



February 2018

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Are
Essential for
Assessing
Cybersecurity
Framework Adoption

Accessible Version

GAO Highlights

Highlights of [GAO-18-211](#), a report to congressional committees

Why GAO Did This Study

Our nation's critical infrastructure includes the public and private systems and assets vital to national security, economic stability, and public health and safety. Federal policy identifies 16 critical infrastructure sectors, including the financial services, energy, transportation, and communications sectors. To better address cyber-related risks to critical infrastructure, in 2014, NIST developed, as called for by federal law and policy, *the Framework for Improving Critical Infrastructure Cybersecurity*, a voluntary framework of cybersecurity standards and procedures for industry to adopt.

The Cybersecurity Enhancement Act of 2014 included provisions for GAO to review aspects of the cybersecurity standards and procedures in the framework developed by NIST. GAO's objective was to assess what is known about the extent to which critical infrastructure sectors have adopted the framework. To do so, GAO analyzed documentation, such as sector-specific guidance and tools to facilitate implementation, and interviewed relevant federal and nonfederal officials from the 16 critical infrastructure sectors.

What GAO Recommends

GAO is making nine recommendations that methods be developed for determining framework adoption by the sector-specific agencies across their respective sectors, in consultation with their respective sector partner(s), such as the sector coordinating councils, the Department of Homeland Security, and NIST, as appropriate. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed.

View [GAO-18-211](#). For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

February 2018

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption

What GAO Found

Most of the 16 critical infrastructure sectors took action to facilitate adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* by entities within their sectors. Federal policy directs nine federal lead agencies—referred to as sector-specific agencies (SSA)—in consultation with the Department of Homeland Security and other agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

In response, guidance for 12 of the 16 sectors for implementing the cybersecurity framework was developed. In addition, nonfederal led sector coordinating councils took additional steps to facilitate framework adoption. For example, 3 sectors that developed implementation guidance encouraged the alignment of the framework with existing cybersecurity guidelines used within their respective sectors.

Nevertheless, officials from the Department of Homeland Security, NIST, SSAs, and the sector coordinating councils identified four challenges to cybersecurity framework adoption, as reported by entities within their respective sectors. Specifically, some entities

- May be limited in their ability to commit necessary resources towards framework adoption.
- May not have the necessary knowledge and skills to effectively implement the framework.
- May face regulatory, industry, and other requirements that inhibit adopting the framework.
- May face other priorities that take precedence over conducting cyber-related risk management or adopting the framework.

Further, the nation's plan for national critical infrastructure protection efforts states that federal and nonfederal sector partners (including SSAs) are to measure the effectiveness of risk management goals by identifying high-level outcomes and progress made toward national goals and priorities, including securing critical infrastructure against cyber threats. However, none of the SSAs had measured the cybersecurity framework's implementation by entities within their respective sectors. None of the 16 coordinating councils reported having qualitative or quantitative measures of framework adoption because they generally do not collect specific information from entities about critical infrastructure protection activities. SSA officials also stated that the voluntary nature and other factors are impediments to collecting such information. While other entities, including a trade association and universities, had attempted to determine the use of the framework within certain sectors; none of those efforts yielded results that would articulate a sector-wide level of framework adoption.

Until SSAs have a more comprehensive understanding of the use of the cybersecurity framework by entities within the critical infrastructure sectors, they will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation.

Contents

Letter	1
Background	4
Most Sectors Have Taken Steps to Facilitate Use of the Framework but Extent of Adoption Is Unknown	11
Conclusions	22
Recommendations for Executive Action	22
Agency Comments and Our Evaluation	24
Appendix I: Objectives, Scope and Methodology	27
Appendix II: Comments from the Department of Agriculture	30
Appendix III: Comments from Department of Defense	32
Appendix IV: Comments from the Department of Energy	34
Appendix V: Comments from the Department of Health and Human Services	36
Appendix VI: Comments from the Department of Homeland Security	38
Appendix VII: Comments from the Department of the Treasury	41
Appendix VIII: Comments from the Environmental Protection Agency	43
Appendix IX: Comments from the General Services Administration	45
Appendix X: GAO Contact and Staff Acknowledgments	46
GAO Contact	46
Staff Acknowledgments	46
Tables	
Table 1: Critical Infrastructure Cyber Community Voluntary Program (C ³ VP) Cybersecurity Framework Promotion Efforts reported since October 2015	10
Table 2: Critical Infrastructure Sectors and Associated Sector- Specific Agency and Sector Coordinating Councils	27

Figures

Figure 1: Sixteen Critical Infrastructure Sectors and the Related Sector-Specific Agencies	6
Figure 2: Critical Infrastructure Sectors that Developed Cybersecurity Framework Implementation Guidance ^a	13

Abbreviations

C ³ VP	Critical Infrastructure Cyber Community Voluntary Program
CS&C	Office of Cybersecurity and Communications
DHS	Department of Homeland Security
NIST	National Institute of Standards and Technology
SCC	sector coordinating council
SSA	sector-specific agency

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



February 15, 2018

The Honorable John Thune
Chairman
The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Lamar Smith
Chairman
The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

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

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

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.

identifiable information. We continued to identify the protection of critical cyber infrastructure as a high-risk area in our February 2017 High-Risk update report.²

To better address these cyber-related risks, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, on February 12, 2013.³ This order aimed to enhance the security and resilience of the nation's critical infrastructure and to 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)⁴ to lead the development of a voluntary, risk-based cybersecurity framework that would comprise a set of industry standards and best practices to help organizations manage cybersecurity risks. In response, NIST issued the *Framework for Critical Infrastructure Cybersecurity* (the framework) in February 2014 with the intention of helping organizations apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.⁵ In addition, the Cybersecurity Enhancement Act of 2014, enacted in December 2014, authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure.⁶

The Cybersecurity Enhancement Act of 2014 also included a provision for us to review, in a series of reports, various aspects of the cybersecurity standards and procedures developed by NIST. Our objective for this report was to assess what is known about the extent to which critical

²GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: Feb. 15, 2017).

³Exec. Order No. 13636, 78 Fed Reg. 11739 (Feb. 19, 2013).

⁴The National Institute of Standards and Technology (NIST) is a component within the Department of Commerce. NIST's 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 our quality of life.

⁵National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014).

⁶Pub. L. No. 113-274 (Dec. 18, 2014).

infrastructure sectors have adopted the *Framework for Improving Critical Infrastructure Cybersecurity*.

To address the objective, we analyzed documentation and evidence that discussed actions carried out by organizations with lead roles in critical infrastructure protection efforts to promote the framework. These organizations included federal lead agencies, referred to as sector-specific agencies (SSA),⁷ and the sector coordinating councils (SCC) that are made up of nonfederal members and are to serve as the voice of each sector and principal entry point for the government to collaborate with each sector. We included SSAs and SCCs representing all of the critical infrastructure sectors in our review.

We also analyzed documentation from, and interviewed officials of, NIST and the Department of Homeland Security (DHS). These included officials from DHS's Office of Cybersecurity and Communications (CS&C), regarding their activities to promote awareness and use of the NIST cybersecurity framework. In addition, we examined what actions SSAs had planned or taken that would result in a qualitative or quantitative assessment of the level of framework adoption by entities within each critical infrastructure sector. Further, we interviewed officials from the relevant federal agencies, including NIST, DHS, and the SSAs and participating SCCs, to determine the adoption of the framework within the private sector and to determine the definition of the term "adoption."⁸ Appendix I discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from March 2017 to February 2018 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

⁷The sector specific agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and Treasury; the Environmental Protection Agency; and the General Services Administration.

⁸In a December 2013 memo, NIST broadly defined "adoption" as any use of the cybersecurity framework as a key part of an organization's systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities. However, this definition was not included in the *Framework for Improving Critical Infrastructure Cybersecurity*, issued in February 2014.

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

Threats to the systems supporting critical infrastructures are evolving and growing. These cyber-based assets are susceptible to unintentional and intentional threats. 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 infrastructures, since the sectors are often interdependent.

Intentional, or adversarial, threats can involve targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These adversaries vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include seeking monetary gain or pursuing an economic, political, or military advantage.

Cyber adversaries make use of various techniques, tactics, and practices—or exploits—to adversely affect an organization's computers, software, or networks, or to intercept or steal valuable or sensitive information. These exploits are carried out through various conduits, including websites, e-mail, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program.

Federal Policy Assigns Responsibility for the Cyber-related Protection of Critical Infrastructure

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

Presidential Policy Directive 21 establishes SSAs as the federal entities responsible for providing institutional knowledge and specialized expertise. SSAs are also to lead, facilitate, or support the security and resilience programs and associated activities of their designated critical infrastructure sectors in the all-hazards environment.⁹

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

⁹The White House, Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 2013). The term "all hazards" is defined by the directive as a threat or an incident, natural or manmade, which warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. "All hazards" includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

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



Sector-specific agency

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

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-18-211

In addition, the directive required DHS to update the National Infrastructure Protection Plan (originally developed in 2006, to include the

cybersecurity of the nation's critical infrastructure).¹⁰ DHS, in response, updated the National Infrastructure Protection Plan in December 2013 in collaboration with public- and private-sector owners and operators and federal and nonfederal government representatives, including SSAs, from the critical infrastructure community. According to the 2013 plan, SSAs are to work with their private-sector counterparts to understand cyber risk and are to evaluate the effectiveness of risk management efforts by developing metrics for both direct and indirect indicator measurements.

To work with the government, SCCs were formed to serve as the voice of each sector and principal entry point for the government to collaborate with each sector. SCCs are self-organized and self-governed 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 SCCs coordinate and collaborate with the SSAs in a voluntary fashion regarding issues within their respective sectors.

Federal Law and Policy Established Responsibility for Developing and Promoting a Cybersecurity Framework

In February 2013, Executive Order 13636 outlined an action plan for improving security for critical cyber infrastructure.¹¹ This included, among other things, direction to NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of standards, procedures, and processes. The executive order also directed SSAs, in consultation with DHS and other interested agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

Further, in December 2014, the Cybersecurity Enhancement Act of 2014 established requirements that are consistent with the executive order

¹⁰Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013). The plan, among other things, describes how the involved business and government entities should use risk management principles to prioritize their cybersecurity activities within and across sectors. The updated plan defines the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.

¹¹Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

regarding NIST's development of a cybersecurity framework.¹² According to this law, NIST's responsibilities in supporting the ongoing development of the cybersecurity framework include, among other things, identifying an approach that is flexible, repeatable, performance-based, and cost-effective.

In response to Executive Order 13636, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014. The framework proposes a risk-based approach to managing cybersecurity risk and is composed of three parts: the framework core, the framework profile, and the framework implementation tiers. The framework core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, which is to provide guidance for developing individual organization profiles. The framework core consists of five concurrent and continuous functions—identify, protect, detect, respond, and recover. When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

In addition, the framework core is to provide guidance for developing individual organization profiles. Through the use of the profiles, the framework is intended to help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources.

The tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. The tiers characterize an organization's practices over a range and are: partial (tier 1); risk informed (tier 2), repeatable (tier 3), and adaptive (tier 4). These tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

In January 2017, NIST released a draft of revisions to the 2014 framework (version 1.1) for public comment. The revisions to the framework included the addition of a section on self-assessing and demonstrating cybersecurity through measurements, as well as further explanation of the relationship between implementation tiers and risk profiles. According to NIST, after reviewing public comments on draft version 1.1, NIST published the second draft of the proposed update to

¹²Pub. L. No. 113-274 (Dec. 18, 2014).

the framework on December 5, 2017. According to NIST, this draft aims to clarify, refine, and enhance the framework.¹³

Further, in May 2017, the President issued Executive Order 13800, which required each federal agency to use the cybersecurity framework, or any successor document, to manage the agency's cybersecurity risk.¹⁴ In response to the order, NIST released *Draft Interagency Report 8170* in May 2017.¹⁵ The report is intended to provide guidance on how agencies can use the framework to complement existing risk management practices and improve their cybersecurity risk management programs.

Accordingly, the report identifies eight areas, based on implementation in nonfederal entities, which are ways that federal agencies can use the framework to address common responsibilities and support a more robust and mature agencywide risk management program. These eight areas are:

1. Integrate Enterprise and Cybersecurity Risk Management
2. Manage Cybersecurity Requirements
3. Integrate and Align Cybersecurity and Acquisition Processes
4. Evaluate Organizational Cybersecurity
5. Manage the Cybersecurity Program
6. Maintain a Comprehensive Understanding of Cybersecurity Risk
7. Report Cybersecurity Risks
8. Inform the Tailoring Process

Federal Entities Have Promoted Awareness of the Cybersecurity Framework

As we previously reported, although not specifically required by Executive Order 13636 or the Cybersecurity Enhancement Act of 2014, NIST has

¹³National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 Draft 2 (Gaithersburg, MD: December 5, 2017).

¹⁴Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

¹⁵National Institute of Standards and Technology, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, DRAFT NISTIR 8170 (Gaithersburg, MD: May 2017).

undertaken efforts to promote the cybersecurity framework.¹⁶ Specifically, NIST maintains a website of publicly available resources that could help facilitate an entity’s adoption of the framework. These resources include guidance for implementing the framework, tools that incorporate the framework, and case studies of entities implementing the framework.¹⁷ On the website, NIST also provides details regarding upcoming events where its officials are to provide information and perspectives about the framework. In addition, the website lists past speaking events, links to the event webpages, and, in some cases, the related presentation slides.

We also reported in December 2015 that DHS had launched the Critical Infrastructure Cyber Community Voluntary Program (C³VP) in February 2014, in accordance with Executive Order 13636. The C³VP mission is to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the framework.¹⁸ Since our 2015 report, C³VP reported that it has continued to increase outreach and awareness of the framework, create and disseminate framework implementation guidance, and provide resources to assist in implementing the framework on the C³VP website.¹⁹ Table 1 summarizes promotion activities reported by C³VP.

Table 1: Critical Infrastructure Cyber Community Voluntary Program (C³VP) Cybersecurity Framework Promotion Efforts reported since October 2015

Effort	Reported Action
Webinars	Conducted 10 webinars reaching over 1,600 stakeholders. For example, in September 2017, C ³ VP hosted a webinar focusing on framework use among small and mid-size businesses.
Industry briefings	Hosted 165 industry briefings across the 16 critical infrastructure sectors.
Small and Midsize Businesses toolkit	Created a toolkit which has been downloaded from its website more than 7,700 times. The toolkit contains a number of resources designed to help businesses recognize and address their cybersecurity risks.

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

¹⁷NIST’s listing of publicly available Cybersecurity Framework industry resources includes, but is not limited to: approaches, methodologies, implementation guides, mappings to the framework, case studies, educational materials, Internet resource centers (e.g., blogs, document stores), example profiles, and other framework document templates.

¹⁸Resources provided by C³VP can be found at: <https://www.us-cert.gov/ccubedvp>.

¹⁹GAO-16-152.

Effort	Reported Action
Regional workshop	Held a regional workshop in June 2016 with over 100 attendees. The workshop included presentations from NIST on the cybersecurity framework, panel discussions on best practices and lessons learned among organizations that have implemented the framework, and best practices and framework use cases among small and midsize businesses.
GovDelivery bulletin	Launched a monthly email bulletin in December 2015 that promotes framework implementation guidance as well as upcoming events and cybersecurity resources.
Handouts	Created a handout to distribute at briefings and workshops containing information about C ³ VP, the framework core functions, and DHS resources corresponding to each function.

Source: Department of Homeland Security documentation. | GAO-18-211

In addition, in the same report, we stated that SSAs promoted and supported adoption of the cybersecurity framework in the critical infrastructure sectors.²⁰ SSAs for all 16 sectors reported that they distributed and promoted the framework to entities within their sectors. Officials representing all of the SSAs stated that they have continued to conduct framework promotional activities, such as speeches during sector meetings on framework implementation and various cybersecurity topics, working groups, and using C³VP and NIST resources. In addition, since October 2015, all of the SSAs have either hosted or participated in conferences, webinars, and workshops aimed at promoting awareness and understanding of the framework.

Most Sectors Have Taken Steps to Facilitate Use of the Framework but Extent of Adoption Is Unknown

Most sectors took actions to facilitate adoption of the NIST cybersecurity framework by entities within their respective sectors. However, sector leaders have identified a number of challenges that entities within their respective critical infrastructure sectors face when attempting to implement the framework. In addition, most sectors do not have a comprehensive understanding of framework adoption by their respective critical infrastructure entities, due in large part to a lack of available data regarding adoption across the respective sectors.

²⁰ [GAO-16-152](#).

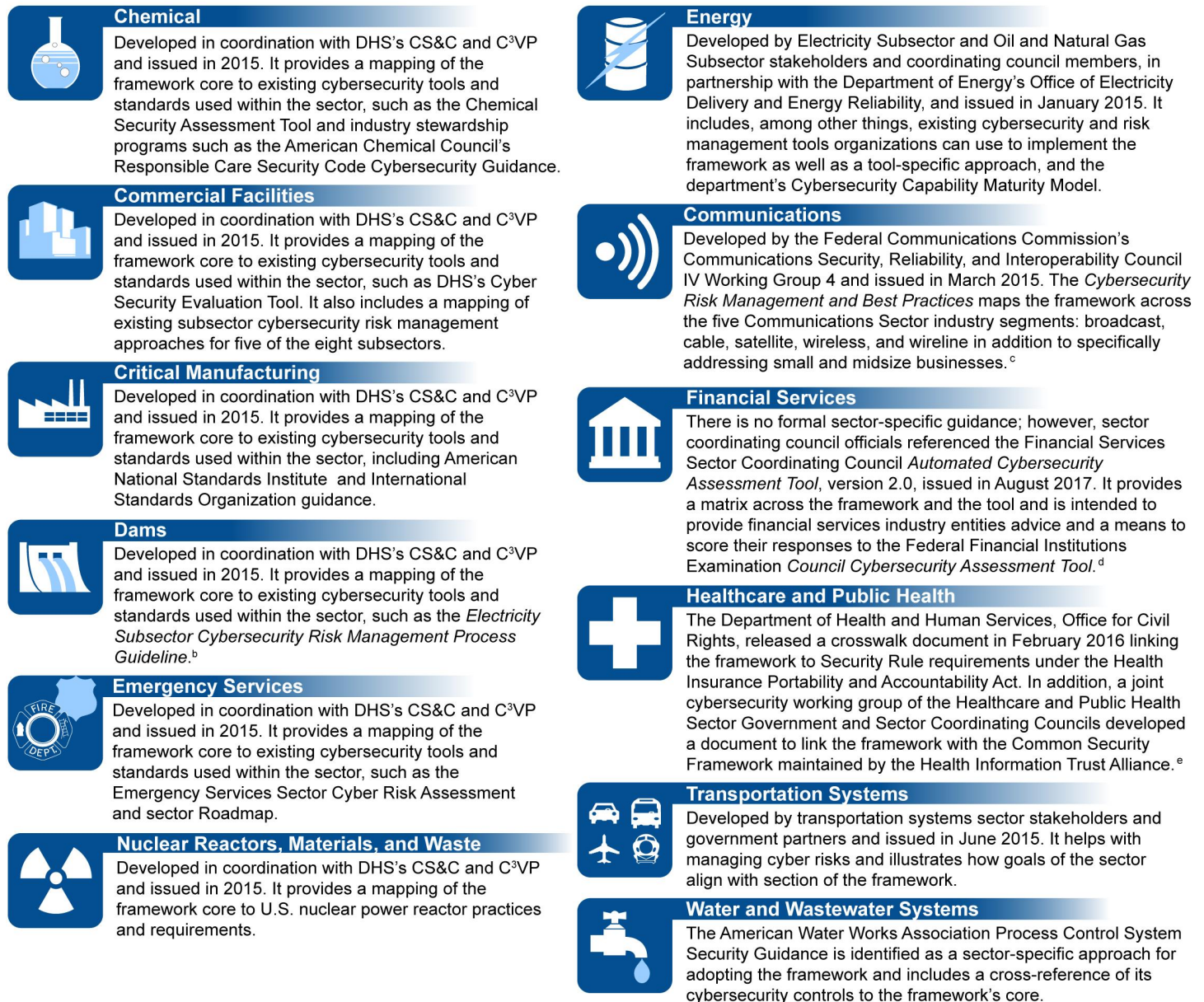
Most Sectors Have Taken Steps to Support Implementation, but Reported Challenges in Entities' Efforts to Adopt the Framework

Executive Order 13636 directs SSAs, in consultation with DHS and other agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments. Of the 16 critical infrastructure sectors, 12 have developed implementation guidance that addresses how entities within their respective sectors can adopt the framework. Of these, 6 sectors worked with DHS to develop the framework implementation guidance. In addition, 6 sectors developed implementation guidance in conjunction with their respective SSAs and with non-federal sector entities, including sector-related trade associations.

The remaining 4 sectors have not developed implementation guidance. Of these, 3 reported that they have engaged with relevant entities, through working groups and other sector meetings, to determine the type of cybersecurity guidance that would be most beneficial for their respective membership. The other sector stated that they have elected not to develop any guidance for entities within their sector.

Figure 2 identifies each of the 12 sectors that developed cybersecurity framework implementation guidance.

Figure 2: Critical Infrastructure Sectors that Developed Cybersecurity Framework Implementation Guidance^a



Source: GAO analysis of implementation guidance and sector-related documentation; Art Explosion (clip art). | GAO-18-211

^aThe implementation guides referenced in the table, as well as a variety of other resources to help support adoption of the framework, are available on NIST's website: <https://www.nist.gov/cyberframework/industry-resources>.

^bDepartment of Energy, Office of Electricity Delivery and Energy Reliability, Cybersecurity Risk Management Process (RMP) Guideline – Final (May 2012).

^cThe Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (March 2015).

^dFederal Financial Institutions Examination Council, *Cybersecurity Assessment Tool* (May 2017).

^eHealth and Human Services Office for Civil Rights, *Health Insurance Portability and Accountability Act Security Rule Crosswalk to NIST Cybersecurity Framework* (Feb. 2016).

In addition to developing implementation guidance, three sectors reported taking additional steps to facilitate adoption of the framework within their respective sectors. Specifically, these sectors encourage the alignment of the NIST cybersecurity framework with existing cybersecurity guidelines currently in use by entities within their sectors.

- The Electricity Subsector and Oil and Natural Gas Subsector stakeholders and coordinating council members, in partnership with the Department of Energy's Office of Electricity, developed guidance for implementing the framework that includes a seven-step approach.²¹ This approach is designed to be used along with any cybersecurity standard, energy-sector specific tool, or commercial tool for managing cybersecurity risk to facilitate framework implementation. In the same document, the department evaluated its existing Cybersecurity Capability Maturity Model,²² which focuses on the implementation and management of cybersecurity practices in the environments in which they operate, in order to align the model to the framework. The Cybersecurity Capability Maturity Model is intended to be descriptive, rather than prescriptive, guidance that can be used by organizations of various types and sizes to strengthen their cybersecurity capabilities. According to the alignment document, the approach is designed for organizations' use with a self-evaluation methodology and toolkit to measure and improve their cybersecurity programs and serve as an example for how to implement the framework.
- The Financial Services sector developed a cybersecurity assessment tool that is intended to aid sector entities in identifying their risks, assess their cybersecurity preparedness, and help inform their risk management strategies. In addition, according to Financial Services SCC officials, the coordinating council is in the process of developing a draft cybersecurity "profile" in response to being a sector with a complex regulatory and cybersecurity environment. The draft profile is

²¹Department of Energy, *Energy Sector Cybersecurity Framework Implementation Plan* (Jan. 2015).

²²Department of Energy, *Cybersecurity Capability Maturity Model*, Version 1.1 (Feb. 2014).

intended to help enhance the collective understanding of the state of cybersecurity for both regulators and industry within the Financial Services sector. In developing the draft profile, the Financial Services SCC mapped the most significant sector-related regulations to the framework. For example, according to sector documents, the framework's "Identify" function regarding "Risk Management Strategy" mapped to nine different regulatory requirements. The draft profile also proposed adding two functions of priority for the Financial Services sector: Governance and Supply Chain/Dependency Management. The proposed additions are meant to provide a greater level of detail as well as to manage dependencies in the financial services sector.²³

- According to sector officials, the Healthcare and Public Health sector encourages the alignment of the NIST cybersecurity framework with existing cybersecurity guidelines currently in use within its respective sector. For example, the sector aligned the Health Information Trust Alliance Framework²⁴ to the cybersecurity framework. This mapping fully incorporated the framework and provided for 135 individual security controls and 14 individual privacy controls that can be implemented by healthcare providers. Department officials stated that the alignment of the framework to the Health Information Trust Alliance Framework allows organizations to demonstrate compliance with NIST through their implementation of the pre-existing Health Information Trust Alliance Framework.

Officials Reported Potential Challenges in Adopting the Framework

While most sectors are taking steps to facilitate adoption of the cybersecurity framework, officials from DHS C³VP, NIST, SSAs, and

²³According to the profile, the Governance function is to provide, among other things, the establishment of appropriate cybersecurity governance in Financial Services organization, the ability to implement robust risk management practices, and the ability to give appropriate attention to the segregation of duties between security implementation, oversight, and audit. The profile also states that the Supply Chain/Dependency Management function is to provide management of risks from internal and external dependencies, the establishment and maintenance of a robust business environment, and the assurance of resilience of the enterprise, Financial Services sector, and the entire critical infrastructure.

²⁴Health Information Trust Alliance Framework, *Common Security Framework*, Version 7 (Jan. 31, 2015). The HITRUST *Common Security Framework* has since been updated to Version 9 (Sep. 10, 2017).

SCCs identified four challenges to framework adoption, as reported by entities within their respective critical infrastructure sectors.

- **Entities may be limited in their ability to commit necessary resources toward framework adoption.** Officials from DHS and 10 SCCs cited the lack of resources as a challenge to greater implementation of the framework. In this regard, an entity's size can affect the amount of resources available to assist in adopting the framework. Specifically, DHS officials and officials from 4 sectors stated that large entities within sectors generally have more people and funds available that can be used to implement the framework, while small and medium-size entities do not always have access to the same degree of resources. Officials from 2 sectors indicated that cybersecurity may be managed by individuals that have multiple responsibilities, and organizations may not be able to dedicate staff to implement the framework. However, with regard to this challenge, NIST officials stated that certain entities may misunderstand the level of resources needed to customize and apply the framework. For example, NIST stated that certain entities have reported adopting the framework for their organizations in as little as 6 hours.
- **Entities may not have the necessary knowledge and skills to effectively implement the framework.** Officials from DHS, NIST, and five SCCs cited the lack of the necessary knowledge and skills to apply the framework to entities' operations as a potential challenge to framework adoption. Officials from one sector stated that potential framework users may require more knowledge on both cybersecurity risks and the utility of implementing the framework. DHS and NIST officials added that some small organizations within sectors have difficulty understanding and using the framework, and that some sectors are often less organized and are still "emerging in maturity."
- **Entities may face regulatory, industry, and other requirements that inhibit adopting the framework.** Officials from eight SCCs cited the existence of other regulatory and industry requirements as a challenge to framework adoption. Specifically, officials from five sectors stated that highly regulated sectors already have federal, state, and local regulatory guidance, requirements, and competing security frameworks in place. SCC officials from another sector stated that these existing requirements may overlap with recommendations of the cybersecurity framework. NIST officials added that regulated sectors that face heavy penalties and close oversight, as well as compliance approaches that pre-date the framework, are less likely to use it. Additionally, SCC officials from one sector indicated that, while other requirements may ultimately link to the framework, those

requirements often contain greater levels of specificity for their relevant industries. Further, officials from another sector stated that executive orders, and other NIST publications, include guidance that proposes alternative approaches to the framework.

- **Entities may face other priorities that take precedence over conducting cyber-related risk management or adopting the framework.** Officials from seven SCCs stated that other factors may take precedence for entities over adopting the framework or performing cyber-related risk management. For example, SCC officials from two sectors stated that certain entities within their sector may prioritize physical security, protection against product contamination, prevention of insider threats, or maintaining continuity of operations during natural disasters as being of greater concern to their core business than addressing cybersecurity risks. SCC officials from another sector stated that, for some entities, just maintaining day-to-day business operations are of greater concern to owners than implementing the framework. Also, SCC officials from one sector stated that certain entities within sectors have not determined if using the framework is necessary. Additionally, SCC officials from a different sector stated that smaller entities within the sectors struggle with the idea that they may be a target for a cybersecurity attack and, therefore, have little incentive to address cybersecurity issues or use the framework to assist them in mitigating cyber-related risk.

In addition to the aforementioned challenges, given the voluntary nature of the framework, sectors' entities are not required to adopt it or to report on framework adoption efforts if they decide to adopt it. Moreover, due to the voluntary nature of the framework and concerns voiced by participants in the development of the framework about making it appear regulatory, NIST determined that defining "adoption" within the framework was not appropriate. Specifically, NIST officials stated that defining "adoption" in the framework could hinder customization for sectors and organizations implementing the framework. NIST officials further stated that sectors and organizations implement and adopt the framework according to their needs, which vary considerably.

Public-Private Sector Partners Have Made Limited Efforts to Determine Framework Adoption by Sector Entities

Once guidance is developed, best practices recommend that entities take steps to evaluate progress toward the achievement of goals—in this case, to implement or adopt the cybersecurity framework. Specifically, the National Infrastructure Protection Plan directs SSAs and their federal and

nonfederal sector partners (including SCCs) to measure the effectiveness of risk management goals by identifying high-level outcomes to facilitate the evaluation of progress toward national goals and priorities, including securing critical infrastructure against cyber threats.

Further, best practices recommend entities take steps to evaluate the performance of actions taken, in this case, the extent to which the cybersecurity framework has been implemented. Specifically, *Standards for Internal Control in the Federal Government* sets internal control standards for federal entities.²⁵ Those standards state that internal control monitoring should occur and that the quality of performance over time should be assessed. Performance measurement involves identifying performance goals and measures, establishing performance baselines by tracking performance over time, identifying targets for improving performance, and measuring progress against those targets.

Although the SSAs have made efforts to facilitate the cybersecurity framework's adoption, the extent of adoption is unknown because none of the SSAs reported taking action to measure framework implementation by their respective sectors.²⁶ For example:

- Department of Defense officials stated that, due to the voluntary nature of the framework, they do not have a mechanism to assess overall use. They added that Defense Industrial Base officials have indicated that, while there is interest in the framework, companies generally have not fully implemented it because they follow cybersecurity-related requirements established in the Defense Federal Acquisition Regulation Supplement: Safeguarding Covered Defense Information and Cyber Incident Reporting.²⁷
- Department of Energy officials stated that, since the framework is a voluntary tool, they had not taken any formal action to solicit or survey the status of implementation amongst energy sector entities. They

²⁴GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014). An internal control provides reasonable assurance that there is effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

²⁶USDA is a co-SSA with HHS for the food and agriculture sector and did not provide a separate response regarding taking action.

²⁷Department of Defense, *Defense Federal Acquisition Regulation Supplement clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting* (October 21, 2016).

further indicated that they did not have any plans to develop such measurements.

- Department of Agriculture and Department of Health and Human Services officials stated that they do not measure adoption of the framework within their sector. Additionally, although the agencies have no future plans to measure framework adoption, HHS officials stated that they have relied on independent data to develop an understanding of their sector's implementation of the framework.
- Department of Health and Human Services officials stated that they do not track deployment or adoption of the framework by the healthcare and public health sector. The officials attributed their lack of tracking deployment or adoption to the fact that they view their role as helping entities see the link between healthcare regulations, which already impose information security requirements on sector entities, and the framework, rather than enforcing adoption of voluntary guidance.
- Department of Homeland Security officials indicated that they do not track metrics on framework adoption or use, but have knowledge about the frequency at which the framework implementation guidance is downloaded from the C³VP website.
- Department of Transportation officials stated that neither they nor their co-SSA partners at DHS have statistical or quantifiable information to determine adoption rates of the framework within the transportation sector. However, the officials said there is a proposed measurement approach that calls for an aggregate, non-attributorial summary of voluntary reports on adoption of the framework. In addition, sector officials have discussed crafting a survey to collect adoption information. However, according to those officials, approval from the Office of Management and Budget would be required to administer the survey, due to Paperwork Reduction Act provisions.²⁸
- Department of Treasury officials stated that they do not capture data on framework adoption rates for the financial services sector. They added that regulators are not asking entities specifically about framework adoption through the regulatory review process, although

²⁸The Paperwork Reduction Act requires agencies to minimize the paperwork burden they impose on the public to carry out their missions and to maximize the practical utility of the information they collect. Under the act, agencies are required to submit all proposed information collections to the Office of Management and Budget (OMB) for approval. 44 U.S.C. § 3507.

according to the officials, doing so could be another means to collect adoption information.

- Environmental Protection Agency officials indicated that they do not have the statutory authority to collect information from the Water and Wastewater Systems sector regarding adoption/implementation of the framework. Further, they stated that the agency does not now have, and has no current plan to develop, qualitative or quantitative means for measuring adoption in the sector.
- General Services Administration officials indicated that, in the government facilities sector, all agencies have been provided the sector plan designating cybersecurity risk-mitigation activities, commonly referred to as a sector-specific plan. However, the officials stated that it is up to each agency to decide the method of adoption.

In addition, no SCCs reported having qualitative or quantitative measures of framework adoption because they generally do not collect specific information from entities about critical infrastructure protection activities. Sector officials stated numerous impediments to measuring the level of adoption across their respective sectors. For example, officials for the Communications, Electrical subsector of Energy, Financial Services, Food and Agriculture, Government Facilities, and Information Technology sectors indicated that they had neither qualitative nor quantitative means to measure framework adoption.

Further, officials for the Commercial Facilities and Emergency Services sectors stated that they did not have a mechanism currently in place or a plan to obtain this information. Also, officials from the Communications sector indicated that individual associations within the sector have conducted their own efforts to support members' cybersecurity needs. However, they stated that it would not be a good use of resources to focus too closely on measuring use of the framework because obtaining the framework's level of use is not a proxy for an entity's security or preparedness. Additionally, officials from the Electrical subsector of the Energy sector and the Financial Services sector reported that, due to regulations, there is competition between various types of frameworks, and due to the voluntary nature of the NIST framework, entities in the sector are not using it the same way.

Nevertheless, while the sectors have not comprehensively measured the adoption of the framework, other organizations have attempted to gather information about the framework's implementation, with varying results. (None of these studies is projectable across any particular sector because of the use of non-random samples, not using a known and

definable population of potential respondents, and/or small sample sizes within sectors.)

- According to Health and Human Services officials, a healthcare trade association conducted a 2017 study of 126 healthcare information security professions within their membership. Within the study, 62 percent of the 126 respondents indicated that their organizations used the framework.
- According to a 2016 survey conducted by an information security company of 338 IT and security professionals across various industries within the United States, the respondents indicated that adoption of the framework was as high as 19 percent within one sector. Additionally, 44 percent of the respondents indicated their organization currently followed more than one security framework and 43 percent indicated adoption of the cybersecurity framework would occur by end of 2016.
- According to a 2015 study conducted by the Oil and Natural Gas SCC, approximately two-thirds of the 53 oil and natural gas companies surveyed are using the framework in some manner. Half of those using the framework have integrated it into the corporate cybersecurity program in varying ways, while the other half use the framework for various other purposes.

Other entities that have made efforts to assess adoption reported that they faced impediments to generating a methodologically sound population of participants to survey. For example, cybersecurity researchers from Harvard University, the University of Arizona, Indiana University, and George Washington University stated they were in the preliminary stages of conducting a survey about framework use. As part of the development process, they randomly sampled 100 publicly traded companies for a survey pre-test, but received only 1 response. The researchers pointed out 3 impediments to obtaining an adequate sample size:

- entities believe there are risks in participating in a survey;
- entities do not want to invite regulations; and
- some industries do not want to respond to the survey because they have many small companies, and may not be able to represent the diverse views within their industry.

Notwithstanding these impediments to measuring the adoption of the framework, a more comprehensive understanding of the framework's use by critical infrastructure entities is necessary if federal entities, SSAs, and

SCCs want to ensure that facilitation efforts are successful and determine whether organizations are realizing positive results by adopting the framework. Until SSAs have a more comprehensive understanding of the use of the cyber framework by the critical infrastructure sectors, they will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation.

Conclusions

Most sectors have taken action to facilitate adoption of the NIST cybersecurity framework within their respective sectors. By developing implementation guidance and aligning existing sector information resources with framework principles, most SSAs and SCCs have established a set of tools that entities could leverage to adopt the framework. However, none of the SSAs have assessed the extent to which their entities have adopted the framework. Without an accurate assessment of framework adoption within each sector, federal entities, SSAs, and SCCs lack a comprehensive understanding of the current adoption level within critical infrastructure sectors. As such, SSAs are unable to tailor their guidance to effectively encourage use of the framework to sector stakeholders.

Recommendations for Executive Action

We are making nine recommendations to sector-specific agencies in our review for them to develop methods to determine the level and type of framework adoption across their respective sectors. Specifically:

- The Secretary of Agriculture, in cooperation with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector. (Recommendation 1)
- The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector. (Recommendation 2)

- The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 3)
- The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 4)
- The Administrator of General Services, in cooperation with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 5)
- The Secretary of Health and Human Services, in cooperation with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 6)
- The Secretary of Homeland Security, in cooperation with the co-SSAs as necessary, should take steps to consult with respective sector partner(s), such as the SCC, and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sectors.
(Recommendation 7)
- The Secretary of Transportation, in cooperation with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 8)
- The Secretary of Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.
(Recommendation 9)

Agency Comments and Our Evaluation

We received comments on a draft of this report from the nine agencies to which we made recommendations—the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury, and the Environmental Protection Agency and the General Services Administration. Among these agencies, five agreed with our recommendations and four neither agreed nor disagreed with the recommendations.

In written comments, the Department of Agriculture neither agreed nor disagreed with the recommendation in our report, but stated that it will attempt to develop a measurement mechanism as part of its annual data calls to the Food and Agriculture Sector. Additionally, the department stated that it was committed to providing its sector members with guidance on framework adoption in 2018. The department's comments are reprinted in appendix II.

In written comments, the Department of Defense stated it concurred with the report. The department's comments are reprinted in appendix III.

In written comments, the Department of Energy neither agreed nor disagreed with the recommendation in our report. The department noted that its role as the Energy SSA does not include authorities to mandate the collection of information on the level and type of framework adoption across the sector. The department added that it will consult with sector partners on the development of methods for determining the level and type of framework adoption. The department's comments are reprinted in appendix IV.

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

In written comments, DHS concurred with the recommendation in our report and stated that its National Protection and Programs Directorate, as the SSA for 9 of the 16 critical infrastructure sectors, will continue to work closely with its private sector partners to ensure framework adoption is a priority. Additionally, the department stated that the directorate will work closely with its private sector partners to better understand the

extent of framework adoption and barriers to adoption by entities across their respective sectors. DHS's comments are reprinted in appendix VI.

In written comments, the Department of the Treasury neither agreed nor disagreed with the report's recommendation. The department stated that it does not have the authority to compel entities to share cybersecurity framework adoption data. However, the department said it would continue to engage and consult with sector partners to inform its discussions with NIST and DHS regarding identifying or developing methods for determining the level and type of framework adoption by the financial sector. The department's comments are reprinted in appendix VII.

In written comments, the Environmental Protection Agency did not explicitly state whether it agreed or disagreed with our recommendation, but said that it is currently constrained by several factors from implementing the recommendation. The agency also said it agrees that a comprehensive assessment of framework adoption within the water sector would assist with evaluating and tailoring efforts to promote its use. Further, the agency stated that it will continue to work with the Water Sector Coordinating Council and sector partners to promote and facilitate adoption of the cybersecurity framework. The agency also suggested options related to developing cross-sector metrics and survey methods and stated that it will collect available data that may be characterized as cybersecurity framework "awareness," such as downloads of guidance materials and participation in classroom trainings and webinars. The agency's comments are reprinted in appendix VIII.

In written comments, the General Services Administration concurred with the recommendation in our report and stated that it would develop an action plan to address the recommendation. The agency's comments are reprinted in appendix IX.

In an e-mail, the Department of Transportation's Director for Audit Relations and Program Improvement stated that the department concurred with report's findings and recommendation.

In addition to the aforementioned comments, we received technical comments from officials of the Departments of Agriculture, Energy, Health and Human Services, and Homeland Security. We also received technical comments on the report from NIST. We incorporated the technical comments in the report, where appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Agriculture, Commerce, Defense, Energy,

Health and Human Services, Homeland Security, Transportation, and Treasury; the Administrators of the Environmental Protection Agency and General Services Administration; and other interested parties. In addition, the report is 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 Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix X.



Nick Marinos
Director, Cybersecurity and Information Management Issues

Appendix I: Objectives, Scope and Methodology

The objective of our review was to assess what is known about the extent to which critical infrastructure sectors have adopted the National Institute of Standards and Technology’s (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.

To address the objective, we analyzed documentation and evidence, such as from the Department of Homeland Security’s (DHS) Critical Infrastructure Cyber Community Voluntary Program (C³VP) and published sector-specific plans, to determine actions carried out by organizations with lead roles in critical infrastructure protection efforts regarding their promotion of the framework. We included federal lead agencies, referred to as sector-specific agencies (SSA), and sector coordinating councils (SCC) that serve as the voice of each sector and principal entry point for the government to collaborate with each sector, which are established in Presidential Policy Directive 21.¹ Additionally, we reviewed the Fixing America’s Surface Transportation Act, which established the Department of Energy as the lead sector-specific agency for the Energy sector. Table 2 provides an overview of the sectors, SSAs and SCCs.

Table 2: Critical Infrastructure Sectors and Associated Sector-Specific Agency and Sector Coordinating Councils

Sector	Sector-specific agency	Sector coordinating council
Chemical	Department of Homeland Security (DHS)	Chemical Sector Coordinating Council
Commercial facilities	DHS	Commercial Facilities Sector Coordinating Council
Communications	DHS	Communications Sector Coordinating Council
Critical manufacturing	DHS	Critical Manufacturing Sector Coordinating Council
Dams	DHS	Dams Sector Coordinating Council
Defense industrial base	Department of Defense	Defense Industrial Base Sector Coordinating Council

¹The sector coordinating councils for three sectors (representing the Defense Industrial Base, Healthcare and Public Health, and Transportation Systems) did not respond to our inquiry regarding assessment of framework adoption in their respective sector.

**Appendix I: Objectives, Scope
and Methodology**

Sector	Sector-specific agency	Sector coordinating council
Emergency Services	DHS	Emergency Services Sector Coordinating Council
Energy	Department of Energy	Energy Sector - Electrical Subsector Coordinating Council Energy Sector - Oil & Natural Gas Subsector Coordinating Council
Financial services	Department of the Treasury	Financial Services Sector Coordinating Council
Food and agriculture	Departments of Agriculture and Health and Human Services	Food and Agriculture Sector Coordinating Council
Government facilities	DHS and General Services Administration	Government Facilities Government Coordinating Council
Health care and public health	Department of Health and Human Services	Healthcare and Public Health Sector Coordinating Council
Information technology	DHS	Information Technology Sector Coordinating Council
Nuclear reactors, materials, and waste	DHS	Nuclear Reactors, Materials, and Waste Sector Coordinating Council
Transportation systems	DHS (Transportation Security Administration/U.S. Coast Guard) and Department of Transportation	Aviation Sector Coordinating Council Freight Rail Sector Coordinating Council Highway and Motor Carrier Sector Coordinating Council Mass Transit and Passenger Rail Sector Coordinating Council Pipeline Sector Coordinating Council
Water and wastewater systems	Environmental Protection Agency	Water and Wastewater Systems Sector Coordinating Council

Source: GAO analysis of Presidential Policy Directive 21. | GAO-18-211

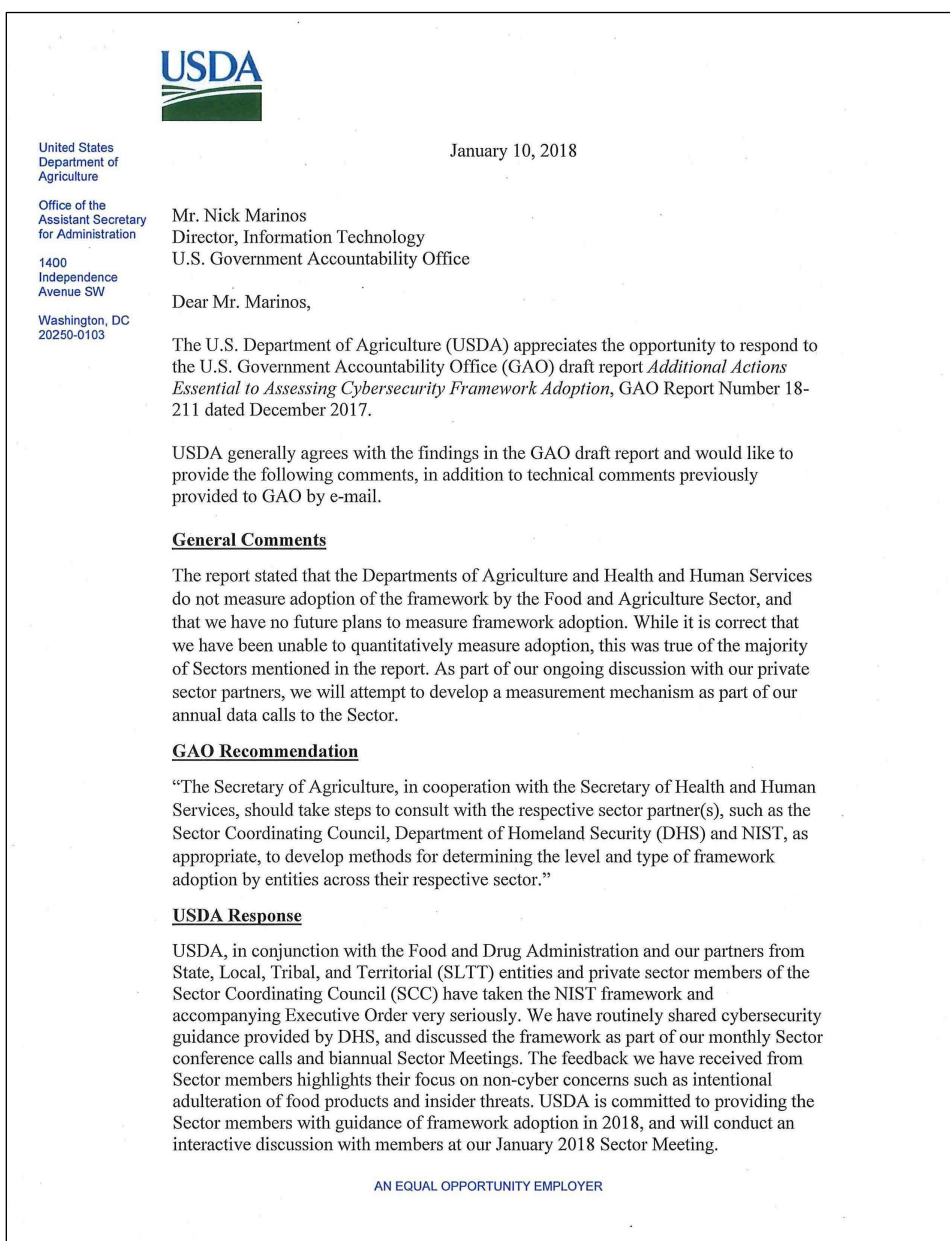
We also conducted interviews with officials from DHS’s C³VP to determine the extent to which they have developed a means to measure the effectiveness of actions taken to promote and support the adoption of the framework. Further, we reviewed published implementation guidance and interviewed SSA officials to determine the extent to which framework implementation guidance has been developed across 16 sectors.

Additionally, we examined what actions had been taken or planned that would result in a qualitative or quantitative assessment of the level of framework adoption by members of their respective sector. We also interviewed officials from federal agencies, including NIST, DHS, and the SSAs, as well as SCCs, to determine the level and type of framework adoption within the private sector and determine their definition of the term “adoption.” Specifically, we asked officials if their respective sector had any qualitative or quantitative means for measuring implementation of the framework by sector entities.

We also interviewed officials from relevant federal agencies, including NIST, DHS, and the SSAs, as well as SCCs, to gather views of challenges to adopting the framework, within their respective critical infrastructure sectors. Specifically, we asked officials what challenges they found with respect to adopting or implementing the framework. We obtained proposed or executed survey information from SSAs, SCCs, private industry, and academic sources.

We conducted this performance audit from March 2017 to February 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Agriculture



**Appendix II: Comments from the Department
of Agriculture**

Thank you again for the opportunity to review and respond to the GAO draft report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Bice" with a stylized flourish.

Donald K. Bice
Acting Deputy Assistant Secretary

AN EQUAL OPPORTUNITY EMPLOYER

Appendix III: Comments from Department of Defense



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
8000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-8000

JAN 11 2018

Mr. Nick Marinos
Director, Information Technology
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-18-211, "CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Essential to Assessing Cybersecurity Framework Adoption," dated December 18, 2017 (GAO Code 101948).

The DoD concurs with the draft report. Our Principal Action Officer is Ms. Vicki Michetti, Director, Defense Industrial Base Cybersecurity Program, (703) 545-2220, vicki.d.michetti.civ@mail.mil.

Sincerely,

A handwritten signature in cursive script, appearing to read "Therese Firmin".

Therese Firmin
Acting Deputy Chief Information Officer
for Cybersecurity

**GAO DRAFT REPORT DATED DECEMBER 18, 2017
GAO-18-211 (GAO CODE 101948)**

**“CRITICAL INFRASTRUCTURE PROTECTION: ADDITIONAL ACTIONS
ESSENTIAL TO ASSESSING CYBERSECURITY FRAMEWORK ADOPTION”**

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

RECOMMENDATION: The GAO recommends that the Secretary of Defense should take steps to consult with the respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.

DoD RESPONSE: The DoD concurs with the draft report.

Appendix IV: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

January 24, 2018

Mr. David C. Trimble
Director
Natural Resources and Environment
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Director Trimble:

The U.S. Department of Energy (DOE) appreciates the opportunity to respond to the Government Accountability Office's (GAO) Draft Report "Critical Infrastructure Protection – Additional Actions Essential to Assessing Cybersecurity Framework Adoption."

DOE's response to the Report's draft recommendation that involves DOE is as follows:

Recommendation 3: "...The Secretary of Energy should take steps to consult with the respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.

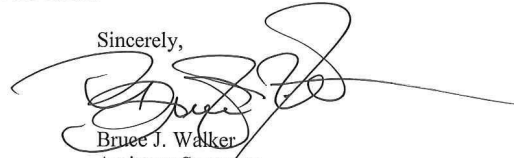
Response: DOE will consult with sector partners on the development of methods for determining the level and type of National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST Framework) adoption. DOE's Cybersecurity Capability Maturity Model (C2M2) tool for the energy sector aligns with the current NIST Framework and DOE has provided C2M2 to over 1,000 organizations and conducted numerous on-site C2M2 facilitations with energy sector companies. In 2018, DOE's Office of Electricity Delivery and Energy Reliability will embark on an effort to update C2M2 to align with version 1.1 of the NIST Framework. A milestone of the update will be a stakeholder workshop in the first half of 2018, which will include the participation of partners from the Sector Coordinating Councils (SCCs), U.S. Department of Homeland Security (DHS), and NIST. A component of the workshop will be an examination and discussion of the adoption of the NIST Framework, C2M2, and other guidance documents.

However, as noted in the draft report, the NIST Framework is a voluntary tool and not a regulatory instrument. DOE's role as the Energy sector-specific agency (SSA) does not include authorities to mandate the collection of information on the level and type of NIST Framework adoption across the sector. DOE appreciates the voluntary nature of the NIST Framework as this construct has allowed DOE to have richer and more constructive



discussions with industry and interagency partners on continually improving the cybersecurity posture of the sector.

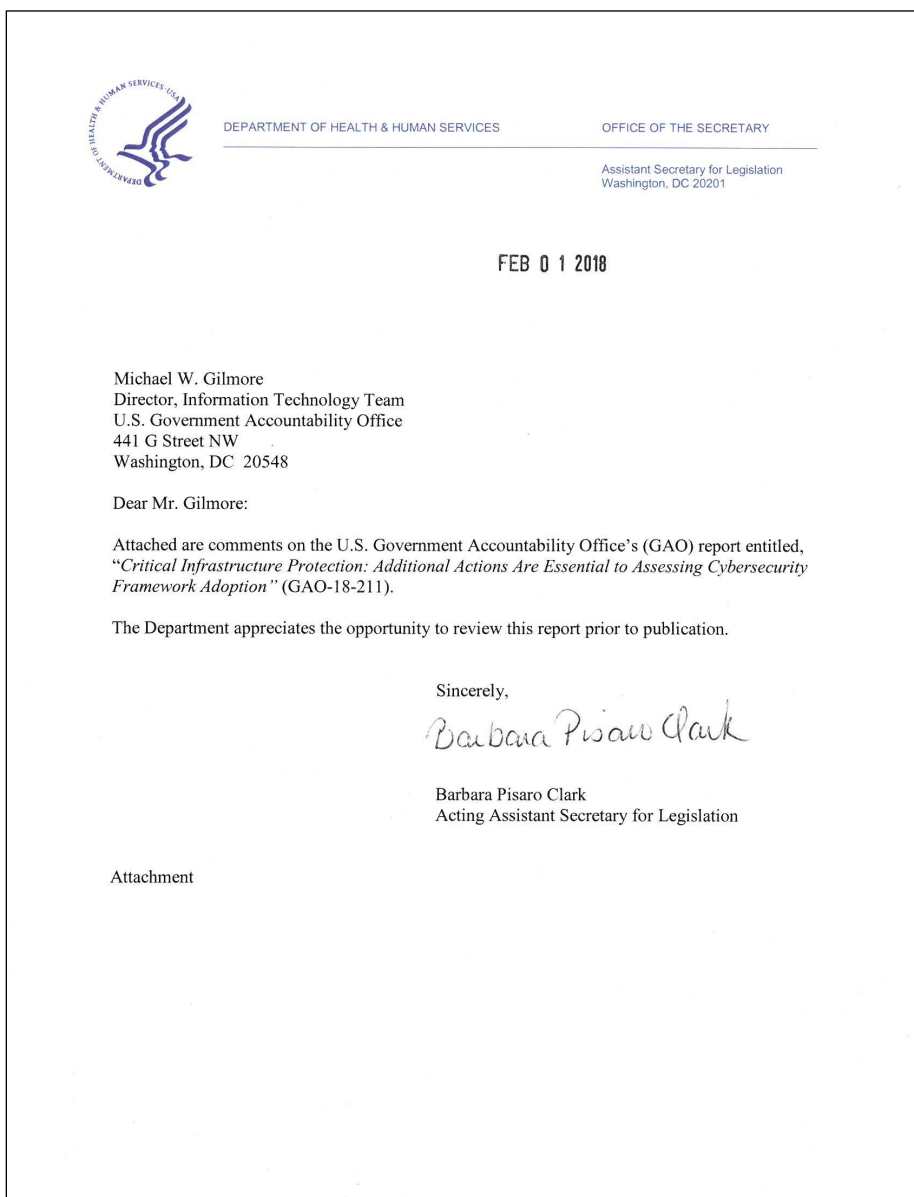
Sincerely,



Handwritten signature of Bruce J. Walker in black ink, featuring a large, stylized initial 'B' and 'W'.

Bruce J. Walker
Assistant Secretary
Office of Electricity Delivery and Energy Reliability

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



**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED - CRITICAL INFRASTRUCTURE PROTECTION:
ADDITIONAL ACTIONS ARE ESSENTIAL TO ASSESSING CYBERSECURITY
FRAMEWORK ADOPTION (GAO-18-211)**

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

Recommendation

The Secretary of Health and Human Services, in cooperation with the Secretary of Agriculture, should take steps to consult with the respective sector partner(s) such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.

HHS Response

HHS concurs with GAO's recommendation and will work with HHS agencies as appropriate to assist in HHS activities regarding sector adoption.

Appendix VI: Comments from the Department of Homeland Security

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



**Homeland
Security**

January 29, 2018

Nick Marinos
Director, Cybersecurity and Information Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-18-211, "CRITICAL
INFRASTRUCTURE PROTECTION: Additional Actions Essential to Assessing
Cybersecurity Framework Adoption"

Dear Mr. Marinos:

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

The Department is pleased to note GAO's positive recognition of DHS National Protection and Programs Directorate (NPPD) efforts to assist the enhancement of critical infrastructure cybersecurity and to encourage adoption of the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" ("Framework"). As GAO highlights, these efforts have included increasing outreach and awareness of the framework, creating and disseminating of framework implementation guidance, and providing resources to assist in implementing the Framework.

As discussed with GAO during this audit, in addition to previous GAO audits that have examined these issues, specifically in GAO-16-152¹ and GAO-16-79², the public-private partnership model between DHS, Government Coordinating Councils (GCCs), Sector Coordinating Councils (SCCs), cross-sector councils, and the Sector Specific Agencies (SSAs) is inherently voluntary. Various challenges within these entities hamper efforts to adopt the framework still exist, including many outside of their control. DHS will continue to work with its sector partners to promote and support the Framework's adoption for cyber risk mitigation.

The draft report contained one recommendation for DHS with which the Department concurs. Attached find our detailed response to the recommendation. Technical comments were previously provided under separate cover.

¹ Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework (GAO-16-152, Issue date: 12/17/2015).

² Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress (GAO-16-79, Issue date: 11/19/2015).

Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,



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

Attachment

**Attachment: Management Response to Recommendation
Contained in GAO-18-211**

GAO recommended that the Secretary of Homeland Security, in cooperation with the co-SSAs as necessary:

Recommendation: Take steps to consult with their respective sector partner(s), such as the Sector Coordinating Council (SCC), and National Institute of Standards and Technology (NIST), as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sectors.

Response: Concur. NPPD, as the SSA for nine of the 16 critical infrastructure sectors, will continue to work closely with its private sector partners to ensure Framework adoption is a priority. NPPD will work closely with its private sector partners to better understand the extent of Framework adoption and barriers to adoption by entities across their respective sectors. During the coming year, through various outreach and awareness engagements, including webinars, road shows, conferences, and regular working group meetings, DHS SSA's will work to develop best practices for Framework adoption for their sector partners, which will then be shared with others, as appropriate. Estimated Completion Date: December 31, 2018.

Appendix VII: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 16, 2018

Nick Marinos
Director
Cybersecurity and Information Management
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review the draft report entitled *Critical Infrastructure Protection: Additional Actions Essential to Assessing Cybersecurity Framework Adoption* (the Report). This letter provides the official response of the Department of the Treasury (Treasury).

The Report assesses adoption of the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure (the NIST Framework) and recommends that Treasury take steps to consult with our sector partners to develop methods for determining the level and type of framework adoption by entities across the financial services sector.

Treasury meets regularly with public and private sector partners and continues to encourage the adoption of the NIST Framework through these engagements. Treasury believes that the Framework adoption will improve current and future cybersecurity risk management efforts of entities, thereby enhancing the security and resilience posture of the financial sector. Treasury actively worked with the sector and NIST during the development of the Framework and to promote its use. We will continue such engagement and consult with sector partners to inform our discussions with NIST and DHS regarding identifying or developing methods for determining the level and type of Framework adoption by the financial sector. We believe that, both for comparability across sectors and because of sector interdependencies, ideally a single methodology to measure Framework adoption would be developed (or identified) that could be leveraged for use by various sectors (or perhaps certain sub-sectors) if feasible.

As GAO is aware, Treasury does not have the authority to compel entities to share NIST Framework adoption data with Treasury. This level of information would be identified through the independent regulatory review process conducted by the various independent financial regulators at both the federal and state level. Such regulatory review information is not shared with unauthorized parties, including Treasury. For this reason, Treasury does not have access to current adoption rates of the NIST Framework at the financial services sector entity level. Moreover, with over 800,000 entities comprising the sector and with multiple regulators for the sector's multiple sub-sectors at both the federal and state level, and with the lack of legal authority, ultimately Treasury would be unable to successfully measure framework adoption across the sector.

**Appendix VII: Comments from the Department
of the Treasury**

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

Sincerely,



Christopher Campbell
Assistant Secretary
Financial Institutions

Appendix VIII: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JAN 17 2018

OFFICE OF WATER

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

Dear Mr. Gomez:

Thank you for the opportunity to review and comment on GAO's draft report, "Critical Infrastructure Protection: Additional Actions Essential to Assessing Cybersecurity Framework Adoption. GAO-18-211." The purpose of this letter is to provide the U.S. Environmental Protection Agency's response to the draft report's findings, conclusions, and recommendation(s).

GAO developed this report to fulfill a requirement under the Cybersecurity Enhancement Act of 2014, to assess periodically the extent to which critical infrastructure sectors have adopted the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). To conduct this assessment, GAO interviewed officials and reviewed documentation from the following entities:

- Federal lead agencies for critical infrastructure protection, designated as sector-specific agencies under Presidential Policy Directive 21, for each of sixteen critical infrastructure sectors;
 - PPD 21 assigns EPA as the SSA for the Water and Wastewater Systems (water) sector;
- Sector coordinating councils, which are comprised of nonfederal members and serve to facilitate government collaboration with each sector; and
- The National Institute of Standards and Technology, which developed the Cybersecurity Framework.

GAO queried these entities regarding any qualitative or quantitative measures of Cybersecurity Framework usage by critical infrastructure facilities. However, neither GAO nor NIST defined metrics for "adoption" or developed methodologies for assessing implementation of the Cybersecurity Framework. Further, GAO did not conduct any surveys of critical infrastructure facilities to make a direct assessment of Cybersecurity Framework adoption.

The EPA generally agrees with GAO's findings and conclusions in the report. The agency, however, has suggestions regarding the recommendation as described below.

GAO Recommendation:

The Administrator of the Environmental Protection Agency should take steps to consult with their respective sector partner(s), such as the SCC, DHS and NIST, as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector.

EPA Response:

The agency agrees with GAO that a comprehensive assessment of Cybersecurity Framework adoption within the water sector would assist with evaluating and tailoring efforts to promote use of the Framework. However, the agency is currently constrained by several factors from implementing this recommendation. Under the Paperwork Reduction Act, the agency cannot participate in a survey to assess Cybersecurity Framework implementation by the water sector without prior approval from the Office of Management and Budget through an Information Collection Request. There is currently no legal requirement that the agency should collect this information from sector facilities.

Additionally, as the GAO report illustrates, water sector facilities are reluctant to divulge sensitive information about specific infrastructure protection activities, including cybersecurity. Based on lessons learned through engaging the Water SCC, the agency believes that for a survey of Cybersecurity Framework adoption in the water sector to be successful, the sector would require: 1) a strong mandate for the collection from a federal entity with overarching responsibility for critical infrastructure cybersecurity; and 2) a unified cross-sector approach to metrics and survey methods for assessing Cybersecurity Framework adoption.

One option to resolve the latter challenge would involve a GAO recommendation to form an interagency workgroup consisting of NIST, DHS and the non-DHS SSAs, with the challenge to develop unified cross-sector metrics and survey methods. Although cybersecurity threats and vulnerabilities associated with process control, business enterprise and communication systems share many commonalities across critical infrastructure sectors, no standard basis exists for assessing the adoption of countermeasures as captured by the Cybersecurity Framework. A standardized approach to metrics and survey methods would permit the comparison of assessment results across sectors, which in turn could assist with targeting or refining federal cybersecurity resources.

The agency will continue to work with the Water SCC and sector partners to promote and facilitate adoption of the Cybersecurity Framework through the programmatic activities. The agency will also collect available data that may be characterized as Cybersecurity Framework "awareness," such as downloads of guidance materials and participation in classroom trainings and webinars.

The EPA appreciates the opportunity to review the draft GAO report. Please contact Dan Schmelling, schmelling.dan@epa.gov or 202-557-0683, with questions or to request further information.

Sincerely,



David P. Ross
Assistant Administrator

cc: EPA GAO Liaison Team

Appendix IX: Comments from the General Services Administration



The Administrator

January 24, 2018

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

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office (GAO) draft report entitled *Critical Infrastructure Protection: Additional Actions Are Essential to Assessing Cybersecurity Framework Adoption* (GAO-18-211).

GAO recommended that "the Administrator of the General Services Administration, in cooperation with the Secretary of Homeland Security, should take steps to consult with the respective sector partner(s), such as the Coordinating Council and NIST [National Institute of Standards and Technology], as appropriate, to develop methods for determining the level and type of framework adoption by entities across their respective sector."

GSA agrees with the recommendation, and will develop an action plan to address the recommendation. Additionally, GSA had no comments on the draft report.

If you have any questions or concerns, please contact me at (202) 501-0800 or Mr. P. Brennan Hart III, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

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

Emily W. Murphy
Administrator

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Appendix X: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore, Assistant Director; Kush K. Malhotra, Analyst-In-Charge; Lisa Hardman; David Plocher; Harold Podell; Tind S. Ryen; Priscilla Smith; Andrew Stavisky; Paige Teigen; and Elaine Vaurio 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 GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

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, <http://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](#), [LinkedIn](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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