United States Government Accountability Office

Report to Congressional Requesters

OCTOBER 2017

CRITICAL INFRASTRUCTURE PROTECTION

DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning

Accessible Version

GAO-18-62

October 2017

CRITICAL INFRASTRUCTURE PROTECTION

DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning

GAO Highlights

Highlights of GAO-18-62, a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure includes cyber and physical assets and systems across 16 different sectors whose security and resilience are vital to the nation. The majority of critical infrastructure is owned and operated by the private sector. Multiple federal entities, including DHS, work with infrastructure owners and operators to assess their risks.

GAO was asked to review DHS's risk assessment practices for critical infrastructure. This report describes:(1) DHS's risk assessment practices in 3 of 16 critical infrastructure sectors and private sector representatives' views on the utility of this risk information, and (2) how this risk information influences DHS's strategic planning and private sector outreach.

GAO selected 3 of 16 sectors–Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Transportation Systems–to examine based on their varied regulatory structures and industries. GAO reviewed DHS guidance related to infrastructure protection, the QHSR and DHS Strategic Plan, and plans for the selected critical infrastructure sectors. GAO interviewed DHS officials responsible for critical infrastructure risk assessments, and the owner and operator representatives who serve as chairs and vice-chairs of coordinating councils for the 3 selected sectors. Information from the 3 sectors is not generalizable to all 16 sectors but provides insight into DHS's risk management practices.

GAO provided a draft of this report to DHS and relevant excerpts to the council representatives interviewed during this review. Technical comments provided were incorporated as appropriate.

View GAO-18-62. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) primarily conducts assessments for each of the three elements of risk—threat, vulnerability, and consequence—for critical infrastructures from the three sectors GAO reviewed—Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Transportation Systems. In limited circumstances, DHS generates risk assessments that both incorporate all three elements of risk and cover individual or multiple subsectors.

- **Threat**: DHS's Office of Intelligence and Analysis assesses threats—natural or manmade occurrences, entities, or actions with the potential to cause harm, including terrorist attacks and cyberattacks—and disseminates this information to critical infrastructure owners and operators. For example, the Transportation Security Administration provides threat intelligence to mass transit security directors and others through joint classified briefings.
- **Vulnerability:** DHS officials provide various tools and work directly with owners and operators to assess asset and facility vulnerabilities—physical features or operational attributes that render an asset open to exploitation, including gates, perimeter fences, and computer networks. For example, DHS officials conduct voluntary, asset-specific vulnerability assessments that focus on physical infrastructure during individual site visits.
- **Consequence:** DHS officials also assess consequence— the effect of occurrences like terrorist attacks or hurricanes resulting in losses that impact areas such as public health and safety, and the economy—to better understand the effect of these disruptions on assets.

These assessments help critical infrastructure owners and operators take actions to improve security and mitigate risks. Six private sector representatives told GAO that threat information is the most useful type of risk information because it allows owners and operators to react immediately to improve their security posture. For example, one official from the Transportation Systems sector said that government threat information is credible and is critical in supporting security recommendations to company decision-makers.

DHS uses the results of its risk assessments to inform the department's strategic planning and to guide outreach to infrastructure owners and operators. Critical infrastructure risk information is considered within DHS's strategic planning. Specifically, according to DHS officials, risk information informs the Department's Quadrennial Homeland Security Review (QHSR)—a process that identifies DHS's critical homeland security missions and its strategy for meeting them. DHS also uses risk information to guide outreach to critical infrastructure owners and operators. For example, DHS officials annually prioritize the most critical assets and facilities nationwide and categorize them based on the severity of the estimated consequences of a significant disruption to the asset or facility. DHS officials then use the results to target their assessment outreach to the infrastructure owners and operators categorized as higher risk. DHS officials also told GAO that they use risk information after an incident, such as a natural disaster, to quickly identify and prioritize affected infrastructure owners and operators to help focus their response and recovery assistance outreach.

Contents

Tables

Figures

Abbreviations

CI	critical infrastructure
CIPAC	Critical Infrastructure Partnership Advisory Council
CS&C	Office of Cybersecurity and Communications
CSA	Cyber Security Advisor
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
GCC	government coordinating council
HSIN-CI	Homeland Security Information Network for Critical Infrastructure
HSNRC	Homeland Security National Risk Characterization
I&A	Office of Intelligence and Analysis
ICC	Intelligence Coordination Center
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team
IP	Office of Infrastructure Protection
IST	Infrastructure Survey Tool
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act of 2002
NCATS	National Cybersecurity Assessment and Technical Services
NCCIC	National Cybersecurity and Communications Integration Center
NCIPP	National Critical Infrastructure Prioritization Program
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NRC	U.S. Nuclear Regulatory Commission
OCIA	Office of Cyber and Infrastructure Analysis
PPD	Presidential Policy Directive
PSA	Protective Security Advisor
QHSR	Quadrennial Homeland Security Review
SCC	sector coordinating council
SOPD	Sector Outreach and Programs Division
SSA	sector-specific agency
TSA	Transportation Security Administration
TSA-OI	Transportation Security Administration – Office of Intelligence
TSSRA	Transportation Sector Security Risk Assessment
US-CERT	U.S Computer Emergency Readiness Team

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

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

October 30, 2017

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The nation's critical infrastructure (CI) includes physical and cyber assets and systems that are so vital to the United States that their incapacity or destruction could have a debilitating impact on national security, public health and safety, or the economy. CI provides the essential services—such as transportation, water, and energy—that underpin American society, and protecting CI assets and systems is a national security priority. The risk environment for CI ranges from natural disasters to cyberattacks by foreign malicious actors. Additionally, while companies have increasingly sought to gain efficiencies by connecting their physical and cyber business systems, the convergence between these systems creates new opportunities for potential cyber attackers to access these systems. Because the majority of CI is owned and operated by the private sector, it is vital that the public and private sectors work together to protect these assets and systems.

The Department of Homeland Security (DHS) coordinates the overall federal effort for national CI protection.[1] As part of its CI protection responsibilities, DHS is to conduct CI risk assessments and integrate relevant information and analyses to identify priorities for protective and support measures to be implemented by DHS, other federal agencies,

[1]The Homeland Security Act of 2002 created DHS and gave the agency responsibilities for coordinating national CI protection efforts. See generally Pub. L. No. 107-296, tit. II, 115 Stat. 2135, 2145 (2002), as amended; 6 U.S.C. § 121.

state and local government agencies and authorities, the private sector, and other entities.[2]

DHS developed the first version of the National Infrastructure Protection Plan (NIPP) in 2006 and updated it in 2009 and 2013. The NIPP describes a voluntary partnership model as the primary means of coordinating government and private sector efforts to protect CI.[3] It provides a framework for developing and implementing a coordinated national effort to protect CI within 16 distinct sectors.[4] The sectors vary in structure, with some sectors, such as the chemical and nuclear sectors, having more regulatory oversight governing their respective security issues in addition to the voluntary partnership model. Other sectors, such as commercial facilities and critical manufacturing, have less regulatory oversight, according to DHS officials.

As part of the partnership structure, each sector has a designated Sector-Specific Agency (SSA), a federal department or agency that serves as the lead coordinator for security and resilience programs and activities for their respective sector.[5] Each sector also has a government coordinating council (GCC), consisting of representatives from various levels of government, and a sector coordinating council (SCC) consisting of owner-operators of these critical assets or members of their respective trade

[2]The Homeland Security Act, as amended, established the position of Assistant Secretary for Infrastructure Protection. See 6 U.S.C. § 121. The Secretary of Homeland Security has delegated critical infrastructure protection responsibilities under the Act to the Under Secretary for the National Protection and Programs Directorate.

[3]Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, D.C.: December 2006). DHS updated the NIPP in January 2009 to include greater emphasis on resiliency; *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency (*Washington, D.C.: January 2009). DHS updated the NIPP in December 2013 to emphasize the integration of physical and cybersecurity into the risk management framework; *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[4]The 16 critical infrastructure sectors are 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.

[5]DHS, *2013 NIPP*.

associations.[6] According to the NIPP, SCCs serve as principal collaboration points between the government and private sector owners and operators for CI security and resilience policy coordination and related sector-specific activities.[7] For example, the NIPP calls for the individual sector-specific agencies, working with relevant sector representatives, to develop sector-specific plans to, among other things, describe how the sector will identify and prioritize its critical assets, including cyber assets, and define approaches the sector will take to assess risks and develop programs to protect these assets.

Focusing on cyber infrastructure, DHS's National Cybersecurity and Communications Integration Center (NCCIC) provides a central place for federal and private-sector organizations to coordinate efforts to address cyber threats and respond to cyber attacks.[8] The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks.

Due to the cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we continue to designate information security as a government-wide high-risk area in our most recent biennial report to

[6]GCCs coordinate strategies, activities, policy, and communications across government entities within each sector and consist of representatives across various levels of government (i.e., federal, state, local, and tribal) as appropriate. SCCs are self-organized, self-run, and self-governed private sector councils that interact on a wide range of sector-specific strategies, policies, activities, and issues. SCC membership can vary from sector to sector, but is meant to be representative of a broad base of owners, operators, associations, and other entities—both large and small—within the sector.

[7]The term "owners and operators" is used here instead of "private sector representatives" because publicly owned facilities are included in DHS's outreach efforts. However, later in this report we refer to the six SCC chairs and vice-chairs from our selected sectors as "private sector representatives" because they work for either private sector companies or trade associations. While we recognize that the sectors they represent can include publicly owned facilities, we use the term "private sector representatives" to help distinguish the opinions of the SCC chairs and vice-chairs from those of SSA and other government officials in this report.

[8]National Security Presidential Directive/NSPD-54 (Homeland Security Presidential Directive/HSPD-23), issued on January 8, 2008, established the Comprehensive National Cybersecurity Initiative, which is aimed at safeguarding federal civilian executive branch government information systems. Pursuant to the directive, DHS established the NCCIC in October 2009.

Congress, a designation we have made in each report since 1997.[9] In 2003, we expanded this high-risk area to include, the protection of critical cyber infrastructure. While DHS has made progress in this area, challenges remain. For example, we reported in November 2015 that while SSAs had taken actions to mitigate cyber risks for their respective CI sectors, most SSAs had not developed metrics to measure and report on the effectiveness of their mitigation activities. We also reported that DHS needed to assess whether its efforts to share information on cyber threats, incidents, and countermeasures with federal and non-federal entities are useful and effective.[10]

Over the last several years, DHS has taken actions to assess vulnerabilities at CI facilities and within groups of related infrastructure, regions, and systems.[11] We reported in September 2014 that DHS offices and components had conducted or required thousands of vulnerability assessments of CI from October 2010 to September 2013, and that DHS needed to enhance integration and coordination of these efforts.[12] DHS concurred with the six recommendations in our report, including our recommendation that it take steps to better coordinate vulnerability

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

[10]We recommended that certain sector-specific agencies collaborate with sector partners to develop performance metrics and determine how to overcome challenges to reporting the results of their cyber risk mitigation activities. Two of these agencies–the Departments of Homeland Security and Transportation–concurred with our recommendation while the Department of Treasury and the Environmental Protection Agency both generally agreed with our recommendation. Two agencies–the Departments of Agriculture and Health and Human Services– did not comment on our recommendations. In 2015, each of the sectors for which these agencies served as SSA or co-SSA, updated its sector-specific plan with information regarding measuring the effectiveness of sector activities. However, as of September 2017, none of these SSAs have provided metrics data demonstrating their progress toward monitoring the effectiveness of their respective sector's cybersecurity activities. We will continue to monitor the status of each SSA's efforts to address these recommendations. See GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[11]According to the NIPP, vulnerabilities may be associated with physical factors (e.g., no barriers or alarm systems); cyber factors (e.g., lack of a firewall); or human factors (e.g., untrained guards). A vulnerability assessment involves the evaluation of specific threats to the asset, system, or network under review to identify areas of weakness that could result in consequences of concern.

[12]GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts,* GAO-14-507 (Washington, D.C.: Sept. 15, 2014).

assessments both within DHS and other CI partners, as appropriate. DHS has taken steps to address this particular recommendation, which are discussed later in this report.

Given the importance of CI to the nation's economy and well-being, you requested that we review DHS's efforts to assess risks to CI. This report addresses the following questions:

1. What are DHS's risk assessment practices in selected CI sectors and what are private sector representatives' views on the utility of this risk information?
2. How, if at all, does CI risk information influence DHS's strategic planning and private sector outreach?

To address our first objective, we reviewed agency documents and interviewed relevant officials to identify DHS's physical and cyber risk assessment practices for 3 of the 16 CI sectors: Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Transportation Systems.[13] We selected these three sectors because they were sectors for which DHS serves as the SSA or the co-SSA. DHS's Office of Infrastructure Protection is the lead component within DHS for the Critical Manufacturing and nuclear sectors, and DHS shares SSA responsibilities with the Department of Transportation for the Transportation Systems sector. These three sectors also have varying levels of federal regulation. Specifically, we chose the Critical Manufacturing sector because according to DHS, the majority of the assets in this sector are privately owned and operated by companies that have minimal interaction with the federal government and other regulatory entities and includes the manufacturing industries that are the most crucial for the continuity of other critical sectors and has significant national economic implications. Additionally, we selected the nuclear sector because all of the facilities in the sector are subject to federal security requirements, which allowed us to observe how a regulatory environment may affect DHS's provision of risk information to CI owners and operators. We also included the Transportation Systems sector because portions of it are regulated and DHS regularly conducts sector-wide complete risk assessments for this

[13]The Nuclear Reactors, Materials, and Waste sector is herein referred to as the nuclear sector.

sector.[14] The information gathered from these three selected sectors is not generalizable to all 16 sectors but does provide insight into how DHS's risk assessment information is used for a variety of CI. We reviewed laws and guidance regarding DHS's roles and responsibilities relating to physical and cyber CI risk assessment practices including the Homeland Security Act of 2002, as amended, and Presidential Policy Directive/PPD-21 (PPD-21). We also examined DHS's National Infrastructure Protection Plan, DHS's Risk Management Fundamentals, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework to identify common practices for generating risk-related information.

To characterize the risk information DHS distributed to CI owners and operators in the three selected sectors, we identified the products and activities associated with each risk element—threat, vulnerability, and consequence. Additionally, to identify cybersecurity products and services distributed by DHS, we reviewed our previous work on DHS's NCCIC to categorize NCCIC products and services.[15] We interviewed DHS officials from the National Protection and Programs Directorate (NPPD), the Office of Policy, the Office of Intelligence and Analysis (I&A), and the Transportation Security Administration (TSA) to discuss DHS's roles and responsibilities related to assessing risks for CI. We also interviewed the SCC chair and vice-chair from each of the three selected sectors to determine how DHS risk assessment information may be used by owners and operators, for a total of six SCC representatives. The information gathered from interviews with these private sector representatives is not generalizable to each of their respective sectors but provides insights into how the asset owners use risk information provided by DHS.

To address our second objective, we reviewed and analyzed DHS planning products, such as the Quadrennial Homeland Security Review (QHSR) and strategic plans for the individual CI sectors, to determine which documents included elements that capture CI risk data for strategic

[14]Complete risk assessments are evaluations wherein the methodology assesses all three elements of risk—threats, vulnerabilities, and consequences. Additional information on each element is discussed later in this report.

[15]GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

decision-making purposes.[16] We examined DHS policies and guidance related to administering risk assessments and obtained information from NPPD officials to determine how DHS may use risk information when prioritizing outreach activities within the three selected sectors.[17] We also reviewed our past work on DHS strategic planning and DHS's actions to address open recommendations and interviewed DHS's Office of Policy to discuss the next iteration of the QHSR due to be released in fiscal year 2018.[18]

We conducted this performance audit from July 2016 to October 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Presidential Directives Define DHS's CI Security Mission

In February 2013, the White House released Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, directing DHS to coordinate the overall federal effort to promote the security and resilience

[16]We also reviewed supporting documents for the QHSR, including the Homeland Security National Risk Characterization.

[17]Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). We reviewed policies and guidance including PPD-21; Executive Order 13636—Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013); National Institute for Standards and Technology—*Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014); and the NIPP.

[18]GAO, *Quadrennial Homeland Security Review: Improved Risk Analysis and Stakeholder Consultations Could Enhance Future Review*, GAO-16-371 (Washington, D.C.: Apr. 15, 2016).

of the nation's CI from all hazards.[19] Within DHS, NPPD has been delegated the responsibility for the security and resilience of the nation's CI, and within NPPD, the Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on CI issues.

Also in February 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," citing repeated cyber intrusions into critical infrastructure as demonstrating the need for improved cybersecurity.[20] Among other things, the order addressed the need to improve cybersecurity information sharing and collaboratively develop risk-based standards; stated U.S. policy to increase the volume, timeliness, and quality of cyber threat information shared with private sector entities; directed the federal government to develop a technology-neutral cybersecurity framework to help CI owners and operators identify, assess, and manage cyber risk; and required DHS to use a consultative process to identify infrastructure in which a cybersecurity incident could result in catastrophic consequences.

The National Infrastructure Protection Plan Provides a Framework for Managing Risk

The NIPP sets forth a risk management framework and outlines DHS's roles and responsibilities regarding CI security and resilience.[21] As shown in Figure 1, the NIPP risk management framework is a planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risk; implementing

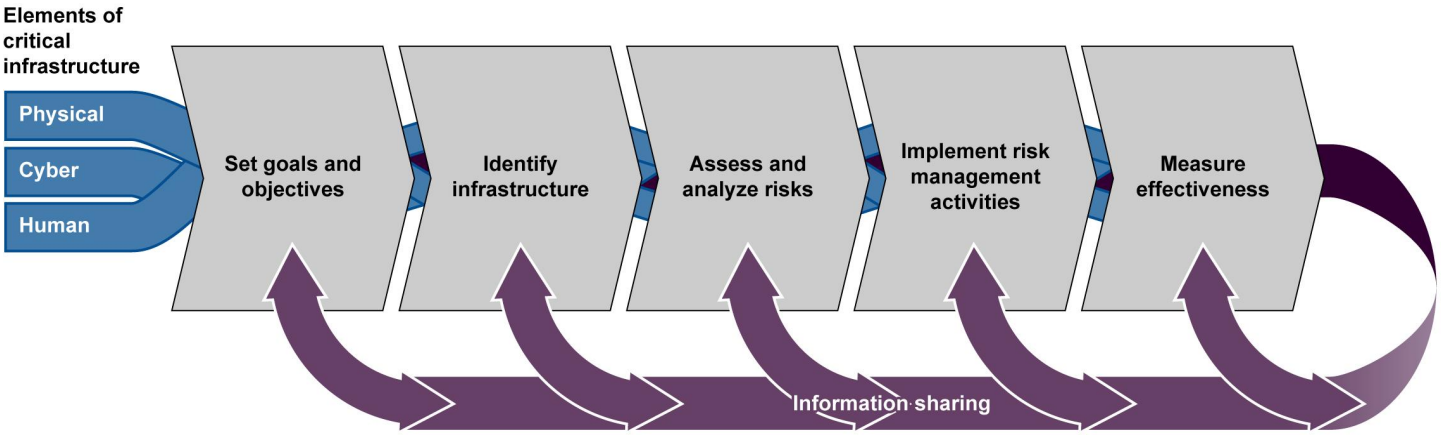
[19]PPD-21, which was developed to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience is an area that may be included in vulnerability assessments to determine the extent to which CI is prepared to withstand and recover from disruptions such as exposure to a given hazard or incidents arising from the deliberate exploitation of vulnerabilities.

[20]Exec. Order No. 13636, 78 Fed. Reg. 11,737 (Feb. 19, 2013). Executive Order 13800, issued May 11, 2017, directs the Secretary of Homeland Security, in coordination with the heads of all appropriate departments and agencies, to among other things, identify authorities and capabilities that agencies could use to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 to be at greatest risk of attack that could result in catastrophic results on public health or safety, economic security, or national security. See Exec. Order No. 13800, 82 Fed. Reg. 22,391 (May 16, 2017).

[21]See DHS, *2013 NIPP*.

protective programs and resiliency strategies; and measuring performance and taking corrective action.[22]

Figure 1: The National Infrastructure Protection Plan's Critical Infrastructure Risk Management Framework



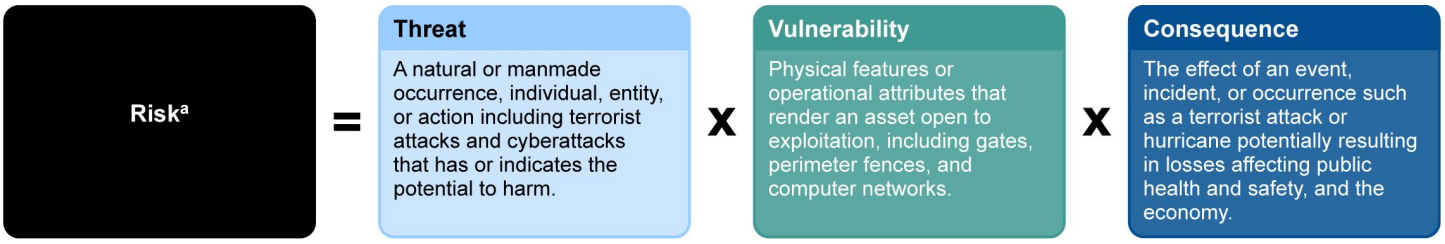
Source: Department of Homeland Security National Infrastructure Protection Plan 2013. | GAO-18-62

The risk management framework calls for public and private CI partners to conduct risk assessments to understand the most likely and severe incidents that could affect their operations and communities, and use this information to support planning and resource allocation in a coordinated manner. According to the NIPP, the risk management framework is also intended to inform how decision makers take actions to manage risk, which according to DHS, is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result, as shown in figure 2.[23]

[22]Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

[23]See DHS, *2013 NIPP*.

Figure 2: Three Elements of Homeland Security Risks Related to Infrastructure Protection



Source: GAO analysis of the Department of Homeland Security's National Infrastructure Protection Plans (2009 and 2013). | GAO-18-62

[a]Risk Management Fundamentals, Homeland Security Risk Management Doctrine (Washington, D.C.: April 2011). As noted in DHS's Risk Management Fundamentals Doctrine, risk is generally recognized as a function of threats, vulnerabilities, and consequences—elements that may explicitly be considered for many homeland security risks, such as those related to infrastructure protection. The doctrine notes that analysts should be careful when calculating risk by multiplying threats, vulnerabilities, and consequences, especially for terrorism, because interdependencies between the three variables, or poorly executed mathematical operations, can lead to inaccurate results.

Multiple DHS Offices Are Involved in CI Risk Assessment Activities

Multiple DHS offices conduct or assist with risk assessments for CI, including the Office of Cybersecurity and Communications (CS&C), Office of Infrastructure Protection, and Office of Cyber and Infrastructure Analysis (OCIA). The Office of Infrastructure Protection and CS&C both use voluntary programs to introduce risk-related tools intended to identify gaps in infrastructure security. These include voluntary security surveys and vulnerability assessments carried out by DHS's Protective Security Advisors (PSA) and Cyber Security Advisors (CSA). PSAs are CI protection and security specialists responsible for assisting asset owners and operators with protection strategies of physical assets, and CSAs are cybersecurity specialists responsible for helping to bolster owners' and operators' cyber assessment capabilities.[24] Both types of advisors use their respective assessment tools to work with CI stakeholders to develop

[24]DHS's PSA program was established in 2004 to assist with ongoing state and local CI security efforts by establishing and maintaining relationships with state Homeland Security Advisors, State Critical Infrastructure Protection stakeholders, and other state, local, tribal, territorial, and private-sector organizations. PSAs are to support the development of the national risk picture by conducting vulnerability and security assessments to identify security gaps and potential vulnerabilities in the nation's most critical infrastructures. As of October 2017, DHS had 82 PSAs serving in 74 districts in 50 states and Puerto Rico. Similarly, according to DHS, 12 CSAs have been employed to serve as advisors on all DHS cyber programs and cybersecurity activities including select cyber evaluations, cyber preparedness activities, and incident coordination activities as of August 2017.

measures intended to make assets more resilient. Other DHS offices with CI risk assessment responsibilities include DHS's Office of Intelligence and Analysis, U.S. Coast Guard, and TSA.

PPD-21 and the NIPP also call for other federal departments and agencies to play a key role in CI security and resilience activities in their capacity as SSAs. In general, an SSA is a federal department or agency responsible for, among other things, supporting the security and resilience programs and related activities of designated CI sectors.[25] DHS is designated as the SSA or co-SSA for 10 of the 16 CI sectors, and has assigned its SSA duties to multiple entities including the Office of Infrastructure Protection, TSA, Coast Guard, and Federal Protective Service. For our three selected sectors, DHS's Sector Outreach and Programs Division (SOPD), within the Office of Infrastructure Protection, serves as the SSA for the Critical Manufacturing and nuclear sectors. DHS's TSA and the U.S. Department of Transportation serve as co-SSAs for the Transportation Systems sector. Other federal agencies or departments external to DHS serve as the SSAs for the remaining 6 sectors for which DHS is not designated as the SSA or co-SSA. Figure 3 provides descriptions of the 16 sectors, identifies the SSA of each sector, and highlights the three selected sectors.

[25]The 2006 NIPP listed 17 critical infrastructure sectors, consistent with Homeland Security Presidential Directive/HSPD-7, which directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across critical infrastructure sectors (Washington, D.C.: Dec. 17, 2003). In 2008, DHS established an 18th sector—critical manufacturing. Presidential Policy Directive/PPD-21 revoked HSPD-7 and realigned the 18 sectors into 16 critical infrastructure sectors, but also provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

Figure 3: Critical Infrastructure Sectors and Their Sector-Specific Agencies as Defined in Presidential Policy Directive-21 and the 2013 National Infrastructure Protection Plan

Source: GAO analysis of Presidential Policy Directive-21 and DHS's National Infrastructure Protection Plan 2013; Art Explosion (clip art). | GAO-18-62

Risk Assessment Activities Vary Based on Sector's Regulatory Environment

For some sectors, assets or operations are regulated by federal or state regulatory agencies that possess unique insight into the risk mitigation strategies of the CI they oversee. These regulators, who may not serve as the designated SSA for the sector, help establish safety and security protocols for the industries they regulate and ensure sector resilience through the policymaking and oversight processes. For example, the Nuclear Regulatory Commission, in its role as the regulatory agency for the nuclear sector, conducts threat assessments to help protect against acts of radiological sabotage and to prevent the theft of special nuclear material.[26] Additionally, pursuant to the Maritime Transportation Security Act of 2002, DHS must use risk management in specific aspects of its homeland security efforts. For example, the Coast Guard and other port security stakeholders are required to carry out certain risk-based tasks, including assessing risks and developing security plans for ports, facilities, and vessels.[27]

NIST Framework Provides Voluntary Cybersecurity Guidance

DHS is also involved in promoting and supporting the adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity. In accordance with requirements in Executive Order 13636, as discussed above, this framework provides voluntary standards and procedures for CI organizations to follow to better manage and reduce cybersecurity risk, and is designed to foster communication among CI stakeholders about cybersecurity management.

[26]The Nuclear Regulatory Commission uses a threat-based model to prescribe requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used.

[27]See Pub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2068-72 (2002); 46 U.S.C. §§ 70102-03.

In December 2015, we reported that SSAs and NIST had promoted and supported adoption of the cybersecurity framework in the CI sectors.[28] For example, in February 2014, 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. We also reported that DHS did not have metrics to measure the success of these program efforts, and recommended that DHS develop metrics to understand the effectiveness of their promotion activities. DHS concurred, and in December 2016 DHS officials stated that they plan to continue to work with SSA partners and NIST to determine how to develop measurement activities and collect information on the voluntary program's outreach and its effectiveness in promoting and supporting the cybersecurity framework. We are currently conducting a review that will identify actions taken by relevant federal entities including NIST, DHS, and other SSAs to promote the adoption of the cybersecurity framework. We will continue to monitor the voluntary program's outreach as well as DHS's efforts to measure its effectiveness in promoting and supporting the cybersecurity framework.

Efforts to Increase Operational Efficiency among CI Assets Result in Physical and Cyber Security Convergence and Expand the Potential for Cyberattacks

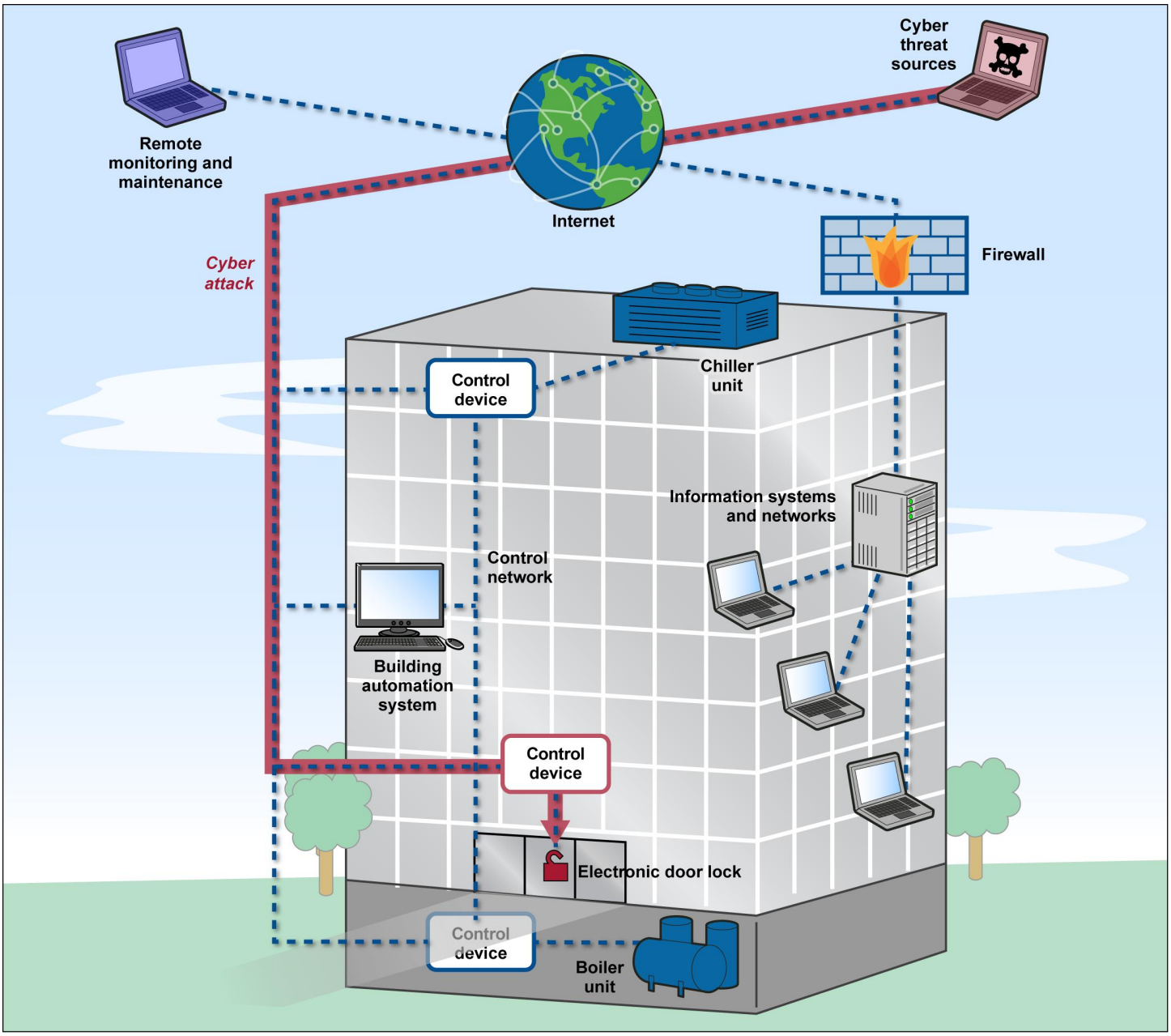
The convergence of physical and cyber security is a major challenge for owners and operators of CI as more physical processes and systems are connected to Internet-enabled networks to improve operational efficiency, according to DHS officials. For example, facilities may make use of automated building control systems to control certain processes or functions, such as security, lighting, or heating, ventilation, and air conditioning (HVAC). These control systems increase efficiency and optimize operational performance by reducing the need for manual controls and adjustments.[29] Building control systems and the devices

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

[29]Building automation systems, also known as energy management control systems, provide centralized control through the use of software and hardware to monitor and adjust building systems, such as climate control and lighting. A building automation system is intended to optimize the integrated performance of the individual components of the system.

within them are often configured with connections to the Internet. These Internet connections allow the systems to be accessed remotely for control and monitoring and, for example, to receive software patches and updates. Figure 4 illustrates how a facility's HVAC and security systems are managed through a building automation system and operated over a control network. In this example, the information systems and networks are protected by a firewall—a cybersecurity countermeasure—while the control network and its devices have direct Internet connectivity without going through a firewall, potentially allowing a cyber-attacker to control the building's electronic door locks.

Figure 4: Example of Convergence of Physical and Cyber Threats to Critical Infrastructure



Source: GAO; Art Explosion (clip art). | GAO-18-62

Broader examples of these types of networked systems include electrical grids and water distribution systems, as well as control systems that operate chemical manufacturing processes, monitor natural gas pipelines,

and control petroleum refineries. Depending on the cyberattack, there is potential to cause a disruption to specific infrastructure operations and a possibility that such an event could lead to cascading effects within the sector or to other sectors in the economy. According to a 2015 DHS report on cyber-physical infrastructure risks, greater connectivity among technologies that connect cyber systems to physical systems expands the potential for cyberattack by malicious actors. The growing convergence of these systems mean that exploited cyber vulnerabilities can result in physical consequences, as well.[30]

DHS Primarily Assesses the Three Elements of Risk Separately for CI, and Private Sector Representatives from Selected Sectors Report Threat Information Most Valuable

DHS primarily assesses the three elements of risk–threat, vulnerability, and consequence–separately for individual CI assets and sectors. According to DHS officials, these assessments help critical infrastructure owners and operators take actions to improve security and mitigate risks. However, according to SCC representatives from three selected sectors, timely and actionable threat assessment data is the most useful type of risk information. In limited circumstances, DHS generates risk assessments that collectively incorporate all three elements of risk which selected SCC representatives found of limited use for their sectors' infrastructure protection efforts due to the amount of time it takes to finalize the assessment data, the inclusion of risk scenarios that are not likely to occur, and the results not being applicable to individual assets.

DHS Shares Threat Assessment Information with CI Owners and Operators

Threat Information Products Help Make Critical Infrastructure in Selected Sectors More Secure and Resilient

DHS's Office of Intelligence and Analysis (I&A) compiles information from a variety of classified and unclassified sources to develop threat-related

[30]Department of Homeland Security, The Future of Smart Cities, Cyber-Physical Infrastructure Risk (Washington, D.C.: Aug. 2015).

analytic products for each of the 16 CI sectors. I&A's threat assessment efforts include classified briefings intended to help CI owners and operators manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient. DHS typically shares these products via its Homeland Security Information Network for Critical Infrastructure (HSIN-CI) platform. I&A also partners with sector-specific agencies to engage asset owners and operators directly during biweekly classified threat briefings to share threat data. During these meetings, both I&A officials and CI owners and operators take this opportunity to identify potential threat-related risks that may inform future I&A threat products.

The Homeland Security Information Network–Critical Infrastructure (HSIN-CI)

HSIN-CI is the Department of Homeland Security's (DHS) information sharing platform and collaboration tool for critical infrastructure stakeholders. It is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect CI. According to DHS, it is an unclassified, web-based communications system for sharing sensitive but unclassified information. Users can access protection alerts, information bulletins, incident reports, situational updates, and analyses. Users can also engage in secure discussions with sector peer groups. Other features include CI protection training, planning and preparedness information, and a document library.

Source: GAO analysis of DHS information. I GAO-18-62

Similarly, TSA's Office of Intelligence (TSA-OI) receives intelligence information regarding threats to transportation-related assets and disseminates it to industry officials with transportation responsibilities, as well as to other federal, state, and local officials. TSA-OI disseminates security information through products including reports, assessments, and briefings. For example, TSA-OI, in conjunction with I&A and the Federal Bureau of Investigation, provides intelligence and security information to mass transit and passenger rail security directors, law enforcement chiefs in major metropolitan areas, and Amtrak officials through joint classified intelligence and analysis briefings. Although it is not an intelligence generator, TSA-OI receives and assesses intelligence from within and outside of the intelligence community to determine its relevance to transportation security. Sources of information outside the intelligence community include other DHS components, law enforcement agencies, and owners and operators of transportation systems. TSA-OI also reviews suspicious activity reporting by Transportation Security Officers, Behavior Detection Officers, and Federal Air Marshals.

DHS officials from IP and TSA told us that they also share threat information within their respective sectors. For example, as the Critical Manufacturing SSA, IP disseminates threat information to sector stakeholders daily. Officials from IP also hold quarterly threat briefings to alert stakeholders of relevant threats. TSA likewise shares transportation security related information, including details on threats, vulnerabilities, and suspicious activities, with Transportation Systems sector stakeholders through unclassified or classified products and briefings. For example, TSA provides Transportation Intelligence Notes to transportation security partners to offer additional information or analysis on a specific topic and also provides situational awareness of ongoing or recent incidents. Table 1 in appendix I summarizes DHS threat

assessment activities and products provided to the three selected sectors.

Examples of Threat Information the Department of Homeland Security Provides to Critical Infrastructure Owners and Operators

Classified Threat Briefings: Officials from the Office of Intelligence and Analysis and the sector-specific agencies participate in briefings at regular intervals with critical infrastructure owners and operators to share threat information gathered from intelligence sources.

Incident-Specific Outreach: The Nuclear Reactors, Materials and Waste sector-specific agency hosts incident-specific meetings and calls for sector stakeholders.

Daily Threat Briefings: DHS publishes a daily e-mail that contains threat information intended to provide situational awareness from a variety of sources including the Federal Emergency Management Agency, Department of Justice, and other stakeholders as appropriate. According to DHS, these emails are distributed to more than 140 recipients in the Critical Manufacturing sector.

Source: GAO analysis of Department of Homeland Security information. I GAO-18-62

NCCIC Established to Share Cyber Threat Information

According to DHS, the NCCIC is a 24x7 cyber situational awareness, incident response, and management center. The center shares information among public and private sector partners to build awareness of cyber vulnerabilities, incidents, and mitigation strategies and its partners include other government agencies, the private sector, and international entities. The NCCIC works with the private sector by integrating (both physically and virtually) CI owners and operators into the center's operations so that, during an incident, threat information can be aggregated and communicated between government and appropriate private sector partners in an efficient manner. The NCCIC manages several programs that provide data used in developing 43 products and services in support of its 11 statutorily required cybersecurity functions.[31] The programs include monitoring network traffic entering and exiting federal agency networks and analyzing computer network vulnerabilities and threats. The products and services are provided to its customers in the private sector; federal, state, local, tribal, and territorial government entities; and other partner organizations. For example, the NCCIC issues indicator bulletins, which can contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents. A list of these products and services is summarized in table 5 in appendix II. As of September 2017, 199 private sector CI owners and operators had

[31]The National Cybersecurity Protection Act of 2014 required NCCIC to perform several cybersecurity functions, including being a federal civilian interface for sharing information on cybersecurity-related information and facilitating cross-sector coordination to address cybersecurity risks and incidents. Pub. L. No. 113-282, § 3(a), 128 Stat. 3066, 3067 (2014); 6 U.S.C. § 148(c). The act also required the center to adhere to nine principles, to the extent practicable, in carrying out these functions. One principle, for example, is ensuring that timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared. 6 U.S.C. § 148(e). The Cybersecurity Act of 2015, enacted as Division N of the Consolidated Appropriations Act, 2016, subsequently established additional functions for the center, among other things. Pub. L. No. 114-113, div. N, § 203, 129 Stat. 2242, 2957-58 (2015); 6 U.S.C. § 148(c), as amended. These acts together identify 11 cybersecurity functions that the center is to perform.

as-needed access to NCCIC through their participation in the Cyber Information Sharing and Collaboration Program (CISCP).[32]

The National Cybersecurity and Communications Integration Center (NCCIC)

The Department of Homeland Security's (DHS) NCCIC serves as a central location where partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. According the DHS, working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation, and recovery efforts.

The NCCIC is made up of four branches:

NCCIC Operations and Integration;

United States Computer Emergency Readiness Team;

Industrial Control Systems Cyber Emergency Response Team; and

National Coordinating Center for Communications.

Source: GAO analysis of DHS information. I GAO-18-62

In February 2017, we reported that the NCCIC had taken steps to perform each of its 11 statutorily required cybersecurity functions, such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities.[33] However, we recommended nine actions to DHS for enhancing the effectiveness and efficiency of the NCCIC, including determining the applicability of the implementing principles and establishing metrics and methods for evaluating performance. DHS concurred with our recommendations and we will monitor DHS's progress toward addressing them.

Selected Private Sector Representatives Reported Threat Data as Most Useful Risk Information

SCC representatives we spoke to from the three selected sectors cited threat assessment data as generally the most useful risk information for CI owners and operators. Each of these six representatives indicated that threat information must be distributed rapidly to owners and operators in order to maintain its value and utility. Three of the six representatives reported that DHS generally provides threat information in a timely manner. For example, SCC representatives from the nuclear sector told us that timely threat information from DHS was helpful in clarifying erroneous reports circulating about the terror attacks in Belgium being aimed at nuclear sites in that region. According to these SCC representatives, working with DHS to gather credible information in a timely fashion was very valuable to their sector because it allowed owners and operators within their sector to determine whether they needed to implement certain protocols to ensure that they were not vulnerable to similar attacks. The remaining three representatives told us that delays in receiving threat information from DHS decreased the value of this information. For example, one representative noted that he believes DHS's process for vetting threat information before it is shared with his

[32]The goal of CISCP is to provide a bilateral exchange of cyber threat indicators. The program is to provide a platform and a trusted forum for exchanging threat and vulnerability information, governed by a Cooperative Research and Development Agreement (CRADA) between DHS and each CISCP participant. The CRADA allows participants to gain as-needed access to NCCIC, a mechanism to receive security clearances, and the ability to participate in bidirectional information sharing.

[33]GAO-17-163.

sector prevents the agency from disseminating valuable threat information in a timely manner. Another representative shared an example where the threats referenced in one of the products distributed by DHS had already been identified and addressed. However, the sixth representative emphasized that despite delays in receiving information from DHS, government threat information is very credible and a major resource often used by security managers proposing security upgrades to their respective chief executive officers. This representative also highlighted the significance of TSA's adoption of industry-defined intelligence priorities as directly supporting training and awareness initiatives to create opportunities for prevention.

The NIPP establishes that the government is to provide the private sector with access to timely and actionable information in response to developing threats and crises. Similarly, the sector-specific plans from each of three selected sectors emphasize reliance upon timely and actionable threat information. For example, the 2015 Transportation System's sector-specific plan discusses the importance of an effective and efficient process for receiving, analyzing, and disseminating pertinent and timely threat information and states that effective protection or response to a potential hazard relies on providing the stakeholders at greatest risk with real-time or near real-time alerts of emerging or breaking events.

According to one SCC representative, threat information is the one element of risk that adds the most value because it allows owners and operators to react immediately to improve their security posture to mitigate the effects of any potential hazards. The representative added that specific products like TSA-OI's annual country-specific threat assessments are particularly useful because a number of companies within his sector have business interests outside the U.S. and these reports help them stay abreast of potential threats abroad.

Three of the six SCC representatives we interviewed reported that information regarding cybersecurity threats has become increasingly important. One SCC representative from the Critical Manufacturing sector stated that many of the security managers within his sector are physical security experts who are now facing more and more questions related to cybersecurity threats as a result of the cyber and physical security convergence their companies are experiencing. Therefore, the Critical Manufacturing sector worked with federal partners to increase access to the NCCIC, FBI, and U.S. Secret Service for additional cybersecurity

support and also began promoting the sector's awareness and use of the NIST framework.

DHS Conducts Voluntary Physical and Cyber Vulnerability Assessments for CI

DHS Conducts Voluntary Physical Vulnerability Assessments for CI Owners and Operators

Infrastructure Survey Tool

The Infrastructure Survey Tool (IST) is one of the Department of Homeland Security's (DHS) voluntary vulnerability assessment tools available to Critical Infrastructure owners and operators. It is a web-based security survey conducted by a Protective Security Advisor in coordination with facility owners and operators to identify the overall security and resilience of a facility. The survey contains more than 100 questions used to gather information on such things as physical security, security forces, security management, information sharing, and protective measures. The IST results inform owners and operators of potential vulnerabilities facing their asset or system and recommend measures to mitigate those vulnerabilities. Facility owners access results and preview the effects of proposed mitigation measures through the interactive IST Dashboard.

Source: GAO analysis of DHS information. I GAO 18 62

NPPD helps CI owners and operators develop capabilities to mitigate vulnerabilities by conducting voluntary physical vulnerability assessments primarily by using PSAs to conduct voluntary vulnerability assessments in coordination with owners and operators. These assessments focus on physical infrastructure and are generally asset-specific and conducted during site visits at individual assets. They are used to identify security vulnerabilities and identify potential risk mitigation strategies for owners and operators to address over time. One tool PSAs use in conducting CI assessments is the Infrastructure Survey Tool to assess facilities that agree to voluntarily participate. According to NPPD officials, vulnerability assessments take longer to develop than threat assessments, and the vulnerabilities identified are typically more static than threats, which are constantly evolving. PSAs store the collected assessment data on DHS's Infrastructure Protection Gateway, an information sharing platform intended for use by DHS and its homeland security partners, including CI owners and operators, for access to infrastructure protection tools and information in support of incident preparedness and response efforts. Table 2 in appendix I summarizes the physical vulnerability assessments DHS conducts for the three selected sectors.

In September 2014, we reported that the vulnerability assessment tools and methods that different DHS offices and components used varied with respect to the areas of vulnerability assessed.[34] For example, we found that while all of the assessment tools we reviewed considered perimeter security, approximately half of these tools (6 of 10) included an assessment of cybersecurity. We also found that DHS had not established guidance on what areas should be included in a vulnerability assessment. We recommended, among other things, that DHS review its vulnerability assessments to identify the most important areas of vulnerability to be assessed, and establish guidance. DHS agreed with our recommendation and in July 2016 reported that IP had taken steps to collect and evaluate information on the various vulnerability assessment tools and methods used by DHS offices and components. More

[34]GAO-14-507.

specifically, IP identified six security areas to incorporate into DHS assessment tools and methods. DHS reported in August 2016 that DHS offices and components received guidance for the areas and the specified levels of detail to be incorporated into existing assessment tools.

As a result of addressing this recommendation, we believe that DHS is better positioned to collect and analyze assessment data to enable comparisons and determine priorities between and across CI sectors. DHS is also taking additional steps to address related recommendations from our September 2014 report that remain open. For example, we recommended that DHS develop and implement ways it can facilitate data sharing and coordination of vulnerability assessments to minimize the risk of potential duplication or gaps in coverage. As of September 2017, in response to this recommendation, DHS officials reported they were coordinating with stakeholders and developing features in an online portal to better facilitate information vulnerability assessment data sharing. We will continue to monitor the status of DHS's efforts to address these recommendations.

In addition, in July 2017, DHS officials reported that they were finalizing a strategy intended to identify ways that vulnerability assessment data can be used by not only CI owners and operators but DHS and other government stakeholders to improve their own decision-making.[35] According to these officials, DHS held workshops with over 120 stakeholders from NPPD as well as senior officials from other designated sector-specific agencies and federal departments who identified the need for DHS to provide more vulnerability assessment data related to lifeline facilities—such as water and wastewater treatment plants and train stations. They also noted that stakeholders recommended that DHS use the vulnerability assessment data it collects to conduct trend analysis in specific CI sectors and geographic regions.

[35]This strategy was developed in response to the explanatory statement accompanying the Consolidated Appropriations Act, 2016, which directs the DHS Office of Infrastructure Protection and the Office of Cyber and Infrastructure Analysis to develop and submit a three-year strategic plan to guide vulnerability assessments, among other things. 161 Cong. Rec. H10172-03 (daily ed. Dec. 17, 2015)

The Cyber Resilience Review

The Cyber Resilience Review is one of the Department of Homeland Security's (DHS) cyber vulnerability assessments available to critical infrastructure owners and operators. It is a voluntary, nontechnical assessment to evaluate an organization's operational resilience and cybersecurity practices. It may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity Cyber Security Advisors. It assesses enterprise programs and practices across 10 domains: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, training and awareness, and situational awareness.

Source: GAO analysis of DHS information. I GAO-18-62

DHS Offers Voluntary Cyber Vulnerability Assessments for CI Owners and Operators

The Office of Cybersecurity and Communications (CS&C) offers CI owners and operators a suite of voluntary vulnerability assessments aimed at securing their cyber systems. For example, CS&C's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is responsible for taking steps to help mitigate vulnerabilities to computer-based systems that are used to monitor and control industrial processes. CS&C also maintains the National Cybersecurity Assessment and Technical Services team which offers cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provides risk analysis and remediation recommendations. The CSA program also provides cyber assessment services for CI owners and operators through on-site vulnerability assessments for cyber systems. CSAs offer the Cyber Infrastructure Survey Tool, an assessment of essential cybersecurity practices instituted by critical infrastructure organizations to protect their critical IT services as well as the Cyber Resilience Review which evaluates an organization's operational resilience and cybersecurity practices. A summary of DHS's critical infrastructure cyber vulnerability assessment efforts can be found in table 3 in appendix I.

Selected Private Sector Representatives View Asset-Specific Vulnerability Assessments As Useful

Sector Coordinating Council representatives from two of the three selected sectors stated that DHS's vulnerability assessment efforts were useful for determining vulnerabilities for individual CI owners and operators, but their opinions varied concerning the usefulness of aggregating sector-wide data and sharing broadly among private sector stakeholders. For example, one SCC representative told us that the risk scores associated with individual vulnerability assessments are of value to the CI owners and operators of the infrastructure for which that assessment was administered.[36] However, this representative also mentioned that these scores have limited value beyond the individual asset because risks differ greatly between companies, rendering sector-wide or regional vulnerability assessments less useful. Another SCC

[36]Survey data from IST vulnerability assessments are composed of weighted scores on a variety of factors for specific critical infrastructures and are provided to owners and operators to inform protective measures, resilience planning, and resource allocation.

representative told us that because the membership of their respective sectors is so broad and diverse, it is difficult for members to discern the value of high-level aggregated vulnerability data—especially from organizations with very different business models. However, another SCC representative indicated that DHS could offer aggregated vulnerability assessment data to all CI stakeholders for the purpose of developing broader situational awareness.

DHS Conducts Consequence Assessments as Part of Its Infrastructure Survey Tool

While DHS's IST is used to assess vulnerabilities for CI, the tool also includes a consequence module intended to allow DHS to assess facility criticality in terms of potential loss of life and economic impact. Also, OCIA analyzes consequence from incidents, and models past events to better understand the effect of these disruptions on assets and predict consequences of future events. Table 4 in appendix I describes the DHS components and corresponding products and activities associated with consequence assessments.

DHS officials we spoke with stated that consequence information is important to owners and operators. These officials added that DHS needs to demonstrate that potential losses can be avoided by owners' and operators' investment in risk mitigation, thereby reducing the overall consequence of a potential incident on the CI owner's operations and the nation. Three of the six SCC representatives we interviewed shared that consequence information was not useful. For example, one SCC representative noted that consequence information is not very useful for owners and operators because timely threat information combined with knowledge of an asset's vulnerabilities put owners and operators in a better position to mitigate potential incidents and, subsequently, any associated consequences. DHS officials acknowledged that a range of perspectives concerning the usefulness of consequence information exists and stated that these differences reflect the array of owner and operator views about how to use risk information for different risk management decisions.

DHS Conducts Complete Risk Assessments for CI Sectors on a Limited Basis

Within DHS, NPPD, TSA, and the Coast Guard are responsible for developing complete risk assessments, which can be conducted for an

entire CI sector or multiple sub-sectors within a CI sector. Both TSA and the Coast Guard regularly conduct complete risk assessments within the Transportation Systems sector. However, according to a senior OCIA official, NPPD receives very few requests for complete risk assessments. Our review of available assessment documentation found that among our three selected sectors, DHS has conducted complete risk assessments for the Transportation Systems sector but not the other two sectors. For example, the Transportation Systems Sector Security Risk Assessment is TSA's annual report to Congress on transportation security. It assesses risk by establishing risk scores for various attack scenarios within the sector, including for domestic aviation; examines risks to individual transportation modes; and compares them to risks within and across modes. Table 6 in appendix III describes the assessment in more detail.

Also within the Transportation Systems sector, the Coast Guard's Maritime Security Risk Analysis Model (MSRAM) serves as the primary tool for assessing and managing security risks for all of the vessels, barges, and facilities regulated by the Coast Guard under the Maritime Transportation Security Act of 2002. Since its development and implementation in 2005, MSRAM has provided the Coast Guard with a standardized way of assessing risk to maritime infrastructure, referred to in the analysis model as targets that can include chemical facilities, oil refineries, hazardous cargo vessels, passenger ferries, and cruise ship terminals. For example, a scenario related to cruise ships identified using this analysis model could include a boat bomb or an attack by a hijacked vessel. MSRAM is designed to allow comparison between different targets at the local, regional, and national levels with the goal of reducing risk by prioritizing security activities and resources.

To prioritize and assess security risks at U.S. ports and facilities, the Coast Guard uses MSRAM to calculate risk using threat judgments provided by the Coast Guard Intelligence Coordination Center. The Center provides threat probabilities for MSRAM based upon judgments regarding specific intent, capability, and geographic preference of terrorist organizations to deliver an attack on a specific type of maritime target class—for example, a boat bomb attack on a ferry terminal. To make these judgments, Center officials use intelligence reports generated throughout the broader intelligence community to make qualitative determinations about certain terrorist organizations and the threat they pose to the maritime domain. At the sector level, Coast Guard MSRAM users are required to use the threat probabilities provided by the Center to ensure that threat information is consistently applied across ports.

MSRAM users at the sector level also assess the vulnerability of targets within their respective areas of responsibility and assess the consequences of a successful attack on these targets.[37] Vulnerability and consequence factors included in the MSRAM assessment can be found in table 7 in appendix III.

According to one NPPD official, various sector councils have requested analysis of certain risk elements, such as vulnerabilities or consequences, as opposed to complete risk assessments. For example, councils have asked for analysis of vulnerabilities and consequences due to potential failures within their sector's respective systems and the potentially cascading effects of these failures on systems beyond their own span of control. This official noted that these requests provide the opportunity for OCIA to develop analytic products that companies within these sectors can then use as part of the risk assessments they conduct for themselves, as well as analytic products more broadly related to homeland security risks.

SCC representatives from our three selected sectors told us that complete risk assessments are of limited utility for CI owners and operators because complete assessments take a long time to produce, often involve risk scenarios that are not likely to occur, or generates results that are so broad that they may not be applicable to individual assets. For example, according to one SCC representative, the diversity among the members of his sector, including size and sophistication of operations, is the primary reason that conducting a complete risk assessment for their sector would not be helpful for individual companies. Similarly, another SCC representative told us that the private sector does not operationalize information from complete risk assessments because the assessments do not add practical value and some of the scenarios evaluated in the assessments are not applicable to many of the companies within their sector.

TSA and NPPD officials provided explanations of the utility of complete risk assessments, particularly for government decision-making purposes.

[37]Vulnerabilities identified as a result of MSRAM represent the probability of a successful attack, given an attempt. Similarly, consequence represents the projected overall impact of a successful attack on a given target or asset. MSRAM's risk assessment process asks users to evaluate each scenario considering the target's reasonable worst-case consequences. The Coast Guard defines this as the "maximum level of consequence for which there is at least a moderate likelihood of the attack mode being able to cause that damage level."

For example, TSA officials told us that they believe the Transportation Systems Sector Security Risk Assessment data gathering methodology for identifying risk inputs adds the most value in the assessment process for CI owners and operators in the Transportation Systems sector. According to these officials, the data gathering process is extensive and involves a substantial number of industry experts who are brought together to analyze potential threats, vulnerabilities, and consequences across the five transportation modes for which TSA is responsible. The officials added that this elicited risk information allows TSA to better allocate resources across the multiple transportation modes. According to one senior OCIA official, NPPD is best suited to execute complete risk assessments that are intended to focus on broad risks to CI and are not specific to individual CI assets. For example, NPPD is providing risk information for the execution of the 2018 Homeland Security National Risk Characterization (HSNRC), which evaluates the full range of risks addressed by DHS.[38] This official stated that their office is working with DHS's Office of Policy to maximize the value of the insights gained from the HSNRC effort and using it to inform NPPD decisions about strategy and policy.

DHS Uses CI Risk Information to Inform Strategic Planning and Guide Outreach to Owners and Operators

DHS uses CI risk information in multiple ways, including informing strategic planning and developing analytic products, and at the component level to guide its day-to-day owner and operator outreach and incident response. DHS is also facilitating risk-based cross-sector planning and information sharing through sector coordinating councils.

[38]The HSNRC is DHS's process for describing high-impact or likely incidents against the homeland—including incidents affecting CI assets.

DHS Uses CI Risk Information to Inform Its Strategic Planning and is Taking Actions to Improve Supporting Risk Analysis

According to DHS Office of Policy officials, DHS is using risk information to inform departmental strategic planning as part of its third QHSR.[39] The QHSR is DHS's process for updating the national homeland security strategy, identifying critical homeland security missions, and assessing the organizational alignment of DHS with the homeland security strategy and missions. The results of the QHSR are used in DHS's Strategic Plan, which outlines how DHS plans to implement the QHSR homeland security goals, lists strategies to achieve these goals, and identifies performance measures to track progress towards these goals. The QHSR incorporates multiple sources of risk information, including the HSNRC. The HSNRC assesses natural hazards such as floods, and manmade hazards such as terrorism. According to Office of Policy and NPPD officials, NPPD provides a broad range of risk-related inputs to support the implementation of the HSNRC risk assessment methodology. These inputs provide DHS officials a better understanding of risks to CI during strategic planning, according to Office of Policy officials.

Our prior work on DHS's QHSR found that DHS assessed homeland security risks for its second QHSR for fiscal years 2014 to 2018 by considering threats, vulnerabilities, and consequences.[40] We also found that while the QHSR risk assessment described a wide range of homeland security challenges and was a valuable step toward using risk information to prioritize and select risk management activities, DHS did not document how its various analyses were synthesized to generate results, thus limiting the reproducibility and defensibility of the results. We found that without sufficient documentation, the QHSR risk assessment results could not easily be validated or the assumptions tested, hindering DHS's ability to improve future assessments. In addition, the QHSR described homeland security hazards, but did not rank those hazards or provide prioritized strategies to address them. We reported that

[39]The Implementing Recommendations of the 9/11 Commission Act of 2007 requires that beginning in fiscal year 2009 and every 4 years thereafter, DHS conduct a review that provides a comprehensive examination of the homeland security strategy of the United States. See 6 U.S.C. § 347. DHS completed its first QHSR in February 2010 and its second in June 2014.

[40]GAO-16-371.

comparing and prioritizing risks helps identify where risk mitigation is most needed and helps justify cost-effective risk management options. Thus, we recommended that future QHSR risk assessment reflect key elements of successful risk assessment methodologies, including being documented, reproducible, and defensible. We also recommended that DHS refine its risk assessment methodology so that in future QHSRs it can compare and prioritize homeland security risks and risk mitigation strategies. DHS concurred with these recommendations and outlined steps it planned to address them.

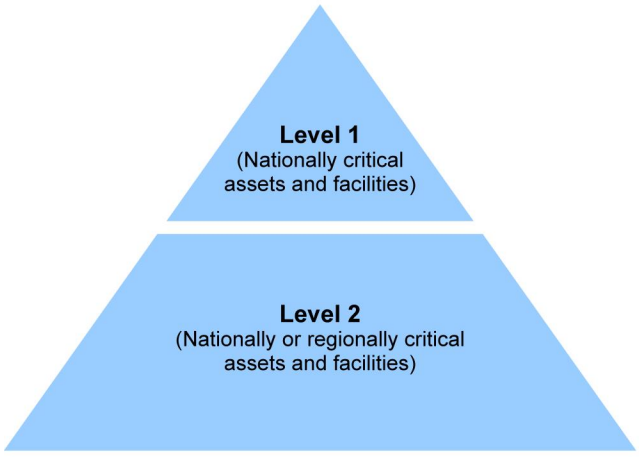
In response to our recommendations, DHS officials described several steps they have taken to address our recommendations. According to these officials, the Office of Policy held initial meetings with government and nongovernment subject matter experts after the release of our report to refine the HSNRC. Also, according to these officials, a Departmental Risk Modeling and Analysis Steering Committee (Risk committee) was convened in June 2016 to review and approve proposed new methodologies to help identify and prioritize threats and hazards for the HSNRC. According to NPPD officials, NPPD proposed updates to the HSNRC process as part of the Risk committee proceedings, such as changing the scope and detail of the assessment.[41] The Risk committee evaluated these requests and finalized proposals for use in the third QHSR, which is scheduled to be released in 2018. We will continue to monitor the status of DHS's actions to address our recommendations and how they are implemented.

[41]In July 2016, the U.S. Office of Management and Budget updated Circular A-123, its guidance on enterprise risk management, to include a requirement that agencies develop a risk profile as a part of the development of their strategic plans. According to NPPD officials, NPPD is working with the Risk committee to modify the HSNRC as part of DHS's efforts to satisfy this new requirement.

DHS's Office of Infrastructure Protection Uses CI Risk Information to Inform Outreach to Owners and Operators and Incident Response

According to IP officials, PSAs use risk information to guide their outreach to CI owners and operators. PSAs use the National Critical Infrastructure Prioritization Program (NCIPP) list—which prioritizes CI assets into different levels according to their criticality—to inform their outreach to owners and operators.[42] PSAs and their leadership use the NCIPP list to prioritize outreach to owners and operators across each level of assets within their area of jurisdiction for participation in DHS's voluntary security survey and vulnerability assessment programs, as shown in figure 5. Generally, PSAs engage CI owners and operators in the order in the pyramid shown in figure 5, starting with Level 1.

Figure 5: National Critical Infrastructure Prioritization Program (NCIPP) Levels



Source: Department of Homeland Security. | GAO-18-62

According to IP officials, PSAs also use risk information to guide incident response. The officials explained that when an incident occurs, they pull

[42]To compile the NCIPP list, consistent with statutory requirements, OCIA conducts a voluntary annual data call to solicit nominations to the list from state homeland security and federal partners. See 6 U.S.C. § 124*l*. NCIPP nominations are to meet minimum specified consequence thresholds outlined in the annual data call for at least two of the following four categories: fatalities, economic loss, mass evacuation length, and degradation of national security. The NCIPP list prioritizes CI assets and facilities based on the severity of these estimated consequences of a significant disruption. Appendix IV provides more information about NCIPP level criteria.

information from a variety of sources, including the database of assets on the NCIPP list, to identify CI in the affected area. OCIA officials then prioritize this information into a list to guide incident response efforts. For example, when Hurricane Hermine approached Georgia in September 2016, PSAs received a list from OCIA that categorized potentially affected CI assets in the region into priority levels. The PSAs used the list to prioritize their outreach to the highest priority assets.

Officials from the CSA program, also plan to use risk information to guide cybersecurity outreach to CI owners and operators. According to CS&C officials, CSAs are currently able to meet resource demands for outreach with little or no delay. However, as the CSA program continues to expand, CSAs plan to use a risk-based methodology to prioritize outreach.[43] This methodology considers cyber threats, vulnerabilities, and consequences to determine how and where CSAs are used, according to CS&C officials.

DHS SSA representatives for our three selected sectors also use risk information to guide their outreach to CI owners and operators. For example, in response to a physical threat to a nuclear facility in Brussels, Belgium, nuclear sector SSA officials engaged with private sector representatives on the SCC and discussed ways to improve their information-sharing process. In another example, Critical Manufacturing SSA officials determined that smaller businesses in their sector did not have business continuity plans.[44] According to these SSA officials, this was a risk that could disrupt the operations of these small businesses and other businesses in their supply chain. SSA officials developed a tool to help Critical Manufacturing sector owners and operators develop their own continuity plans—including templates, tabletop exercises, and a self-directed risk assessment for private sector owners and operators to use. According to the Critical Manufacturing sector-specific plan, the expanded use of business continuity planning will enhance the resilience of the Critical Manufacturing Sector.

[43]As of August 2017, DHS had deployed 12 Cyber Security Advisors.

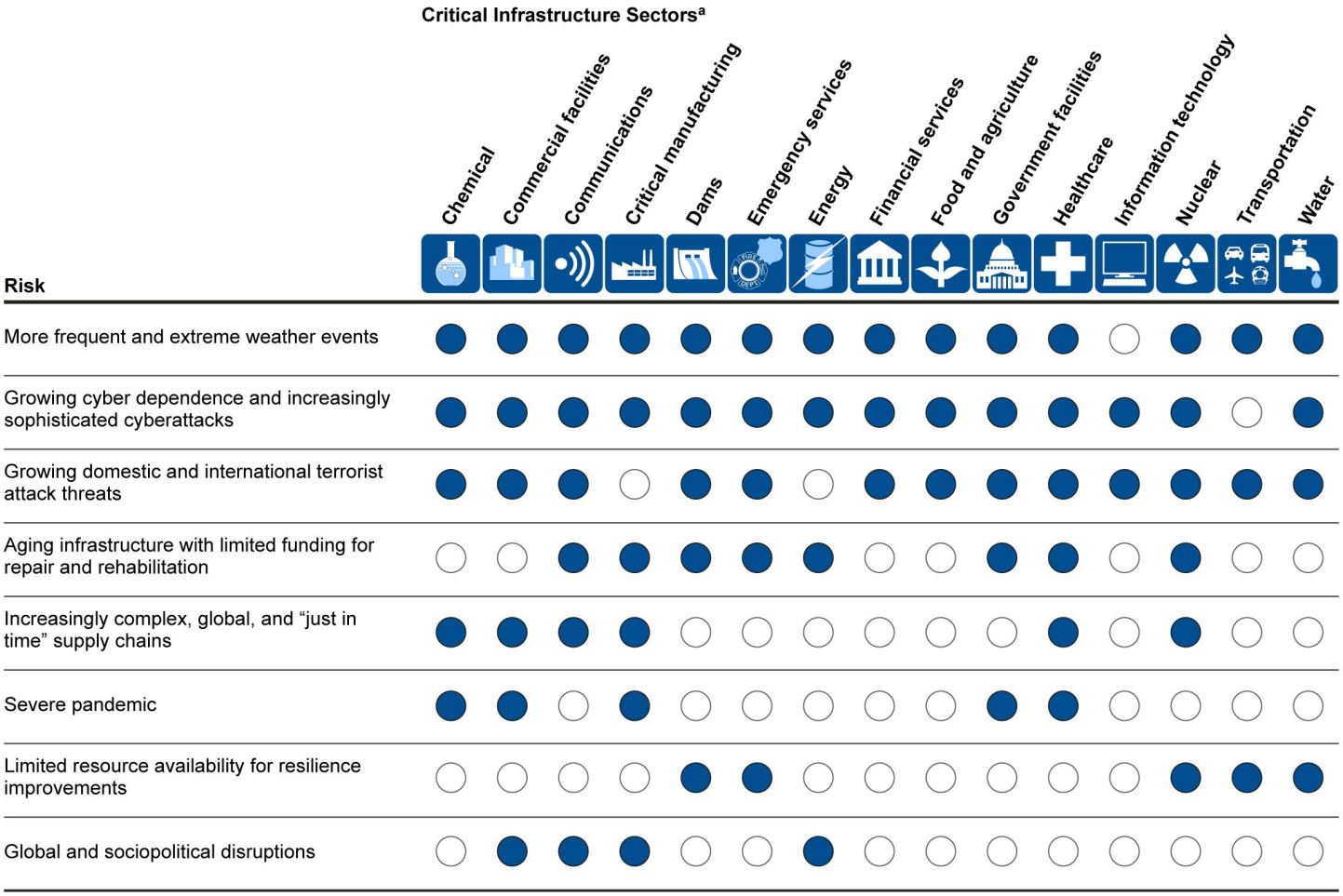
[44]Business continuity plans are plans for a company to continue operations in the event of a disaster or disruption to its infrastructure.

DHS Facilitates Sharing of Cross-Sector Risk Information through Coordinating Councils and Planning Documents

As part of DHS's responsibility described in the NIPP, DHS created the Critical Infrastructure Partnership Advisory Council (CIPAC), a forum for stakeholders including government officials and asset owners and operators, to facilitate planning and information sharing. CIPAC membership consists of representatives from the government and sector coordinating councils—federal, state, and local agency officials, and private owners and operators, respectively—who work together to coordinate strategies, activities, and policies across governmental entities within each of the 16 CI sectors. There is also a Critical Infrastructure Cross-Sector Council comprised of SCC chairs and vice chairs from each of the 16 sectors that meets quarterly to discuss, among other things, details about risks and opportunities to share information across sectors. Additionally, this Critical Infrastructure Cross-Sector Council provides a forum for the leaders of the SCCs to provide senior-level, cross-sector strategic coordination with DHS. The chairperson of the cross-sector council also communicates with owners and operators across the sectors as situations arise. For example, the chairperson convened a teleconference within 24 hours of a recent terror attack in the United Kingdom to share information and answer questions about potential risks or lessons learned for CI owners and operators.

In addition, DHS engages private sector owners and operators in cross-sector discussions through sector planning documents. For example, the 2015 sector-specific plans for each of the three sectors we studied include descriptions of cross-sector interdependencies. These include summaries of lifeline functions—such as energy, water, communications, and transportation systems—which are essential to the operations of most CI partners and communities. During development of the 2015 sector-specific plans the sectors and SSAs also collaborated and identified emerging risks that spanned across multiple sectors, as shown in figure 6.

Figure 6: Cross-Sector Risks Identified during the 2015 Sector-Specific Plan Update



Source: GAO analysis of Department of Homeland Security documents. | GAO-18-62

[a]The Defense Industrial Base sector-specific plan was not available at the time DHS evaluated these risks and therefore is not included in this figure.

Agency and Third Party Comments

We provided a draft of this product to DHS for review and comment. DHS provided technical comments, which we incorporated as appropriate. We also provided draft excerpts of this product to the selected sector coordinating council representatives we interviewed, who provided technical comments that we also incorporated as appropriate.

We are sending copies of this report to interested congressional committees and the Secretary of Homeland Security. 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 (404) 679-1875 or CurrieC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Chris P. Currie
Director, Homeland Security and Justice Issues

Appendix I: Selected Risk Information Products and Activities Distributed by the Department of Homeland Security

The following tables highlight threat, vulnerability and consequence products and activities developed by the Department of Homeland Security for the purpose of providing risk information to critical infrastructure owners and operators.

Table 1: Department of Homeland Security (DHS) Components That Distribute Threat Information to Critical Infrastructure Owners and Operators in Three Selected Sectors, with Corresponding Products and Activities

Threat Information Actors	Information Sharing Products and Activities and Explanation (if applicable)
Office of Intelligence and Analysis (I&A)	
Homeland Threat Division	For the three selected sectors (Critical Manufacturing, Nuclear Reactors, Materials, and Waste, and Transportation Systems), I&A distributes threat information. I&A participates in biweekly briefings with critical infrastructure owners and operators with appropriate security clearances. These briefings are hosted by the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection. Critical Infrastructure owners and operators can express interest and request more specific information on threats at these events. Information is distributed primarily via DHS's Homeland Security Information Network for Critical Infrastructure (HSIN-CI).[a]
NPPD, Sector Outreach and Programs Division	
Critical Manufacturing sector-specific agency (SSA)	Daily Threat Briefs: Daily e-mails contain threat information from a variety of sources including the Federal Emergency Management Agency, Department of Justice, and Critical Manufacturing Information Sharing and Analysis Organization.[b] Classified Threat Briefings: Provide the opportunity for appropriately cleared members of the Critical Manufacturing sector to access classified intelligence products and are generally held during the annual Critical Manufacturing Road Show.[c] Cyber Awareness Documents: The SSA developed awareness documents on DHS's cybersecurity capabilities such as available alerts and warnings, cyber assessments, evaluations, and reviews to assist critical infrastructure sectors in identifying, prioritizing, and managing their cyber-infrastructure risk.
Nuclear Reactors, Materials, and Waste (SSA)	Quarterly Classified Threat Briefings: The SSA hosts quarterly classified threat briefings in conjunction with I&A which provides briefings to sector stakeholders with the appropriate clearance. Unclassified Threat Calls: Teleconferences hosted in coordination with DHS's I&A and Office of Cybersecurity and Communications. Incident-Specific Sector Outreach: The SSA hosts incident-specific sector coordination messages and calls.
Transportation Security Administration (TSA)	

Threat Information Actors	Information Sharing Products and Activities and Explanation (if applicable)
TSA Office of Intelligence (TSA-OI)	The Transportation Intelligence Note (TIN): Provides additional information or analysis on a single specific issue/topic, or provides situational awareness of an ongoing or recent event/incident. TINs can be produced at the classified and unclassified levels and vary from 1 to 5 pages in length. TINs are regularly distributed to TSA officers and transportation security partners. Assessments: According to TSA-OI, assessments typically include analysis of the threat, a discussion of potential actors, targets, and tactics, and may include an outlook or review of potential countermeasures or vulnerabilities. They may also include speculative or predictive analysis, as well as appendices providing detailed charts or supporting information. These documents are produced at the classified and unclassified levels. TSA-OI produces various assessments, including: • modal threat assessments (aviation, freight rail, pipeline, highway, mass transit, ferries); • special event threat assessments (transportation focus only, usually covers National Special Security Events); • tactics, techniques, and procedures assessments; and • current airport threat assessments (threat information for various classes of airports across the United States). Briefings: According to TSA-OI officials, TSA may share transportation security related information, including details on threats, vulnerabilities, and suspicious activities, with transportation stakeholders during unclassified or classified briefings. These briefings may be provided on an as-needed basis to individual security professionals, public and private stakeholders, local and regional groups, or more regularly to entire industries at forums such as trainings, workshops, and conferences. These briefings may also be conducted at TSA headquarters, at other secure locations, over a secure phone line, or via video or teleconference. For example, TSA regularly briefs senior security staff at a passenger air carrier every 3 months at TSA headquarters covering areas of international operation.

Source: GAO analysis of DHS information. | GAO 18-62

Note: This list includes examples of TSA's information-sharing products, but is not intended to be an exhaustive list.

[a]The Homeland Security Information Network for Critical Infrastructure (HSIN-CI) is a network for homeland security mission operations to share sensitive but unclassified information. HSIN-CI is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure.

[b]According to an SCC official, the Critical Manufacturing Information Sharing and Analysis Organization is a private-sector organization staffed by analysts who assess open-source information about critical infrastructure risk information.

[c]The Critical Manufacturing Roadshow showcases the activities of the Department of Homeland Security and other U.S. government entities as they strive to meet the information needs and provide necessary tools for the Critical Manufacturing sector coordinating council to enhance its awareness and resilience while building public-private partnerships.

Table 2: Physical Vulnerability Assessments Conducted by the Department of Homeland Security (DHS) for Three Selected Critical Infrastructure Sectors

Vulnerability Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
National Protection and Programs Directorate - Protective Security Advisors (PSAs)	
Enhanced Critical Infrastructure Protection (ECIP) Visits	PSAs conduct these visits with critical infrastructure (CI) owners and operators to establish DHS's relationship with the facility and communicate available infrastructure protection services that could enhance their security.
Infrastructure Survey Tool (IST)	The IST is a web-based security survey intended to assess a facility's vulnerabilities. Conducted by a PSA in coordination with facility owners and operators, it identifies facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery.
Rapid Survey Tool	This vulnerability assessment survey is a web-based data collection capability that examines the most critical aspects of a facility's security and resilience posture with baseline questions. The results are analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities.
Infrastructure Visualization Platform (IVP)	IVP is a data collection and presentation medium that supports critical infrastructure security, special event planning, and responsive operations. It provides immersive imagery, geospatial, and hypermedia data of critical facilities, surrounding areas, transportation routes, and more. It also integrates assessment data from other PSA assessments.
Regional Resiliency Assessments Program (RRAP)	RRAP is an assessment of critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regionally and nationally significant consequences.
Transportation Security Administration (TSA)	
Baseline Assessment for Security Enhancements (BASE)[a]	The BASE program is a voluntary security assessment of national mass transit, passenger rail, and highway systems. It was developed to increase domain awareness, enhance prevention and protection capabilities and further response preparedness of transit systems nationwide. According to TSA, these assessments direct TSA to identify critical assets, infrastructure systems and the vulnerabilities associated with these infrastructures.
Pipeline Security Critical Facility Security Reviews (CFSR)	TSA conducts field-based physical security reviews to assess security measures in place at pipeline critical facilities according to TSA officials. Site-specific information is collected from the operator on security procedures and physical security measures in place at the facility. The Implementing Recommendations of the 9/11 Commission Act of 2007 required TSA to develop and implement a plan for inspecting the critical facilities of the top 100 pipeline systems in the nation.[b] TSA conducted these required inspections between 2008 and 2011 through the Critical Facility Inspection program and is continuing the effort through TSA's Critical Facility Security Review (CFSR) program. After a CFSR, TSA shares its findings with the operator and makes recommendations for improving the facility's security posture.

Vulnerability Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
Joint Vulnerability Assessment (JVA)	According to TSA officials, the JVA Unit conducts vulnerability assessments triennially at selected airports to reduce the risk of an attack and to mitigate the consequences of an attack on airports and the civil aviation system. JVAs are conducted to identify vulnerabilities, both internal and external, to an airport. In accordance with 49 U.S.C. § 44904, the JVA Unit conducts JVAs in concert with the Federal Bureau of Investigation, which submits a threat assessment report of its own under separate cover.

Source: GAO analysis of DHS information. I GAO-18-62

[a] According to TSA officials, BASE assessments are not vulnerability assessments. However, we included BASE in our analysis because these assessments are used to identify potential weaknesses within mass transit systems and infrastructures.

[b]See Pub. L. No. 110-53, § 1557, 121 Stat. 266, 475-76 (2007); 6 U.S.C. § 1207.

Table 3: Critical Infrastructure Cyber Vulnerability Assessments Conducted by the Department of Homeland Security (DHS)

Vulnerability Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	
Cyber Security Evaluation Tool (CSET)	CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from this tool is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems.
Design Architecture Review (DAR)	DAR provides critical infrastructure (CI) asset owners and operators with a comprehensive technical review and cyber evaluation of their industrial control system's architecture and interdependencies.
Network Architecture Validation and Verification (NAVV)	An industrial control systems assessment conducted with CI owners and operators. It assesses the network traffic within the industrial control system network to identify potential communications.
Stakeholder Engagement and Cyber Infrastructure Resilience Division	
External Dependency Management (EDM) Assessment	The EDM is a nontechnical assessment of an organization's external dependencies management practices. The goals of the EDM are to (1) assess the activities and practices used in an organization to manage cyber risks from external dependencies; (2) measure the stability and maturity of processes (to produce consistent results over time, foster efficiencies and confidence, and integrate with overall enterprise risk management); and (3) provide a roadmap for improvement, including a clear, objective review and recommendations that are based on industry leading practices.
National Cybersecurity Assessment and Technical Services (NCATS)	
Risk and Vulnerability Assessments (RVA)	According to CS&C officials, an RVA is a voluntary 2-week engagement during which NCATS conducts internal testing at the stakeholder location and external testing from its laboratories.
Cyber Hygiene	Cyber Hygiene is an external remote scanning capability developed for federal partners. The scan provides partners with a priority list of low, medium, high, and critical vulnerabilities in their cyber infrastructure. The scan can be run consistently and generate weekly reports, according to CS&C officials.
Cyber Security Advisors (CSAs)	

Vulnerability Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
Cyber Infrastructure Survey Tool (C-IST)	The C-IST is an assessment of essential cybersecurity practices in place for critical services within CI organizations.
Cyber Resilience Review (CRR)	The CRR is a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. It may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. It assesses enterprise programs and practices across a range of 10 domains including risk management, incident management, service continuity, and others.

Source: GAO analysis of DHS information. I GAO-18-62

Table 4: Department of Homeland Security (DHS) Components That Conduct Consequence Assessments for Critical Infrastructure, with Corresponding Products and Activities

Consequence Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
National Protection and Programs Directorate (NPPD) – Office of Infrastructure Protection	
Infrastructure Survey Tool (IST)	The IST survey contains more than 100 questions and 1,500 variables. It is used to gather information on the security posture of critical infrastructure (CI), can inform owners and operators of potential vulnerabilities facing their asset or system, and also contains about a dozen questions specific to consequence. According to a DHS official, these questions are high-level and explore an asset's lifeline criticality, potential loss of life, and other elements. Although the tool is primarily focused on vulnerability, Protective Security Advisors use the resulting consequence information to prioritize infrastructure or to contextualize a facility with respect to criticality.
Regional Resiliency Assessment Program (RRAP)	A voluntary assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regionally and nationally significant consequences.
NPPD – Office of Cyber and Infrastructure Analysis (OCIA)	
Global Positioning System (GPS) National Risk Estimate	DHS's GPS National Risk Estimate (NRE) is a scenario-based risk assessment for four critical infrastructure sectors using subject matter experts from inside and outside of government intended to assess the risks and potential effects from disruptions in the GPS on critical infrastructure.
Infrastructure Impact Assessment (IAA)	Provides an overview of risks to critical infrastructure from various hazards. The information in an assessment is intended to inform DHS leadership and partners on the recent information about conditions and provide an analytic assessment of the most critical concerns related to a particular incident, often broken down by sector.
In Response To Your Questions (IRQ)	IRQs provide expert interpretation of the situation under discussion and explain why some concerns can be ruled out. They help leadership prioritize further work or coordination.
Infrastructure Protection (IP) Note, or later, Critical Infrastructure Security and Resilience (CISR) Note	Typically provides a proactive view of the expected losses and other potential harms that could result from a scenario or a developing condition sufficiently far in advance that plans, policies, and procedures could be developed to mitigate these risks.
Infrastructure of Concern List	The Infrastructure of Concern List identifies infrastructure that is likely to be of concern given the incident that is taking place, and provides a prioritized list of critical infrastructure to help guide response efforts.

Source: GAO analysis of DHS information. I GAO-18-62

Appendix II: NCCIC Cybersecurity Products and Services

Table 5 below highlights the cybersecurity products and services that the National Cybersecurity and Communications Integration Center (NCCIC) reported providing to its customers in fiscal years 2015 and 2016.

Table 5: National Cybersecurity and Communications Integration Center (NCCIC) Products and Services Produced or Performed in Fiscal Years 2015 and 2016

NCCIC Product or Service	Description	NCCIC Component
1. Cyber Information Sharing and Collaboration Program (CISCP) Indicator Bulletins	Provides incident analysis information derived from new cyber incidents and/or malicious code, threats, and vulnerabilities to CISCP partners including local and state government, critical Infrastructure, private industry, or a country Computer Emergency Response Team (CERT)	US-CERT
2. US-CERT Indicator Bulletins	A short turnaround bulletin containing threat-specific indicators of compromise.	US-CERT
3. Malware Initial Findings Reports	Preliminary analysis and initial mitigation recommendations for submitted malware artifacts.	US-CERT
4. Preliminary Digital Media Analysis Reports	Reports of initial findings from a forensic investigation of digital media.	US-CERT
5. Digital Media Analysis Reports	Reports of full forensic analysis of digital media.	US-CERT
6. Malware Analysis Reports	Reports containing full analysis, indicators of compromise, tactics, techniques, and procedures and mitigation recommendations for submitted malware artifacts.	US-CERT
7. Request for Information	A request made by a third party for information, or more information, on either general cybersecurity issues or specific incidents or issues of interest to the requestor.	US-CERT
8. Victim/Abuse Notifications	A victim notification is sent to a third party based on information that they may be a victim of a cybersecurity event. An abuse notification is sent to a third party based on information that they may have systems that are being used for malicious purposes.	US-CERT
9. Joint Analysis Report	An analysis report produced in coordination with US-CERT's trusted partners (i.e. law enforcement or Intelligence community).	US-CERT
10. Joint Indicator Bulletins	An indicator bulletin produced in coordination with US-CERT's trusted partners (i.e. law enforcement or Intelligence community).	US-CERT
11. US-CERT Analysis Reports	Provides indicators of compromise and tactics, techniques, and procedures related to specific threats.	US-CERT
12. Customer and Partner Engagements (Conference Presentations)	US-CERT's efforts to build and leverage partnerships across the federal government; state, local, tribal, and territorial governments; the private sector; and the international community. Enhancing trust through customer and partner engagement is critical to enabling greater information sharing and improving coordination about cyber events.	US-CERT

NCCIC Product or Service	Description	NCCIC Component
13. Vulnerability Information	Provides information about software vulnerabilities, including summaries, technical details, remediation information, and lists of affected vendors. Many vulnerability notes are the result of private coordination and disclosure efforts.	US-CERT
14. Incident Response Team Reports	A report provided to external customers on the impact of a particular compromise. For example, officials stated that their activities to assist the Office of Personnel Management during its information breach would fall under this product. An output of this product would be a report to the affected party. Other outputs of this product may result in binding operational directives to agencies, or information for the Office of Management and Budget memoranda.	US-CERT
15. Incident Notifications	US-CERT detects malicious cyber activity targeting federal agencies through tools such as EINSTEIN.	US-CERT
16. Industrial Control Systems (ICS) Joint Working Group	A collaborative and coordinating body that provides a vehicle for communicating and partnering across all Critical Infrastructure (CI) Sectors between federal agencies and departments, as well as private asset owners/operators of industrial control systems.	ICS-CERT
17. ICS Briefings	Briefings provided in small group or large group formats discussing ICS-CERT and current threats, actions and products.	ICS-CERT
18. ICS Reports	Reports on cyber activity related to critical infrastructure on current threats, actions to take and defensive measures.	ICS-CERT
19. ICS Classroom Training	Technical training about security control systems that are provided in person either at an entity or through individual sign-up.	ICS-CERT
20. ICS Online Training	Online training modules with a blended learning approach, which makes accessing course material easier and more efficient, reduces redundancy in training materials, and eliminates the need to travel to participate in ICS-CERT training.	ICS-CERT
21. ICS Cyber Assessment	Assessments include a Design Architecture Review (DAR), a technical review and cyber evaluation of ICS operations; a Cybersecurity Evaluation Tool, a basic one day assessment ending in a report on the organization's cyber posture; and a Network Architecture Verification and Validation (NAVV), where DHS uses tools to review and analyze network traffic occurring within the ICS network.	ICS-CERT
22. ICS Incident Response Deployment	Incident response assistance either on-site or remote and incident analysis that varies based upon the nature of the cybersecurity incident.	ICS-CERT
23. ICS Vulnerability Alerts	An alert provided from ICS-CERT indicating a vulnerability identified and what actions an entity can take to mitigate the vulnerability, including implementing a patch.	ICS-CERT
24. Title Globe Communications Testing	A monthly test of the communications capabilities of federal departments and agencies. The results of the tests are provided to each entity, with quarterly reports sent to the White House.	NCC
25. Shared Resources High Frequency Radio Program	Testing of the over 1600 high-frequency radio stations across the country that have agreed to pass federal traffic in times of crisis. It is meant to be a contingency communication system when other communications go out.	NCC
26. Emergency Support Function 2 Webinars and Videos	Online resources for training and knowledge management related to Emergency Support Function 2.	NCC

NCCIC Product or Service	Description	NCCIC Component
27. Emergency Support Function 2 National Level Exercise Participation & Planning	Activities related to national level exercises to support Emergency Support Function 2.	NCC
28. Emergency Support Function 2 Regional Exercise Participation	Exercises to test regional communication infrastructures related to Emergency Support Function 2.	NCC
29. National Coordinating Center (NCC) Watch Request for Information (RFI)/Advisories/ Situational Report (SITREP)	An RFI is produced to identify impacts or concerns from government and/or industry partners. An RFI is supplemented with an Advisory summarizing the responses received from the RFI. A SITREP is produced when an incident will require additional reporting.	NCC
30. NCC Watch Train Derailment Notifications	Notification of communications disruption disseminated to government and industry partners, as a result of an incident identification from the Department of Transportation Crisis Management Center.	NCC
31. Watch Global Positioning System (GPS) Testing Notices	Notification of a scheduled test in a geographical area to determine if there are equipment malfunctions or external problems (e.g. natural disaster) with a communications medium.	NCC
32. NCC Watch Bulletin/Notifications	Other alerts.	NCC
33. NCC 0900 Monday Weekly Call	Operations round table to discuss situation awareness with members of the communications infrastructure.	NCC
34. NCC Event Infrastructure Analysis	An assessment of communications in a specific area that is either supportive or could be affected by the scheduled event.	NCC
35. Request for Information Response	An entity requests information from NCCIC and the Watch Floor responds if it can and/or it provides the request to the appropriate NCCIC component.	NCCIC Watch Floor
36. NCCIC Analysis Product (i.e. Weekly Analysis Synopsis Product)	NCCIC analysis products for special events (e.g. the Super Bowl) or malware.	NCCIC Watch Floor
37. External Exercises	Exercises that include federal, state local tribal, territorial, private, and international partners and range from individual table-top exercises to multi-organization exercises. Other examples are when NCCIC is asked to teach an entity how to conduct exercises, manage a cyber exercise or provide analysis on an exercise already completed.	NCCIC Watch Floor
38. National Level Exercises	Exercises that are longer and orders of magnitude more costly than a regular exercise and include thousands of participants. Examples include Cyberstorm and Cyberguard.	NCCIC Watch Floor
39. Tours	Classified and unclassified tours of the NCCIC floor including an operations briefing on how NCCIC accomplishes its mission.	NCCIC Watch Floor
40. Cyber Hygiene Scan Reports	Automated weekly reports for customers who requested NCCIC to continuously scan for vulnerabilities.	NCCIC Watch Floor
41. Watch Floor Situational Reports and Situational Assessments	Reports delivered after an incident has occurred based on what NCCIC knows and does not know regarding the incident. Reports are tailored for specific sectors and may be updated when further analysis has been conducted by NCCIC.	NCCIC Watch Floor
42. Information Sharing and Liaison Services	Vehicles by which federal and nonfederal entities are able to become a part of the NCCIC watch floor, such as Memoranda of Agreement or Cooperative Research and Development Agreements.	NCCIC Watch Floor

NCCIC Product or Service	Description	NCCIC Component
43. Risk & Vulnerability Assessments	Penetration testing requested from an entity that provides the entity with knowledge on how to harden their security and identify the signs that an attacker is on their network.	NCCIC Watch Floor

Source: GAO Analysis of Department of Homeland Security data | GAO-18-62

Appendix III: Summary of Department of Homeland Security Complete Risk Assessments for Critical Infrastructure

The following tables highlight complete risk assessments regularly conducted by the Transportation Security Administration and the U.S. Coast Guard within the Transportation Systems sector.

Table 6: Summary of the Transportation Security Administration's (TSA) 2016 Transportation Sector Security Risk Assessment (TSSRA)

Complete Assessment Actors and Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
TSA	
Transportation Sector Security Risk Assessment (TSSRA)[a]	TSA's annual report on transportation security establishes risk scores and assesses threat, vulnerability, and consequence for various attack scenarios across the five transportation modes for which TSA is responsible. **Threat:** As part of each TSSRA process, TSA considers threat actors that pose, or may pose, a risk to U.S. transportation security. Threat estimates for the TSSRA are provided by TSA's Office of Intelligence and Analysis, which evaluates the intent and capability of homegrown violent extremists, as well as transnational extremists, such as al-Qaeda and its affiliates. **Vulnerability:** TSA compiles vulnerabilities for each transportation mode through engagement with subject matter experts from TSA, as well as industry stakeholder representatives from each mode. Each mode has a separate session to discuss countermeasures and provide input for the TSSRA team to determine a range of vulnerabilities for their respective mode. **Consequence:** TSA has assessed consequence through the TSSRAs by analyzing both direct and indirect consequences of the various attack scenarios. According to the TSSRA, direct consequences (or impacts) include the immediate economic result of an attack such as deaths, injuries, and infrastructure damage. Indirect consequences are the secondary macro- and micro-economic impacts on industries and consumers.

Source: GAO analysis of TSA's 2016 Transportation Sector Security Risk Assessment. I GAO-18-62

[a]According to TSA, the TSSRA was developed both in response to direction by Congress to conduct risk assessments for the Transportation Systems sector and to fulfill TSA's operational and strategic need for a comprehensive risk assessment to aid in planning, risk-based decision making, and resource allocation. See, e.g., Pub. L. No. 110-53, § 1511, 121 Stat. 426-29 (2007); 6 U.S.C. § 1161 (requiring the submission of a nationwide risk assessment of a terrorist attack on railroad carriers).

Table 7: Summary of the U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) Vulnerability and Consequence Assessments

MSRAM Assessment Products/Activities	Explanation and Information Sharing Mechanism (if applicable)
U.S. Coast Guard	
Vulnerability assessment factors	**Achievability:** A measure of the ability to successfully attack the target in the absence of security measures. This factor is designed to capture the innate degree of difficulty of the attack on a target. For example, weather or climate requirements for the scenario (wind, temperature, etc.) may alter the potential likelihood of the attack. **System security:** A measure of the probability that the security strategy in place, made up of the owner/operator, law enforcement agencies, or the Coast Guard, will successfully interdict a terrorist attack before it occurs. **Target hardness:** A measure of the target's ability to physically withstand the specific attack type.
Consequence assessment factors	**Death/injury:** Represents the expected number of deaths/injuries from a successful attack. This includes both deaths at the time of attack, and deaths that occur later but are still clearly a direct result of the attack (e.g., burn victims, or victims who become sick and die from exposure to chemical or biological agents). **Economic – primary:** Represents the expected property damage and immediate business interruption from a successful attack. This includes the actual costs of replacing or repairing maritime infrastructure, as well as business losses resulting from the attack. **Environmental:** Represents the expected environmental impacts of a successful attack. This impact predominately captures impacts from oil and oil-like substances. **National security:** Represents the expected impact of a successful attack on a target involved in providing national security. **Symbolic:** Represents the symbolic impact of a successful attack based on the iconic value of the target in terms of its local, regional, national, and international importance. **Economic – secondary:** Represents the expected follow-on economic effects of a successful attack. For example, an attack on a fuel refinery could interrupt energy production and distribution, which is considered a secondary economic effect. This assessment should take into account redundancy and recoverability of the target.

Source: U.S. Coast Guard. I GAO-18-62

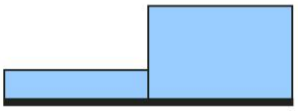
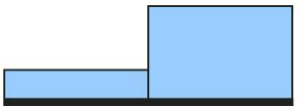
Appendix IV: National Critical Infrastructure Prioritization Program Consequence-Based Criteria and Relative Thresholds

Figure 7 below illustrates the Department of Homeland Security's (DHS) approach for prioritizing the list of systems and assets that the Secretary of Homeland Security determines would, if destroyed or disrupted, cause national or regional catastrophic effects.[1] DHS has prioritized these CI assets into different levels according to their criticality, to inform their outreach to owners and operators.[2] Consistent with the National Infrastructure Protection Plan risk management framework, the criteria for determining which level each asset is assigned to on the National Critical Infrastructure Prioritization Program (NCIPP) list are entirely consequence based thresholds and include fatalities, economic loss, mass evacuation length, or national security impacts.

[1]See 6 U.S.C. § 124*l*(a)(2). According to DHS officials, the Secretary of Homeland Security delegated responsibility for developing the NCIPP list to the Assistant Secretary for Infrastructure Protection.

[2] Level 1 assets are nationally critical; Level 2 assets are state and regionally critical.

Figure 7: National Critical Infrastructure Prioritization Program (NCIPP) Consequence-Based Criteria and Relative Thresholds

NCIPP criteria	Thresholds[a]
Prompt fatalities Number of fatalities that occur immediately following an event as a direct result of the scenario; does not include injuries, illnesses, or future development of life-threatening ailments.	 Level 2 Level 1
Economic consequences First-year direct and indirect costs following an incident. Costs may include evacuation and response efforts, asset replacement, downstream costs resulting from disruption of product or service, and long-term costs resulting from environmental damage, but may not include monetary value for fatalities.	 Level 2 Level 1
Mass evacuation length Evacuation of a substantial portion of an urban area for an extended period of time as a result of the loss of infrastructure, not the nature of an event. Evacuation is related to permanent residents only and does not include transient populations such as commuters or tourists.	 Level 2 Level 1
National security Severe degradation of the country's national security capabilities.	No level-specific thresholds

Source: GAO analysis of Department of Homeland Security documents. | GAO-18-62

[a]A scale for this graphic is not provided because the exact thresholds for the NCIPP criteria are designated "for official use only."

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Chris Currie, at (404) 679-1875 or CurrieC@gao.gov

Staff Acknowledgments

In addition to the contact named above, Ben Atwater (Assistant Director) and Landis Lindsey (Analyst-in-Charge) managed this audit engagement. Chuck Bausell, Michele Fejfar, Daniel Glickstein, Tracey King, Steve Komadina, Tom Lombardi, Kush Malhotra, Gabrielle Matuzsan, and Claire Peachey made significant contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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