations, security, and incident response.

consisted of guidelines and tools for organizations to manage cybersecurity risk, instead of measuring framework adoption.

Officials also stated that the Roadmap for Improving Critical Infrastructure Cybersecurity was an update on next steps for the framework, instead of a method to measure adoption and improvements. Further, although DOE officials identified the DHS Homeland Security Information Network as a potential way to collect information from private sector partners, they did not find a specific mechanism to report on framework adoption or improvements within the tool. Based off these evaluations of the initiatives, DOE officials stated that they were not aware of any specific tools, guidelines, or initiatives from these programs that were developed to measure usage or improvements from use of the framework on an individual or sector-wide scale.

- Officials from DOT's Office of Intelligence, Security, and Emergency Response noted that NIST's Measurements for Information Security Program was not available at the time the initial draft of the transportation systems survey was shared with sector leads and stakeholders. The officials also stated that because DHS is a co-SRMA with DOT, the agency has always had inherent opportunities to leverage existing partnerships to further its initiatives. The officials added that they are currently evaluating the input received from survey stakeholders prior to reporting any information on lessons learned or improvements, and will determine whether and how to leverage DHS's Homeland Security Information Network for such reporting.
- Officials from EPA's Office of Groundwater and Drinking Water noted that the NIST and DHS initiatives have limitations. Specifically, they stated the initiatives do not address all of the challenges identified by SRMAs, including the lack of authority to require sector entities to participate in their collection of information on improvements from use of the framework and no requirements for sector entities to provide improvements from use of the framework.
- Officials from HHS's Office of the Assistant Secretary for Preparedness and Response noted that the agency plans to reference and recommend the initiatives in the latest update of its framework implementation guide. The officials also stated that, after the publication of their guide, they plan to restart their Risk Management working group to find ways to use the initiatives to measure sector improvements in the future.

- Officials from Treasury's Office of Cybersecurity and Critical Infrastructure Protection stated that they assessed the relevance of the NIST and DHS initiatives to the financial services sector and believe awareness of each initiative may benefit the sector generally. Treasury also noted that the agency regularly promotes the use of the initiatives and similar guidelines to the financial sector.

However, Treasury has not used these initiatives to collect and report on sector-wide improvements from use of the framework. Treasury officials stated that the agency lacks the authority to compel financial institutions to respond to regular inquiries regarding the sector's use of the framework, or resulting improvements.

We acknowledge the limitations of the NIST and DHS initiatives, and understand that additional actions may be necessary to overcome the various challenges to measuring improvements. Nevertheless, it is important for the remaining seven SRMAs to implement our previous recommendations to collect and report sector-wide improvements to fully understand the value of the framework and to better protect their critical infrastructure from cyber threats.

Agency Comments

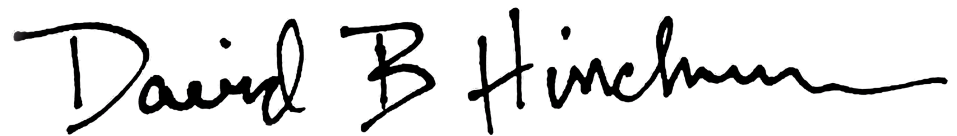
We requested comments on a draft of this report from the Department of Commerce, DOD, DOE, DHS, DOT, EPA, GSA, HHS, Treasury, and USDA. We received technical comments from the Department of Commerce's NIST, DOE, DHS, DOT, and USDA, which we incorporated as appropriate. DOD, EPA, GSA, HHS, and Treasury stated that they had no comments on the draft report.

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

Letter

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 (214) 777-5719 or hinchmand@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 I.

A handwritten signature in black ink that reads "David B Hinchman". The signature is written in a cursive style with a long, sweeping underline.

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Josh Leiling (Assistant Director), Kendrick M. Johnson (Analyst-In-Charge), Christopher Businsky, Vijay D'Souza, Rebecca Eyer, Franklin Jackson, Evan Kreiensieck, Ceara Lance, and Ibrahim Suleman 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/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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



Please Print on Recycled Paper.