United States Government Accountability Office

Report to Congressional Committees

December 2015

CRITICAL INFRASTRUCTURE PROTECTION

Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework

Accessible Version

GAO-16-152

December 2015

CRITICAL INFRASTRUCTURE PROTECTION

Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework

GAO Highlights

Highlights of GAO-16-152, a report to congressional committees

Why GAO Did This Study

U.S. critical infrastructures, such as financial institutions and communications networks, are systems and assets vital to national security, economic stability, and public health and safety. Systems supporting critical infrastructures face an evolving array of cyber-based threats. To better address cyber-related risks to critical infrastructure, federal law and policy called for NIST to develop a set of voluntary cybersecurity standards and procedures that can be adopted by industry to better protect critical cyber infrastructure.

The Cybersecurity Enhancement Act of 2014 included provisions for GAO to review aspects of the cybersecurity standards and procedures developed by NIST. This report determines the extent to which (1) NIST facilitated the development of voluntary cybersecurity standards and procedures and (2) federal agencies promoted these standards and procedures. GAO examined NIST's efforts to develop standards, surveyed a non-generalizable sample of critical infrastructure stakeholders, reviewed agency documentation, and interviewed relevant officials.

What GAO Recommends

GAO recommends that DHS develop metrics to assess the effectiveness of its framework promotion efforts. In addition, DHS and GSA should set a time frame to determine whether implementation guidance is needed for the government facilities sector. DHS and GSA concurred with the recommendations.

View GAO-16-152. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In accordance with requirements in a 2013 executive order which were enacted into law in 2014, the National Institute of Standards and Technology (NIST) facilitated the development of a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure. This process, which involved stakeholders from the public and private sectors, resulted in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. The framework is to provide a flexible and risk-based approach for entities within the nation's 16 critical infrastructure sectors to protect their vital assets from cyber-based threats. To develop the framework in a collaborative manner, NIST solicited input from sector stakeholders through a formal request for information and conducted multiple workshops with critical infrastructure owners and operators, industry associations, government agencies, and other stakeholders. Participants GAO surveyed were generally satisfied with the approach NIST took to develop the framework. Further, the framework meets the requirements established in federal law that it be flexible, repeatable, performance-based, and cost-effective. For example, the framework contains multiple implementation "tiers," which allows it to be adapted to an organization's specific conditions and needs.

Agencies with responsibilities for supporting protection efforts in critical infrastructure sectors (known as sector-specific agencies), and NIST have promoted and supported adoption of the cybersecurity framework in the critical infrastructure sectors. For example, the Department of Homeland Security (DHS) established the Critical Infrastructure Cyber Community Voluntary Program to encourage adoption of the framework and has undertaken multiple efforts as part of this program. These include developing guidance and tools that are intended to help sector entities use the framework. However, DHS has not developed metrics to measure the success of its activities and programs. Accordingly, DHS does not know if its efforts are effectively encouraging adoption of the framework.

Sector-specific agencies have also promoted the framework in their sectors by, for example, presenting to meetings of sector stakeholders and holding other promotional events. In addition, all of the sector-specific agencies except for DHS and the General Services Administration (GSA), as co-SSAs for the government facilities sector, had decided whether or not to develop tailored framework implementation guidance for their sectors, as required by Executive Order 13636. Specifically, DHS and GSA had not yet set a time frame to determine whether sector-specific implementation guidance is needed for the government facilities sector. By not doing so, DHS and GSA may be hindering the adoption of the cybersecurity framework in this sector.

Contents

Tables

Figure

Abbreviations

C^3	Critical Infrastructure Cyber Community
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
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
PPD	Presidential Policy Directive
SSA	sector-specific agency

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

December 17, 2015

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, and it relies extensively on computerized systems and electronic data to carry out its missions.[1] The cyber threat to critical infrastructure continues to grow and represents a serious national security challenge. Foreign malicious actors have directly attacked and extracted highly sensitive materials from the networks 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, we continued to designate federal information security as a government-wide high-risk area in our most recent biennial

[1]The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (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.

report to Congress, a designation we have made in each report since 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure and we continued to do so in the most recent update to our high-risk list.[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. It called for, among other things, the Director of the National Institute of Standards and Technology (NIST) 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 addition, the Cybersecurity Enhancement Act of 2014 was enacted in December 2014 to authorize, among other things, NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure.[4]

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 objectives for this review were to determine the extent to which (1) NIST facilitated development of voluntary standards and procedures to reduce cyber risks to critical infrastructure, and (2) federal agencies promoted the standards and procedures to reduce cyber risks to critical infrastructure.

To determine the extent to which NIST facilitated development of voluntary standards and procedures to reduce cyber risks to critical infrastructure, we reviewed the methodology and process used by NIST to create the *Framework for Improving Critical Infrastructure Cybersecurity*.[5] We examined how NIST developed the framework, including how industry comments were integrated into the document. In

[2]*High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

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

[4]Pub. L. No. 113-274 (Dec. 18, 2014).

[5]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

addition, we surveyed participants in the framework's development. Our population for this survey included individuals who (1) provided written comments with contact information in response to a NIST request for information notice or (2) registered for at least one of the workshops hosted by NIST to develop the framework. There were 2,082 individuals in the population that we targeted, and we sent the survey request to all of them and received 252 completed surveys.[6] We also interviewed relevant NIST officials involved in the framework's development and federal officials from agencies with lead roles in critical infrastructure protection efforts, referred to as sector-specific agencies (SSA), representing all 16 critical infrastructure sectors established in federal policy. Also, we evaluated the framework against the requirements from Executive Order 13636 and the Cybersecurity Enhancement Act of 2014 to determine whether these criteria were implemented in the framework.

To determine the extent to which federal agencies, including the SSAs and NIST, promoted the standards and procedures to reduce cyber risks, we analyzed documents and the website of the DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program to assess the framework promotional guidance and tools provided to the critical infrastructure sectors. We also collected and analyzed relevant documentation from the SSAs about efforts to promote the framework. In addition, we analyzed the metrics and information being used by the DHS C^3 Voluntary Program to measure its activities' success in promoting the adoption of the framework. Further, we collected and analyzed relevant documents and surveyed individuals who responded to NIST's request for information and registered for one of the workshops hosted by NIST for the development of the framework to identify DHS, SSA, and NIST efforts to promote the framework. We also interviewed federal officials from the nine SSAs— including DHS— representing the 16 critical infrastructure sectors, and NIST regarding their efforts to promote the framework and create sector-specific framework implementation guidance.

[6]To make the survey as inclusive as possible, we sent out a questionnaire to all of the workshop registrants and respondents to NIST's requests for information, and were able to obtain a 12 percent response rate in the time available for survey fieldwork. Because we do not know if the answers that nonrespondents would have given would materially differ from those that did respond, our results can only represent the views of those who did respond. Their views are not generalizable to the registrant and respondent population as a whole.

We conducted this performance audit from February 2015 to December 2015 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 I discusses our objectives, scope, and methodology in greater detail.

Background

U.S. critical infrastructure is made of 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 national security, economic security, national public health or safety, or any combination of these matters. 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. Sector-specific agencies (SSA) are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of their designated critical infrastructure sector in the all-hazards[7] environment.

The Nation Faces an Evolving Array of Cyber-Based Threats

Threats to systems supporting critical infrastructure and federal information systems are evolving and growing. Risks to cyber-based assets can originate from unintentional and intentional threats. Unintentional or non-adversarial threat sources include failures in equipment, software coding errors, or resource depletion, such as accidental actions of employees. They also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of its control. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage

[7]"All hazards" is defined by Presidential Policy Directive 21 as a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

and information warfare, and terrorists. These threat 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. Table 1 describes the sources of cyber-based threats in more detail.

Table 1: Common Cyber Threat Sources

Source	Category	Description
Non-adversarial/non-malicious	Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications.
	Failure in environmental controls	Failures in temperature/humidity controllers or power supplies.
	Failure in software	Failures in operating systems, networking, and general-purpose and mission-specific applications.
	Natural or man-made disaster	Fires, floods, tsunamis, tornadoes, hurricanes, and earthquakes, which are beyond an entity's control.
	Unusual or natural event	Natural events beyond the entity's control that are not considered to be disasters (e.g., sunspots).
	Infrastructure failure or outage	Failure or outage of telecommunications or electrical power.
	Unintentional user errors	Failures resulting from erroneous, accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities.
Adversarial	Hackers or hacktivists	Hackers break networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals.
	Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. These individuals engage in purely malicious activities and should not be confused with non-malicious insider accidents.
	Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs, use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
	Criminal groups and organized crime	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion.
	Terrorist	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.

Source	Category	Description
	Unknown malicious outsiders	Unknown malicious outsiders are threat sources or agents that, due to a lack of information, agencies are unable to classify as being one of the five types of threat sources or agents listed above.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-16-152

Cyber threat 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. Table 2 provides descriptions of common exploits or techniques, tactics, and practices used by cyber adversaries.

Table 2: Common Methods of Cyber Exploits

Exploit	Description
Watering hole	A method by which threat actors exploit the vulnerabilities of websites frequented by users of the targeted system. Malware is then injected into the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cyber-security supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Structured Query Language (SQL) injection	An exploit that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database, resulting in data loss or corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing the adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.

Exploit	Description
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming code (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.
Cross-site request forgery	An exploit that takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory pathname in an application that does not properly neutralize special elements (e.g. '…', '/', '…/', etc.) within the pathname.
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally controlled format strings in print-style functions to gain access to information and/or execute unauthorized code or commands.
Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site which may contain malware that can compromise the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ()".
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from un-trusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanisms are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certification authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Sockets Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit which combines elements of two or more of the aforementioned techniques.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-16-152

Federal Policy and Law Address the Protection of Cyber Critical Infrastructure

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

Presidential Policy Directive 21 (PPD-21)[8] assigns roles and responsibilities for the critical infrastructure sectors to the SSAs. The directive identified 16 critical infrastructure sectors and designated associated federal SSAs. Table 3 shows the 16 critical infrastructure sectors and the SSA for each sector.

Table 3: Critical Infrastructure Sectors and Related Sector-Specific Agencies

Critical infrastructure sector	Description	Sector-specific agency
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical sector produces products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security (DHS)
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	DHS
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical manufacturing	Transforms materials into finished goods. The sector includes the manufacture of primary metals, machinery, electrical equipment, appliances and components, and transportation equipment.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and similar structures, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	DHS
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Financial services	Provides the financial infrastructure of the nation. This sector consists of commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions.	Department of the Treasury

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

Critical infrastructure sector	Description	Sector-specific agency
Food and agriculture	Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.	Department of Agriculture Department of Health and Human Services (Food and Drug Administration)
Government facilities	Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.	DHS General Services Administration
Health care and public health	Protects the health of the population before, during, and after disasters and attacks. The sector consists of direct health care, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.	Department of Health and Human Services
Information technology	Produces information technology and includes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
Nuclear reactors, materials, and waste	Provides nuclear power. The sector includes commercial nuclear reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; the decommissioning of reactors; and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	DHS (Transportation Security Administration and U.S. Coast Guard) Department of Transportation
Water and wastewater systems	Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.	Environmental Protection Agency

Source: GAO analysis of Presidential Policy Directive-21. | GAO-16-152

PPD-21 identified SSA roles and responsibilities to include collaborating with critical infrastructure owners and operators; independent regulatory agencies; and state, local, tribal, and territorial entities as appropriate, as well as providing, supporting, or facilitating technical assistance and consultations for their respective sectors to identify vulnerabilities and help mitigate incidents, as appropriate.

Federal law and policy have also established roles and responsibilities for federal agencies to work with industry to enhance the cybersecurity of the nation's critical infrastructures. These include Executive Order 13636, the

Cybersecurity Enhancement Act of 2014, and the National Infrastructure Protection Plan (NIPP).[9]

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued in February 2013, outlines an action plan for improving security for critical cyber infrastructure. This includes, among other things, requirements for NIST to develop a voluntary critical infrastructure cybersecurity framework and performance measures. In developing the cybersecurity framework, NIST is to engage in an open public review and comment process. The order also directs 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.

The Cybersecurity Enhancement Act of 2014, enacted in December 2014, established requirements that are consistent with the order regarding NIST's development of a cybersecurity framework. NIST's responsibilities in developing the cybersecurity framework under this law include, among other things, identifying an approach that is

- flexible,
- repeatable,
- performance-based, and
- cost-effective.

In response to Executive Order 13636, NIST issued the *Framework for Critical Infrastructure Cybersecurity* in February 2014, which is intended to help organizations apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. 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

[9]DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013).

sectors,[10] which is to provide guidance for developing individual organization profiles. Through the use of 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.[11] (Further information on the framework core is provided in app. II.)

The NIPP defines the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort. DHS developed the NIPP in collaboration with public- and private-sector owners and operators and federal and nonfederal government representatives, including SSAs, from the critical infrastructure community. It details DHS's roles and responsibilities in protecting the nation's critical infrastructures and how sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. It emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments.

According to the NIPP, SSAs are to work with their private-sector counterparts to understand cyber risk and develop sector-specific plans that address the security of the sector's cyber and other assets and functions. The SSAs and their private-sector partners are to update their sector-specific plans based on DHS sector-specific plan guidance issued in 2014.

[10]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.

[11]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.

NIST Developed the Cybersecurity Framework in a Facilitated Manner to Fulfill Responsibilities

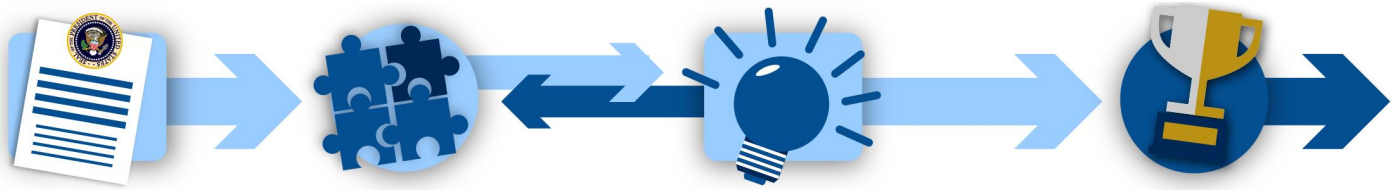
NIST used several methods to obtain and incorporate stakeholder views when developing its cybersecurity framework. Respondents to our survey were generally satisfied with NIST's efforts and methods to develop the framework. Also, NIST met the requirements under Executive Order 13636 and the Cybersecurity Enhancement Act to develop an approach that can help critical infrastructure organizations manage cyber risk.

NIST Obtained and Incorporated Stakeholder Views in Developing the Framework

Executive Order 13636, released in February 2013 required NIST to create a flexible performance-based cybersecurity framework that includes a set of standards, procedures, and processes that align policy, business, and technological approaches to address cyber risks. In addition, under the Cybersecurity Enhancement Act, enacted into law in December 2014, NIST is required to facilitate and support the development of a voluntary set of standards, guidelines, methodologies, and procedures to cost-effectively reduce cyber risks to critical infrastructure.

In February 2014, NIST issued the *Framework for Critical Infrastructure Cybersecurity*. In developing the framework, NIST used several methods to obtain and incorporate the views of experts from government, industry, and academia. Specifically, it solicited public comments through formal "requests for information," held workshops with stakeholders to identify and develop elements of the framework, and published a draft version of the framework for further review and comment. Figure 1 summarizes the development of the framework.

Figure 1: Process for Development of the National Institute of Standards and Technology's Cybersecurity Framework



Mandate

- Executive Order 13636

Collaboration Process

- National Institute of Standards and Technology (NIST) issued a request for information to solicit commentary on standards
- NIST hosted 6 cybersecurity workshops to engage industry in the development of the cybersecurity framework

Development

- NIST collected, categorized, and posted responses to the request for information to its cybersecurity website for public view
- NIST conducted an initial analysis of request for information common cybersecurity practices and themes based on request for information responses
- NIST presented and discussed initial request for information analysis at 2nd cybersecurity workshop
- NIST created a framework outline between the 2nd and 3rd cybersecurity workshops
- NIST drafted the initial framework between the 3rd and 4th cybersecurity workshops
- Commentary from workshops was put into the development process for the framework
- NIST published a formal draft for comment, and considered the comments received for the final product

Final Product

- NIST released the first version of the *Framework for Improving Critical Infrastructure Cybersecurity*
- NIST issued a 2nd request for information to obtain commentary on user's experience with framework
- NIST hosted a 6th workshop to gather public input on initial experiences with framework

Source: GAO analysis of NIST documentation. | GAO-16-152

NIST began the collaboration process for developing the framework on February 26, 2013, when it issued a formal request for information in the Federal Register to seek comments regarding risk management practices, frameworks, standards, guidelines, and best practices. NIST received 246 unique comments in response to the request from organizations and individuals representing, among others, large companies, associations, sector coordinating councils, federal agencies, universities, and international companies. NIST analyzed the comments received to, among other things, identify common cybersecurity practices and methods to facilitate discussions on the development of the framework.

After the initial request for information, NIST hosted six workshops at various locations across the country to drive the development of the framework. Workshop participants and attendees included critical

infrastructure owners and operators, industry associations, individual companies, and government agencies. Table 4 summarizes the NIST workshops.

Table 4: Summary of National Institute of Standards and Technology (NIST)–Hosted Cybersecurity Framework Workshops

Workshop	Date	Location	Workshop summary	Outcome
1	April 2013	Department of Commerce, Washington, DC	Collected information about current risk management practices; use of frameworks, standards, guidelines, and best practices; and specific industry practices to begin development of the framework.	Initial ideas and concepts to develop framework
2	May 2013	Carnegie Mellon University, Pittsburgh, PA	Created the initial body of standards, guidelines, best practices, tools, and procedures used to populate the initial draft framework; achieved consensus on cross-sector principles, common points, and themes; and identified initial gaps from comments provided by industry in response to the formal request for information in the Federal Register.	NIST initial analysis of comments received from formal request for information
3	July 2013	University of California, San Diego, CA	Discussed how to refine and generate content for the framework, with a focus on core elements and incorporating cross-sector needs.	Draft of initial framework components
4	September 2013	University of Texas at Dallas, Richardson, TX	Reviewed and refined the content in the draft of the preliminary framework and discussed topics related to implementation of the framework.	Preliminary draft of framework
5	November 2013	North Carolina State University, Raleigh, NC	Engaged stakeholders on the preliminary framework; discussed strategies around implementation and further development of the framework.	Feedback on improvements to preliminary framework
6	October 2014	Florida Center for Cybersecurity, Tampa, FL	Discussed industry initial experiences with the published framework.	NIST receipt of user experience with the framework

Source: GAO analysis of documentation of NIST workshops. | GAO-16-152

At each workshop, NIST facilitated discussions with attendees and accepted industry input to collaboratively identify and develop standards and guidelines for the framework. Based on the input from the first four workshops, NIST prepared and published a preliminary draft of the framework for public review and comment following its fourth workshop.

NIST analyzed responses to its request for information, conclusions from workshops, and stakeholder analysis to select components for the framework, such as identifying security common practices, principles, and approaches that supported the objectives of Executive Order 13636. To identify the framework components that reflected the comments received, NIST used input from volunteer industry stakeholders. These stakeholders helped to, among other things, evaluate common themes

identified by NIST as well as cybersecurity areas that needed additional exploration to encourage industry engagement in the framework development process. After the initial draft was issued for comment, NIST held the fifth workshop to obtain further stakeholder input. Subsequently, NIST published its final draft of the framework in February 2014.

Following issuance of the framework, on August 26, 2014, NIST issued a second request for information to seek comments on users' experience with the framework, as part of its efforts to promote use of the framework, and held an additional workshop to obtain information on how organizations learned about and used the framework. NIST received 57 unique comments in response to the second request for information from organizations and individuals that represented, among others, large companies, associations, and sector coordinating councils.

In addition to the framework, NIST developed a roadmap to discuss future plans for the framework, which included identifying areas of improvement of the preliminary framework. To promote the use and adoption of the framework, NIST officials stated they plan to update the framework based on industry feedback and develop guidance on how organizations can use the framework to reduce cybersecurity risks.

Participants Who Responded to Our Survey Were Generally Satisfied with NIST's Development Efforts

One of NIST's responsibilities under the Cybersecurity Enhancement Act was to incorporate industry input in the development of the standards and methodologies to manage cybersecurity risks for critical infrastructure. A majority of the 252 respondents to our survey indicated satisfaction with the mechanisms employed by NIST to develop the framework. For example, 186 of 251 respondents[12] indicated that they were "very satisfied" or "satisfied" that NIST provided opportunities for them to provide feedback on the framework during its development process. Similarly, a majority (170 of 187) indicated the workshops hosted by NIST were "very" or "somewhat effective" in engaging industry involvement in development of the

[12]Not all questions were applicable to or otherwise answered by the 252 respondents to our survey. Our results represent those answering each specific question. 251 of the 252 respondents answered the question on their satisfaction or dissatisfaction with the opportunities NIST provided to the respondent to provide feedback on the frameworks content. The respondents answered that they were "very satisfied" or "satisfied" (186); "as satisfied as dissatisfied" (27); "dissatisfied" or "very dissatisfied" (8); and "no basis to judge" (30).

framework.[13] Appendix III provides additional details on survey respondents' evaluations of NIST's collaborative approach to developing the framework.

NIST's Cybersecurity Framework Meets Requirements

NIST implemented the requirements for development of a cybersecurity approach as required by Executive Order 13636 and the Cybersecurity Enhancement Act of 2014.

Executive Order 13636 required NIST to develop among other things a flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. In addition, NIST was to develop a set of standards that align policy, business, and technological approaches to address cyber risks.

Similar to Executive Order 13636, the Cybersecurity Enhancement Act of 2014 authorizes NIST to, among other things, facilitate and support the development of a voluntary set of standards, guidelines, methodologies, and procedures to cost-effectively reduce cyber risks to critical infrastructure. In carrying out these activities, NIST is required to identify, among other things, a flexible, repeatable, performance-based, and cost-effective approach that can be voluntarily adopted to help identify, assess, and manage cyber risks.

To ensure the framework could assist owners and operators with their cyber risk as called for by the executive order and the act, NIST created implementation tiers to allow organizations to determine their cybersecurity risks and identify processes that align to their business approaches to manage those risks. According to the framework, implementation tiers describe how cybersecurity risk is managed by an organization and the degree to which its risk management practices exhibit key characteristics defined in the framework. There are four tiers discussed in the framework, with each one building upon the previous tier: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4).

[13] 187 of the 252 respondents answered the question about the effectiveness of the workshops in engaging industry involvement in the development of the framework. The responses on the effectiveness were: "very effective" (107); "somewhat effective" (63); "slightly effective" (14); "not at all effective" (1); and "no opinion" (2).

Further, based on our analysis, the framework supported and developed by NIST is intended to be:

- **Flexible**: The NIST framework can be modified to an organization's cybersecurity condition and needs. Its processes also provide for a flexible and risk-based implementation of the framework and can be used with a broad array of cybersecurity risk management processes.
- **Repeatable**: Under the framework, organizations are able to create a framework profile to compare their current cybersecurity state to their targeted state. This allows for identification and prioritization of improvement opportunities within the context of a continuous and repeatable process that can be assessed as the organization moves toward its targeted state.
- **Performance-based**: Organizations can use the framework implementation tiers to measure progress for managing cybersecurity risk. Specifically, the implementation tiers allow organizations to track their performance in managing cyber risks from an informal, reactive response to an approach that is agile and risk-informed. For example, in order to track performance, organizations are encouraged to identify their desired tier according to organizational goals and to progress to higher tiers to continue reducing cybersecurity risks.
- **Cost-effective**: The framework's implementation tiers can be used to allow organizations to evaluate their current cyber activities to determine if adoption of cybersecurity risk management practices was sufficient given their mission and regulatory requirements. Additionally, these tiers allow organizations to determine activities that are most important to their critical services, allowing them to prioritize expenditures to maximize the impact of their investment in cybersecurity.

Further, in accordance with the executive order and the act, the framework is voluntary. The framework emphasizes that the information it contains is guidance for individual organizations to use to improve their cybersecurity posture. According to NIST, the implementation tier approach allows for organizations to determine activities that are most important to critical service delivery as well as prioritize expenditures to maximize the impact of their cybersecurity investment.

Federal Entities Are Promoting the Cybersecurity Framework, but DHS Is Not Measuring the Effectiveness of Its Efforts

DHS, SSAs, and NIST have promoted adoption and use of the cybersecurity framework by critical infrastructure owners and operators through a variety of methods. Specifically, DHS established a program, in accordance with Executive Order 13636, to encourage adoption of the framework and has taken a number of actions, including disseminating guidance and working with stakeholders to promote it. However, DHS is not measuring the effectiveness of these actions in order to evaluate the results of its activities and programs. For their part, SSAs for most sectors are developing tailored guidance for implementing the framework in their sectors, and NIST has promoted the framework through public events and its website.

DHS's Voluntary Program Promotes the Framework but Is Not Measuring the Effectiveness of Efforts

DHS, as required by Executive Order 13636, established the Critical Infrastructure Cyber Community (C^3) Voluntary Program in February 2014 to support the voluntary adoption of the framework. The program is intended to enhance critical infrastructure cybersecurity and encourage the adoption of the NIST framework. According to DHS C^3 Voluntary Program officials, one of the program's primary missions is to help SSAs develop guidance for their respective sectors on how to implement the framework.

According to DHS program officials, the C^3 Voluntary Program has framework promotion actions broken out into three phases. Phase 1 is focused on outreach and building awareness of the framework. Phase 2, which was initiated in 2015, involves entity capability building, where DHS promotes the framework to specific types of entities, such as academia, business, and state governments, and highlighting resources to assist in implementing the framework from DHS, other federal agencies, and the private sector. Phase 3 is to facilitate the creation of communities of interest around critical infrastructure cybersecurity.

To promote awareness of the framework during phase 1, DHS launched a website with guidance and links to resources to assist critical infrastructure organizations interested in implementing the framework. DHS also developed a webinar series in January 2015 to provide organizations additional resources for addressing and improving cybersecurity risk management practices. Several past webinars are available on demand on the website. DHS C^3 Voluntary Program officials stated that the 10 webinars conducted as of October 2015 had reached over 1,800 participants. Other outreach and communication tools included reaching out to the 16 critical infrastructure sectors through dozens of conferences and sector meetings. In addition, DHS program officials

stated that they specifically targeted promotional efforts to entities identified as having nationally critical assets. According to officials, as of October 1, 2015, the C^3 Voluntary Program had held 256 briefings since November 2013.

For phase 2, which began in 2015, DHS C^3 Voluntary Program officials stated that they continued to feature the website as a source of resources, such as assessment and cybersecurity tools that assist both federal and private sector stakeholders. Specifically, DHS identified specific resources that may assist entities in aligning their cybersecurity with the five core framework functions;[14] these included resources for academia; business (large, midsize, and small); federal government; and state, local, tribal and territorial governments. For example, to assist in identifying cyber resilience and practices, DHS points to its cyber resiliency review.[15] According to officials, as of October 1, 2015, the resiliency review had been downloaded from the site over 6,500 times. Further, to assist with cybersecurity incident detection, DHS identified the Cyber Information Sharing and Collaboration Program, which is intended to share incident information.[16] The C^3 Voluntary Program also developed a Small and Midsize Business Toolkit, which contains a number of resources to help entities recognize and address cybersecurity risks, including information for startups and a guide to free tools intended to provide cybersecurity assistance. The toolkit, which was posted on the program's website in May 2015, had received over 2,000 downloads as of October 1, 2015, according to officials.

Among the respondents to our survey who indicated that the C^3 Voluntary Program had promoted the framework to them, a majority stated that they were encouraged to use the framework as a result. Specifically, 59

[14]The five framework functions are (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

[15]The cyber resiliency review is a no-cost, voluntary, nontechnical assessment of an organization's operational resilience and cybersecurity practices. The cyber resiliency review may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

[16]The Cyber Information Sharing and Collaboration Program is a no-cost information-sharing partnership between enterprises and DHS that is intended to share situational awareness across critical infrastructure communities, enhance cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverage government and industry subject matter expertise to collaboratively respond to cybersecurity incidents.

responses out of 112 responding to the question indicated that the C3 Voluntary Program promotional activities were "very" or "somewhat" effective in encouraging the use of the framework.[17]

DHS C3 Voluntary Program officials also had worked with the critical infrastructure sectors to develop guidance on how to use the framework. According to DHS program officials, they reached out to the SSAs for 13 of the 16 sectors to assist them in developing and publishing framework implementation guidance for their respective sectors. As of August 2015, program officials stated that the C3 Voluntary Program was assisting SSAs and 10 sectors in developing framework implementation guidance. According to DHS, sector-specific implementation guidance will provide each sector with a tailored approach on how to best use the framework within their industry and make it easier for organizations to (1) use the framework to secure themselves against cyber risk, (2) learn about available tools and resources and approaches that can support cybersecurity risk management and the framework, and (3) gain an understanding of how different sectors and industries are approaching cybersecurity risk management broadly.

DHS C3 Voluntary Program officials stated that they worked to ensure that the DHS guidance to SSAs for updating their sector-specific plans in 2015 included references to the framework. For example, the guidance stated that, when updating the sector-specific plans, SSAs should include activities that the sectors would pursue to advance critical infrastructure security and resilience and how those activities would align with the framework performance goals, among others. According to SSA officials from 15 of the 16 critical infrastructure sectors, their draft 2015 sector-specific plans include information on the framework, such as having framework promotion as a priority or goal.[18]

[17]112 of the 252 respondents answered the question about the effectiveness of DHS promotional efforts in encouraging the use of the framework. The responses on the effectiveness were: "very effective" or "somewhat effective" (59); "slightly effective" or "not at all effective" (36); and "no opinion" (17).

[18]Department of Defense officials representing the SSA for the defense industrial base sector stated that the 2015 draft sector-specific plan does not include information on the framework, and that after discussions with the sector coordinating council there was consensus that sector companies would voluntarily adopt the framework as they determined to be necessary.

According to DHS officials, Phase 3, which is to facilitate the creation of communities of interest around DHS cybersecurity initiatives, began in 2015 and will continue into 2016. DHS officials stated that the intended outcome of this phase is to facilitate the development of self-sustaining communities by continuing to provide forums for information sharing among critical infrastructure owners and operators across the nation. DHS officials stated that phase 3 will be accomplished through a series of regional events, webinars, and development of new resources that promote information sharing and community building.

DHS Is Not Measuring the Effectiveness of Its Framework Promotion Efforts

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. As we have previously reported, according to leading practices in the federal government and in industry, organizations should measure performance in order to evaluate the success or failure of their activities and programs.[19] In addition, the *Standards for Internal Control in the Federal Government*, known as the "Green Book," sets internal control standards for federal entities.[20] Those standards state that internal control monitoring should occur and that the quality of performance over time should be assessed.

DHS C^3 Voluntary Program documentation identifies three metrics that align with program goals: (1) making resources accessible, (2) increasing participation by entities with the C^3 Voluntary Program, and (3) harmonizing approaches with the framework. For these metrics, DHS program officials tracked the number of times resources were accessed on the program website, DHS tools were downloaded, and in-person meetings were conducted to promote the framework. For example, according to DHS officials, since the website launch, it had been viewed over 117,000 times and over 22,000 resources had been downloaded as of October 2015.

[19]GAO, *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings,* GAO-14-713 (Washington, D.C.: Sept. 25, 2014); and *Aviation Weather: Agencies Need to Improve Performance Measurement and Fully Address Key Challenges,* GAO-10-843 (Washington, D.C.: Sept. 9, 2010).

[20]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). 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.

However, none of these metrics indicate the effectiveness of the program's efforts to promote adoption of the framework, and program officials are not otherwise measuring or tracking how effective those efforts or materials are in encouraging individuals and organizations to voluntarily adopt the framework. For example, they are not tracking what percentage of an individual sector they have promoted to or how effective their efforts and guidance are at encouraging the use of the framework by entities within a critical infrastructure sector.

According to DHS C^3 Voluntary Program officials, they have not established these metrics or monitoring mechanisms because DHS has focused on getting as much information and resources out as possible. However, without understanding whether its promotional efforts are effective, the C^3 Voluntary Program may not be able to tailor its products and guidance to effectively encourage adoption of the framework to sector stakeholders. As a result, sectors may not fully benefit from the cybersecurity principles and practices embedded in the framework to mitigate their cybersecurity risk.

Sector-Specific Agencies Promoted the Framework, and Most Decided to Develop Tailored Implementation Guidance

The SSAs for all 16 critical infrastructure sectors identified promoting the framework as a priority for both the SSA and the sector. As a result, the SSAs for all 16 sectors reported that they promoted the framework to their sector. All of the officials representing the SSAs stated that they conducted framework promotional activities, such as presenting the framework at sector- or industry-focused conferences and meetings and meetings of their sector's government coordinating council and sector coordinating councils. In addition, SSA officials from three sectors stated that the framework provides a common taxonomy for discussing risk management within and across sectors, and one official specified that it allowed for a discussion of cybersecurity and risk management with those that may not be security experts.

Promotional efforts and methods varied from sector to sector, including using DHS C^3 Voluntary Program and NIST personnel or resources, speaking at industry conferences, and providing information during sector coordinating council meetings. For example, within the water sector, the Environmental Protection Agency (EPA) and the sector coordinating council are working to understand how entities within the sector are managing risk, including using the framework. Specifically, EPA is supporting the council by providing contractor and subject matter expert support as the council develops metrics and administers a survey to the sector through 2016. EPA officials stated that once the sector

coordinating council receives and analyzes the information received from the survey, it will provide the information to EPA. Another example is the transportation systems sector, where DHS, as the co-SSA, held several promotional activities for Cybersecurity Month in October 2015.

Respondents to our survey who indicated that their SSA promoted use of the framework stated that they were usually encouraged to use the framework as a result. Specifically, 60 of the 82 respondents who responded to that question indicated that SSA promotional activities were "very" or "somewhat" effective in encouraging the use of the framework.[21]

In addition, most SSAs have determined whether to develop framework implementation guidance to address sector-specific risks and operating environments for their sector. Executive Order 13636 requires SSAs to determine whether or not it is necessary for their sector to develop sector-specific framework implementation guidance, and SSAs for 15 of the 16 sectors had made this determination as of October 2015. Of the 15 sectors, 5 have completed and released framework implementation guidance.[22] These framework implementation guides were created by SSAs, sector stakeholders, or a combination of both. For example, the energy sector was the first sector to produce implementation guidance, and the SSA worked with sector stakeholders to produce it. The health care and public health sector had a sector stakeholder provide a crosswalk between their risk framework and the NIST cybersecurity framework. HHS officials representing the health care and public health SSA stated that they are beginning an effort to create further implementation guidance for the sector's seven subsectors.

[21]82 of the 252 respondents answered the question about the effectiveness of SSA promotional efforts in encouraging the use of the framework. The responses on the effectiveness were: "very effective" or "somewhat effective" (60); "slightly effective" or "not at all effective" (16); and "no opinion" (6).

[22]The five sectors with completed and published implementation guidance are Communications, Energy, Healthcare and Public Health, Transportation Systems, and Water and Wastewater Systems.

Seven other sectors have begun drafting implementation guidance.[23] According to officials, these sectors were finalizing their guidance and had involved their sector stakeholders to review it.

For the food and agriculture sector, Department of Agriculture and Food and Drug Administration officials representing the SSAs for the sector stated that they had yet to begin drafting framework implementation guidance and were exploring the creation of sector guidance with their stakeholders.

The Departments of Defense (DOD) and the Treasury, as SSAs for the defense industrial base and financial services sectors, respectively, decided not to create sector-specific framework implementation guidance. According to DOD officials representing the defense industrial base SSA, the department determined, after discussions with the defense industrial base sector coordinating council, that implementation guidance is not needed. The DOD officials stated that there was a consensus within the sector coordinating council that sector companies would voluntarily adopt the framework as they determined to be necessary. Treasury officials representing the SSA for the financial services sector stated that they determined, with input from the sector, that implementation guidance should not be created by Treasury as the financial services SSA. According to the Treasury officials this decision was made in cooperation with the financial services sector coordinating council, and they concluded that implementation guidance was not necessary due to the regulatory structure of the sector.

DHS and the General Services Administration (GSA), which are the co-SSAs for the government facilities sector, have yet to determine if sector implementation guidance should be developed. A GSA official representing the SSA for the government facilities sector stated that there are metrics in the sector-specific plan that will allow GSA to gather information from the sector on its promotional and implementation needs and use that information to best meet the needs of the sector. According to DHS and GSA officials they are waiting until this information is gathered and assessed before discussing whether sector-specific implementation guidance will be needed. DHS and GSA officials do not

[23]The seven sectors drafting implementation guidance are Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste.

have a specific time frame for when the information will be gathered or for when they will make a decision. Without a decision by DHS and GSA under Executive Order 13636 whether guidance is needed to address sector-specific risks and operating environments, implementation of the framework in the government facilities sector may be hindered.

NIST Continues to Promote the Framework

Although not specifically required to by Executive Order 13636 or the Cybersecurity Enhancement Act of 2014, NIST has continued its efforts to promote the framework. NIST encouraged the use of the framework at workshops and public events it hosted and updated its website to provide information on upcoming events and resources related to the framework. Specifically, NIST's website for the framework (www.nist.gov/cyberframework) provides a list of publically available resources to assist entities interested in using the framework. The website includes guidance and tools created by federal and private sector entities for implementing the framework. NIST encourages entities to submit publically available framework implementation guidance that they create so that NIST can provide information about it with the other guidance and tools already highlighted. The website also lists upcoming events where NIST officials will provide framework information and perspectives. Past speaking events from across the country are also listed with links to the event webpage and in some cases the NIST presentation slides.

Respondents to our survey who indicated they had been promoted to by NIST noted that they were encouraged to use the framework as a result. Specifically, 102 responses out of 132 indicated that NIST promotional activities were "very" or "somewhat" effective in encouraging the use of the framework.[24]

Additionally, NIST officials stated they are following implementation of the framework, and a section on the NIST website is dedicated to accounts from entities of how they have implemented the framework. As of October 2015, the section listed an Intel use case for framework implementation

[24]132 of the 252 respondents answered the question about the effectiveness of NIST promotional efforts in encouraging the use of the framework. The responses on the effectiveness were: "very effective" or "somewhat effective" (102); "slightly effective" or "not at all effective" (16); and "no opinion" (14).

and a link to a podcast on how the University of Pittsburgh is using the framework.

NIST officials added that they are seeking feedback on the framework. Specifically, officials stated that they are researching how organizations are applying the framework methodologies, what value they are obtaining from the framework, and what challenges they are facing in implementing the framework. NIST officials stated they are currently focused on the overall effectiveness of the framework for the benefit of those using it to improve future versions. They further stated that they continue to ask stakeholders when an appropriate time to update the framework would be. To solicit this feedback, officials stated that they are asking individuals attending NIST presentations and may issue a request for information through the *Federal Register* regarding whether or not the critical infrastructure community believes that it is necessary to begin updating the framework.

Conclusions

NIST has generally fulfilled its requirements, established in Executive Order 13636 and the Cybersecurity Enhancement Act, to develop a cybersecurity framework for adoption by critical infrastructure sectors. By using a collaborative process for developing the framework, NIST has helped ensure that the resulting guidance, standards, and methodologies, if effectively implemented, can help cost-effectively reduce cyber risks to critical infrastructure.

To facilitate the voluntary adoption of the framework by critical infrastructure owners and operators, DHS, sector-specific agencies, and NIST are taking a variety of actions. However, while DHS has established a program dedicated to encouraging the framework's adoption, without establishing metrics to assess the effectiveness of these efforts, it has less assurance that it is meeting its objectives. In addition, while most SSAs have determined the need for sector-specific guidance to implement the framework, DHS and GSA have yet to meet this requirement for the government facilities sector, which may hinder adoption of the framework in this sector.

Recommendations for Executive Action

To better facilitate adoption of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, we are making the following recommendations:

We recommend that the Secretary of Homeland Security direct officials responsible for the Critical Infrastructure Cyber Community Voluntary Program to develop metrics for measuring the effectiveness of efforts to promote and support the framework.

We also recommend that the Secretary of Homeland Security and the Administrator of GSA set a time frame for determining the need for sector-specific guidance to implement the framework in the government facilities sector.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Transportation, and the Treasury and to GSA and EPA.

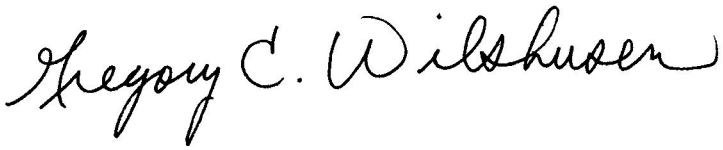
In written comments signed by the Director, Departmental GAO-OIG Liaison Office (reprinted in app. IV), DHS concurred with our two recommendations. DHS agreed with the need to further refine and mature metrics for measuring the effectiveness of efforts to promote and support the framework. DHS also provided details about efforts to track output metrics addressing the C^3 Voluntary Program outreach campaign. The department also stated that it and GSA, as the co-SSAs for the government facilities sector, have taken actions to set a time frame to determine the need for tailored guidance to implement the framework for the sector. DHS stated that the two agencies had reached out to the government facilities government coordinating council to request its input as to whether tailored sector guidance would be desired. In addition, they included making a decision on the necessity of framework implementation guidance on the agenda of the next quarterly government coordinating council meeting, scheduled for January 2016.

In written comments signed by the Administrator (reprinted in app. V), GSA also concurred with the recommendation. GSA stated that a request for information to determine the need for the development of sector-specific framework implementation guidance had been sent to the government coordinating council of the government facilities sector. The administration also stated that it and DHS, as the co-SSAs of the government facilities sector, had scheduled a January 2016 government coordinating council meeting to discuss the results of the request for information to determine the need for sector-specific framework implementation guidance.

In addition, officials from the Departments of Commerce, Health and Human Services, and Homeland Security provided technical comments via e-mail that have been addressed in this report as appropriate. The Departments of Agriculture, Defense, Energy, Transportation, and the Treasury and EPA responded via e-mail that they had no comment on the 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 the 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 me at (202) 512-6244 or wilshuseng@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 VI.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine the extent to which (1) the National Institute of Standards and Technology (NIST) facilitated the development of voluntary standards and procedures to reduce cyber risks to critical infrastructure, and (2) federal agencies promote the standards and procedures to reduce cyber risks to critical infrastructure.

To determine how NIST facilitated the development of voluntary standards and procedures for critical infrastructure, we reviewed and analyzed the actions taken by NIST to develop its *Framework for Improving Critical Infrastructure Cybersecurity*. In addition, we analyzed Executive Order 13636, issued in February 2013, and the Cybersecurity Enhancement Act of 2014, enacted in December 2014, to identify key NIST responsibilities for developing a cybersecurity framework. We analyzed documents and performed interviews with NIST officials to assess its collaborative efforts with industry stakeholders in soliciting input in the development of the framework, including workshops it hosted and the website it set up to disseminate updates on the framework. Specifically, we reviewed documentation and videos of the six workshops hosted by NIST intended to obtain industry, academia, and government representative feedback in the development of the framework, in addition to NIST's two requests for information to the public for input on cybersecurity standards and methodologies. We also analyzed the resulting framework to assess whether NIST had fulfilled its responsibilities under law.

Additionally, to address this objective, we conducted a web-based survey of individuals who (1) provided written comments with contact information in response to a NIST request for information notice or (2) registered for at least one of the workshops hosted by NIST to develop the framework. There were 2,082 individuals in the population that we targeted, and to make the survey as inclusive as possible we sent the survey request to all of them. The questionnaire included questions about the effectiveness of NIST's collaborative efforts in fulfilling requirements to develop the framework using an open and public comment process. To minimize errors arising from differences in how questions might be interpreted and to reduce variability in responses that should be qualitatively the same, we conducted pretests with critical infrastructure representatives over the telephone. Based on feedback from these pretests, we revised the questionnaire to improve the clarity of the questions. An independent survey specialist within GAO also reviewed a draft of the questionnaire prior to its administration.

After completing the pretests, we administered the survey to the NIST workshop attendees and request for information respondents on August 10, 2015, notifying them that our online questionnaire would be activated within a couple of days. On August 18, 2015, we sent a second e-mail message to these individuals, informing them that the questionnaire was available online and providing them with unique passwords and usernames. We collected responses through August 24, 2015. We were able to obtain 252 completed questionnaires, a 12 percent response rate, in the time available for survey fieldwork. Because we do not know if the answers that nonrespondents would have given would materially differ from those that did respond, our results can only represent the views of those who did respond. Their views are not generalizable to the registrant and respondent population as a whole.

To address our second objective, we reviewed and analyzed actions and documentation related to promoting the framework by the nine sector-specific agencies (SSAs) responsible for the 16 critical infrastructure sectors established in Presidential Policy Directive-21, including the Department of Homeland Security (DHS), and NIST. For DHS, we analyzed agency documentation and the website of its Critical Infrastructure Cyber Community (C^3) Voluntary Program to identify the framework promotional guidance and tools provided to the critical infrastructure sectors. Also, we analyzed the metrics and information being used by the DHS C^3 Voluntary Program to determine if DHS could measure the effectiveness of its activities and programs to promote the adoption of the framework. We also interviewed DHS officials on their activities related to the promotion of the framework, including their current and future promotional efforts.

To analyze the promotional efforts by the nine SSAs, we analyzed relevant documentation and interviewed agency officials representing each of the SSAs. We specifically asked each of the SSAs whether promoting the framework was a priority in their draft 2015 sector-specific plans and whether they had decided to develop framework implementation guidance in accordance with Executive Order 13636. See table 5 for the sectors and SSAs included in our review.

Table 5: Critical Infrastructure Sectors in the Scope of This Review and Their Associated Sector-Specific Agency

Sector	Sector-specific agency
Chemical	Department of Homeland Security (DHS)
Commercial facilities	DHS
Communications	DHS
Critical manufacturing	DHS
Dams	DHS
Defense industrial base	Department of Defense
Emergency services	DHS
Energy	Department of Energy
Financial services	Department of the Treasury
Food and agriculture	Departments of Agriculture and Health and Human Services
Government facilities	DHS and General Services Administration
Health care and public health	Department of Health and Human Services
Information technology	DHS
Nuclear reactors, materials, and waste	DHS
Transportation systems	Transportation Security Administration/U.S. Coast Guard (DHS) and Department of Transportation
Water and wastewater systems	Environmental Protection Agency

Source: Presidential Policy Directive 21. | GAO-16-152

To analyze NIST's promotional efforts, we analyzed documentation and interviewed relevant NIST officials. We reviewed the NIST framework website to understand how NIST was informing the public about its public events to promote the framework and presenting entities with guidance to implement the framework for other agencies, sectors, and third parties.

In addition, we surveyed individuals who responded to NISTs requests for information and registered for one of the workshops hosted by NIST for the development of the framework to identify and evaluate the effectiveness of DHS, SSA, and NIST efforts to promote the framework. We also interviewed federal officials from DHS's C^3 Voluntary Program, the nine SSAs representing the 16 critical infrastructure sectors, and NIST regarding their efforts to promote the framework and create sector-specific framework implementation guidance.

We conducted this performance audit from February 2015 to December 2015 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: The Core of NIST's Cybersecurity Framework

The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* is intended to help organizations apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. 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 includes a listing of functions, categories, subcategories, and informative references that describe specific cybersecurity activities the framework identified as common across all critical infrastructure sectors. According to NIST, the framework core represents a common set of activities for managing cybersecurity risk. The framework also states that while it is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use subcategories and informative references that are cost-effective and efficient and that enable them to manage their cybersecurity risk.

Table 6 includes the five functions and 22 categories of the framework core, and Table 7 includes information for one of the categories, asset management, as described in the NIST framework and appendix A of the framework. The information presented here represents how each function has categories, subcategories, and informative references. For more information on the framework, framework core, and categories, see the NIST framework website at www.nist.gov/cyberframework.

Table 6: NIST Cybersecurity Framework Functions and Categories

Function	Category
Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology

Function	Category
Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning Communications Analysis Mitigation Improvements
Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery Planning Improvements Communications

Source: NIST *Framework for Improving Critical Infrastructure Cybersecurity*. | GAO-16-152

Table 7 provides an example of the subcategories and related informative references for a single category of the identify function: asset management.

Table 7: Example of the Information Included for One of the Framework Core Categories

Function	Category	Subcategory	Informative references
Identify	**Asset Management:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried.	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		Software platforms and applications within the organization are inventoried.	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		Organizational communication and data flows are mapped.	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		External information systems are catalogued.	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9

Function	Category	Subcategory	Informative references
		Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

Source: NIST *Framework for Improving Critical Infrastructure Cybersecurity*. | GAO-16-152

Appendix III: Survey Questions and Responses on Development of the Cybersecurity Framework

The following table presents selected questions and responses from our survey of registrants at the National Institute of Standards and Technology's (NIST) workshops for developing the NIST *Framework for Improving Critical Infrastructure Cybersecurity* and commenters who responded to NIST's request for information. There were 2,082 individuals in the population that we targeted, and to make the survey as inclusive as possible we sent the survey request to all of them. We obtained 252 completed questionnaires, a 12 percent response rate, in the time available for survey fieldwork. Because we do not know if the answers that nonrespondents would have given would materially differ from those that did respond, our results represent the views of those who did respond. They are not generalizable to the registrant and respondent population as a whole. Not all questions were applicable to or otherwise answered by the respondents to our survey. Our results represent those answering each specific question.

Table 8: Key GAO Survey Questions and Responses on the Development of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework

Survey question	Responses				Total
To what extent, if at all, did NIST use what you would consider to be a collaborative process to allow you the opportunity to participate in the development of the cybersecurity framework?	Very great extent 184	Moderate extent 38	Little/some/no extent 8	No basis to judge/no opinion 22	**252**
If you attended a workshop, how effective were the workshop(s) in engaging industry involvement in the development of the cybersecurity framework?	Very effective / Somewhat effective 170	Slightly effective 14	Not at all Effective 1	No opinion 2	**187**
How satisfied or dissatisfied are you with the opportunities that NIST provided to you to provide feedback on the content of the framework?	Very satisfied/satisfied 186	As satisfied as dissatisfied 27	Dissatisfied/very dissatisfied 8	No basis to judge 30	**251**
Would you agree or disagree with the following statement, "My comments were adequately reflected in the development of the NIST cybersecurity framework?	Strongly agree/agree 119	Neither agree nor disagree 36	Disagree/strongly disagree 12	No opinion / not applicable 35	**202**
Thinking about the overall process that NIST used for the development of the cybersecurity framework, how much improvement, if any, would be necessary to make the collaboration process more effective?	No improvement / little improvement needed 138	Moderate improvement needed 51	Substantial improvement needed 10	No basis to judge/ no opinion 23	**222**

Source: GAO analysis of survey responses. | GAO-16-152

Appendix IV: Comments from the Department of Homeland Security

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

Homeland Security

November 25, 2015

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Re: Draft Report GAO-16-152, "CRITICAL INFRASTRUCTURE PROTECTION: Measures Needed to Assess Agencies' Promotion of the NIST Cybersecurity Framework"

Dear Mr. Wilshusen:

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's efforts to promote and encourage use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (the "Framework") in the critical infrastructure sectors. To accomplish this, as noted in the report, DHS, specifically the National Protection and Programs Directorate, Office of Cybersecurity and Communications (NPPD/CS&C), implemented the Critical Infrastructure Cyber Community (C^3) Voluntary Program, an innovative public-private partnership that provides critical infrastructure owners and operators with tools and resources to facilitate use of the Framework to manage cyber risks.

The draft report contained two recommendations with which the Department concurs. Specifically GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct officials responsible for the Critical Infrastructure Cyber Community Voluntary Program [C^3 Voluntary Program] to develop metrics for measuring the effectiveness of efforts to promote and support the Framework.

Response: Concur. NPPD/CS&C agrees with the need to further refine and mature its metrics for measuring the effectiveness of efforts to promote and support the Framework,

and has invested significantly in developing timely and relevant output and outcome metrics. At the same time, the voluntary nature of the C^3 Voluntary Program creates challenges in accurately measuring private sector participation. Accordingly, the Department has undertaken efforts to address some of these challenges. For example, the Cyber Resilience Review (CRR) is a free voluntary assessment of an organization's cybersecurity practices. As of June 30, 2015, each question and corresponding maturity level in the CRR is fully mapped to the Framework. After conducting a CRR assessment for a given organization, NPPD/CS&C receives summary information about that organization's cybersecurity posture mapped to the Framework sub-categories. NPPD/CS&C has also developed a database of this summary information across sectors. This database, in turn, can be utilized to identify trends and progress in Framework implementation across and within critical infrastructure sectors. Moreover, this analysis allows provides targeted support that helps individual organizations more effectively implement the Framework.

In addition, NPPD/CS&C continues to track output metrics addressing the C^3 Voluntary Program's outreach campaign, including:

- **Monthly Webinar Participation:** In January 2015, the C^3 Voluntary Program launched a monthly webinar series. Since then, the Voluntary Program has hosted 10 webinars, which have reached over 1,800 people. The webinars have focused on all stakeholder groups including academia, state, local, tribal, and territorial (SLTT) governments, large enterprises, and small and midsize business.

- **Number of Industry Briefings:** Since November 2013, the C^3 Voluntary Program has hosted 256 industry briefings across the 16 critical infrastructure sectors.

- **Number of Regional Events:** Since June 2014, the C^3 Voluntary Program has held four regional events across with a total of 600 attendees. These regional events have also driven increased traffic to SLTT-specific resources. For example, the C^3 Voluntary Program observed a 300% increase in traffic to the "Getting Started for SLTT Governments" web page in the two months immediately following a recent event in Hamilton, NJ event that focused specifically on SLTT governments.

- **Small and Midsize Business Roadshow**: The C^3 Voluntary Program developed a Small and Midsize Business (SMB) Roadshow in conjunction with the DHS Private Sector Office, the U.S. Chamber of Commerce, and a variety of private sector partners. Since June 2015, there have been 12 SMB Roadshow events across the country. SMB Roadshow events are scheduled to continue throughout 2016.

2

The SMB Roadshow events have led to increased interest in the SMB Toolkit, a web-based set of guidance and resources, which has been downloaded over 2,000 times since the SMB Roadshow began. Further, the announcement of a new SMB web page in June 2015 led to an increase in traffic of nearly 20% over the previous month.

The C^3 Voluntary Program is also responsible for working with the Sector-Specific Agencies (SSAs) to develop NIST Framework guidance tailored to each sector. As of November 2015, this guidance has been drafted and is in final review for seven of the sixteen sectors. When completed, NPPD/CS&C will hold after-action meetings with the sectors to discuss the effectiveness of efforts to promote and support the Framework and generate an after-action report focused on the overall value and impact of our efforts. Estimated Completion Date (ECD): June 30, 2016.

Recommendation 2: Set a time frame for determining the need for sector-specific guidance to implement the framework in the government facilities sector.

Response: Concur. GAO notes in its report that SSAs, DHS, and the GSA, specifically with regard to the government facilities sector, had not yet made the decision as to whether or not tailored sector guidance as stated by the Executive Order (EO) 13636 would be developed.

The Federal Protective Service within NPPD has already adopted the approach they have recommended, and more specifically, that SSAs have taken the following actions to not only provide a timeframe but also complete the activities required to arrive at a decision:

- SSAs reached out to the *Government Facilities Government Coordinating Council* (GCC), (note, this sector does not have a Sector Coordinating Council (SCC)), to provide members with the Framework information again, and also to request their input as to whether tailored sector guidance would be desired.

- Responses received from the Government Facilities GCC did not clearly indicate that tailored sector guidance would be needed. The SSAs determined that this would be included as part of the quarterly GCC meeting agenda to facilitate a fuller discussion before making the final decision.

- SSAs provided additional documentation to the GAO team on recent actions noted above.

Supporting documentation substantiating these actions was previously provided to GAO. We request that GAO consider this recommendation resolved and closed.

3

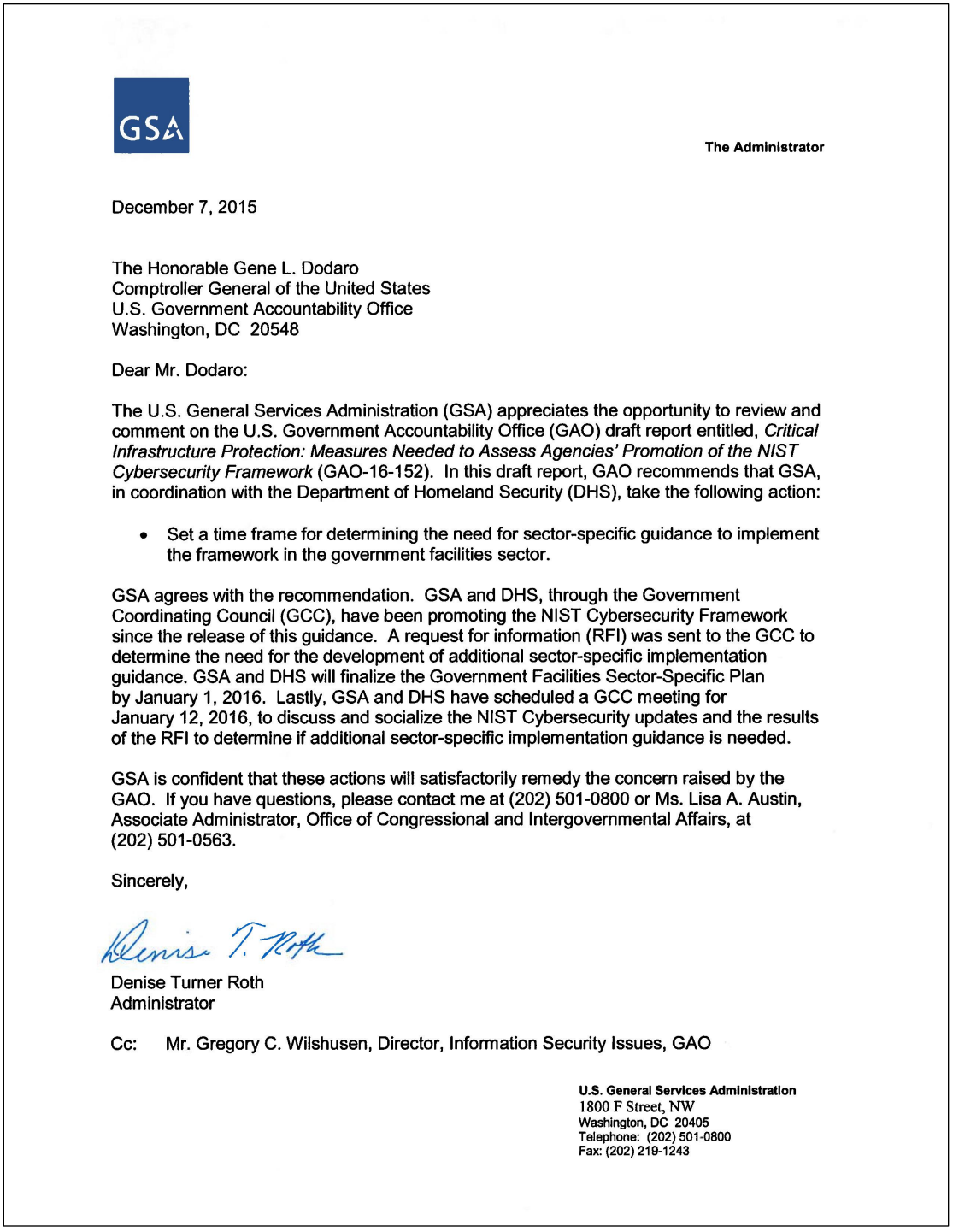
Again, thank you for the opportunity to review and comment on the draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

4

Appendix V: Comments from the General Services Administration



GSA

The Administrator

December 7, 2015

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: Measures Needed to Assess Agencies' Promotion of the NIST Cybersecurity Framework* (GAO-16-152). In this draft report, GAO recommends that GSA, in coordination with the Department of Homeland Security (DHS), take the following action:

- Set a time frame for determining the need for sector-specific guidance to implement the framework in the government facilities sector.

GSA agrees with the recommendation. GSA and DHS, through the Government Coordinating Council (GCC), have been promoting the NIST Cybersecurity Framework since the release of this guidance. A request for information (RFI) was sent to the GCC to determine the need for the development of additional sector-specific implementation guidance. GSA and DHS will finalize the Government Facilities Sector-Specific Plan by January 1, 2016. Lastly, GSA and DHS have scheduled a GCC meeting for January 12, 2016, to discuss and socialize the NIST Cybersecurity updates and the results of the RFI to determine if additional sector-specific implementation guidance is needed.

GSA is confident that these actions will satisfactorily remedy the concern raised by the GAO. If you have questions, please contact me at (202) 501-0800 or Ms. Lisa A. Austin, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

Denise T. Roth

Denise Turner Roth
Administrator

Cc: Mr. Gregory C. Wilshusen, Director, Information Security Issues, GAO

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore, Assistant Director; Sher'rie Bacon; Wilfred Holloway; Lee McCracken; David Plocher; Carl Ramirez; and Jeffrey Woodward made key contributions to this report.

Appendix VII: Accessible Data

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Homeland Security

Page 1

U.S. Department of Homeland Security

Washington, DC 20528

November 25, 2015

Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office

441 G Street NW

Washington, DC 20548

Re: Draft Report GA0-16-152, "CRITICAL INFRASTRUCTURE PROTECTION: Measures Needed to Assess Agencies' Promotion of the NIST Cybersecurity Framework"

Dear Mr. Wilshusen:

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's efforts to promote and encourage use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (the "Framework") in the critical infrastructure sectors. To accomplish this, as noted in the report, DHS, specifically the National Protection and

Programs Directorate, Office of Cybersecurity and Communications (NPPD/CS&C), implemented the Critical Infrastructure Cyber Community (C^3) Voluntary Program, an innovative public-private partnership that provides critical infrastructure owners and operators with tools and resources to facilitate use of the Framework to manage cyber risks.

The draft report contained two recommendations with which the Department concurs. Specifically GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct officials responsible for the Critical Infrastructure Cyber Community Voluntary Program [C^3 Voluntary Program] to develop metrics for measuring the effectiveness of efforts to promote and support the Framework.

Response: Concur. NPPD/CS&C agrees with the need to further refine and mature its metrics for measuring the effectiveness of efforts to promote and support the Framework,

Page 2

and has invested significantly in developing timely and relevant output and outcome metrics. At the same time, the voluntary nature of the C^3 Voluntary Program creates challenges in accurately measuring private sector participation. Accordingly, the Department has undertaken efforts to address some of these challenges. For example, the Cyber Resilience Review (CRR) is a free voluntary assessment of an organization's cybersecurity practices. As of June 30, 2015, each question and corresponding maturity level in the CRR is fully mapped to the Framework. After conducting a CRR assessment for a given organization, NPPD/CS&C receives summary information about that organization's cybersecurity posture mapped to the Framework sub-categories. NPPD/CS&C has also developed a database of this summary information across sectors. This database, in tum, can be utilized to identify trends and progress in Framework implementation across and within critical infrastructure sectors. Moreover, this analysis allows provides targeted support that helps individual organizations more effectively implement the Framework.

In addition, NPPD/CS&C continues to track output metrics addressing the C^3 Voluntary Program's outreach campaign, including:

- Monthly Webinar Participation: In January 2015, the C^3 Voluntary Program launched a monthly webinar series. Since then, the Voluntary Program has hosted 10 webinars, which have reached

over 1,800 people. The webinars have focused on all stakeholder groups including academia, state, local, tribal, and territorial (SLTT) governments, large enterprises, and small and midsize business.

- Number of Industry Briefings: Since November 2013, the C^3 Voluntary Program has hosted 256 industry briefings across the 16 critical infrastructure sectors.
- Number of Regional Events: Since June 2014, the C^3 Voluntary Program has held four regional events across with a total of 600 attendees. These regional events have also driven increased traffic to SLTT-specific resources. For example, the C^3 Voluntary Program observed a 300% increase in traffic to the "Getting Started for SLTT Governments" web page in the two months immediately following a recent event in Hamilton, NJ event that focused specifically on SLTT governments.
- Small and Midsize Business Roadshow: The C^3 Voluntary Program developed a Small and Midsize Business (SMB) Roadshow in conjunction with the DHS Private Sector Office, the U.S. Chamber of Commerce, and a variety of private sector partners. Since June 2015, there have been 12 SMB Roadshow events across the country. SMB Roadshow events are scheduled to continue throughout 2016.

Page 3

The SMB Roadshow events have led to increased interest in the SMB Toolkit, a web-based set of guidance and resources, which has been downloaded over 2,000 times since the SMB Roadshow began. Further, the announcement of a new SMB web page in June 2015 led to an increase in traffic of nearly 20% over the previous month.

The C^3 Voluntary Program is also responsible for working with the Sector-Specific Agencies (SSAs) to develop NIST Framework guidance tailored to each sector. As of November 2015, this guidance has been drafted and is in final review for seven of the sixteen sectors. When completed, NPPD/CS&C will hold after-action meetings with the sectors to discuss the effectiveness of efforts to promote and support the Framework and generate an after-action report focused on the overall value and impact of our efforts. Estimated Completion Date (ECD): June 30, 2016.

Recommendation 2: Set a time frame for determining the need for sector-specific guidance to implement the framework in the government facilities sector.

Response: Concur. GAO notes in its report that SSAs, DHS, and the GSA, specifically with regard to the government facilities sector, had not

yet made the decision as to whether or not tailored sector guidance as stated by the Executive Order (EO) 13636 would be developed.

The Federal Protective Service within NPPD has already adopted the approach they have recommended, and more specifically, that SSAs have taken the following actions to not only provide a timeframe but also complete the activities required to arrive at a decision:

- SSAs reached out to the Government Facilities Government Coordinating Council (GCC), (note, this sector does not have a Sector Coordinating Council (SCC)), to provide members with the Framework information again, and also to request their input as to whether tailored sector guidance would be desired.
- Responses received from the Government Facilities GCC did not clearly indicate that tailored sector guidance would be needed. The SSAs determined that this would be included as part of the quarterly GCC meeting agenda to facilitate a fuller discussion before making the final decision.
- SSAs provided additional documentation to the GAO team on recent actions noted above.

Supporting documentation substantiating these actions was previously provided to GAO. We request that GAO consider this recommendation resolved and closed.

Page 4

Again, thank you for the opportunity to review and comment on the draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Text of Appendix V: Comments from the General Services Administration

Page 1

December 7, 2015

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: Measures Needed to Assess Agencies' Promotion of the NIST Cybersecurity Framework (GA0-16-152). In this draft report, GAO recommends that GSA, in coordination with the Department of Homeland Security (OHS), take the following action:

- Set a time frame for determining the need for sector-specific guidance to implement the framework in the government facilities sector.

GSA agrees with the recommendation. GSA and OHS, through the Government Coordinating Council (GCC), have been promoting the NIST Cybersecurity Framework since the release of this guidance. A request for information (RFI) was sent to the GCC to determine the need for the development of additional sector-specific implementation guidance. GSA and OHS will finalize the Government Facilities Sector-Specific Plan by January 1, 2016. Lastly, GSA and OHS have scheduled a GCC meeting for January 12, 2016, to discuss and socialize the NIST Cybersecurity updates and the results of the RFI to determine if additional sector-specific implementation guidance is needed.

GSA is confident that these actions will satisfactorily remedy the concern raised by the GAO. If you have questions, please contact me at (202) 501-0800 or Ms. Lisa A. Austin, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

Denise Turner Roth

Administrator

Cc: Mr. Gregory C. Wilshusen, Director, Information Security Issues, GAO

U.S. General Services Administration

1800 F Street, NW

Washington, DC 20405

Telephone: (202) 501-0800

Fax: (202) 219-1243

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, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

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