United States Government Accountability Office

Testimony
Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 12, 2016

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed

Statement of Chris Currie, Director
Homeland Security and Justice

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed

Why GAO Did This Study

Protecting the security of CI is a top priority for the nation. CI includes assets and systems, whether physical or cyber, that are so vital to the United States that their destruction would have a debilitating impact on, among other things, national security or the economy. Multiple federal entities, including DHS, are involved in assessing CI vulnerabilities, and assessment fatigue could impede DHS's ability to garner the participation of CI owners and operators in its voluntary assessment activities.

This testimony summarizes past GAO findings on progress made and improvements needed in DHS's vulnerability assessments, such as addressing potential duplication and gaps in these efforts.

This statement is based on products GAO issued from May 2012 through October 2015 and recommendation follow-up conducted through March 2016. GAO reviewed applicable laws, regulations, directives, and policies from selected programs. GAO interviewed officials responsible for administering these programs and assessed related data. GAO interviewed and surveyed a range of stakeholders, including federal officials, and CI owners and operators.

What GAO Recommends

GAO made recommendations to DHS in prior reports to strengthen its assessment efforts. DHS agreed with these recommendations and reported actions or plans to address them. GAO will continue to monitor DHS efforts to address these recommendations.

View GAO-16-791T. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

GAO's prior work has shown the Department of Homeland Security (DHS) has made progress in addressing barriers to conducting voluntary assessments but guidance is needed for DHS's critical infrastructure (CI) vulnerability assessments activities and to address potential duplication and gaps. For example:

Determining why some industry partners do not participate in voluntary assessments. In May 2012, GAO reported that various factors influence whether CI owners and operators participate in voluntary assessments that DHS uses to identify security gaps and potential vulnerabilities, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority CI declined to participate. GAO concluded that collecting data on the reason for declinations could help DHS take steps to enhance the overall security and resilience of high-priority CI crucial to national security, public health and safety, and the economy, and made a recommendation to that effect. DHS concurred and has taken steps to address the recommendation, including developing a tracking system in October 2013 to capture declinations.

Establishing guidance for areas of vulnerability covered by assessments. In September 2014, GAO reported that the vulnerability assessment tools and methods DHS offices and components use vary with respect to the areas of vulnerability—such as perimeter security—assessed depending on which DHS office or component conducts or requires the assessment. As a result it was not clear what areas DHS believes should be included in its assessments. GAO recommended that DHS review its vulnerability assessments to identify the most important areas of vulnerability to be assessed, and establish guidance, among other things. DHS agreed and established a working group in August 2015 to address this recommendation. As of March 2016 these efforts were ongoing with a status update expected in the summer of 2016.

Addressing the potential for duplication, overlap, or gaps between and among the various efforts. In September 2014, GAO found overlapping assessment activities and reported that DHS lacks a department-wide process to facilitate coordination among the various offices and components that conduct vulnerability assessments or require assessments on the part of owners and operators. This could hinder the ability to identify gaps or potential duplication in DHS assessments. GAO identified opportunities for DHS to coordinate with other federal partners to share information regarding assessments. In response to GAO recommendations, DHS began a process of identifying the appropriate level of guidance to eliminate gaps or duplication in methods and to coordinate vulnerability assessments throughout the department. GAO also recommended that DHS identify key CI security-related assessment tools and methods used or offered by other federal agencies, analyze them to determine the areas they capture, and develop and provide guidance for what areas should be included in vulnerability assessments of CI that can be used by DHS and other CI partners in an integrated and coordinated manner. DHS agreed, and as of March 2016, established a working group to address GAO recommendations.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

Thank you for the opportunity to discuss the Department of Homeland Security's (DHS) efforts to assess critical infrastructure vulnerabilities. Critical infrastructure (CI) includes assets and systems, whether physical or cyber, that are so vital to the United States that their incapacity or destruction would have a debilitating impact on, among other things, national security or the economy.[1]

Protecting the security of our critical infrastructure is a top priority for the nation. For example, in 2013, the President issued Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience to increase the overall security and resilience of U.S. critical infrastructure.[2] In addition, in 2013, DHS issued an update to its National Infrastructure Protection Plan (NIPP),[3] which provides the overarching approach for integrating the nation's critical infrastructure security and resilience activities into a single national effort.[4] A fundamental component of DHS's efforts to protect and secure our nation's infrastructure is its reliance on voluntary collaboration between private sector owners and operators of critical infrastructure and their government counterparts. The NIPP outlines the roles and responsibilities of DHS with regard to critical infrastructure protection and resilience and sector-specific agencies (SSA)—federal departments and agencies responsible for critical infrastructure protection and resilience activities in 16 critical infrastructure sectors. Sectors include the commercial facilities, energy, and transportation sectors. Appendix I lists the 16 CI sectors and their SSAs.

Over the last several years, DHS has taken actions to assess vulnerabilities at CI facilities and within groups of related infrastructure,

---

[1]See 42 U.S.C. § 5195c(e).

[2]*Presidential Policy Directive-21—Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[3]See DHS, *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013), which is an update to previous versions of the NIPP.

[4]According to DHS, in this context, resilience is the ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions. See DHS, Risk Steering Committee, *DHS Risk Lexicon* (Washington, D.C.: September 2010).

regions, and systems. According to DHS, a vulnerability assessment is a process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard that has the potential to harm life, information, operations, the environment, or property.[5]

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, some of which are voluntary, and that DHS needed to enhance integration and coordination of these efforts.[6] Specifically, DHS officials representing the National Protection and Programs Directorate (NPPD), Transportation Security Administration (TSA), and the Coast Guard conducted more than 5,300 assessments using six different voluntary assessment tools and methods covering various types of assets and systems.[7] During the same time period, as many as 7,600 asset owners and operators were required to perform self-assessments to comply with Coast Guard requirements pursuant to

---

[5]According to the NIPP, vulnerabilities may be associated with physical (e.g., no barriers or alarm systems), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors. A vulnerability assessment can be a stand-alone process or part of a full risk assessment and 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. For the purposes of this testimony, we use the term "tools and methods" when referring to specific survey questionnaires or tools that DHS offices and components and other federal agencies use in conducting vulnerability assessments or in offering self-assessments to CI owners and operators. These tools and methods contain various areas that can be assessed for vulnerabilities, such as perimeter security, entry controls, and cybersecurity, among others.

[6]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).

[7]During the early stages of our review, NPPD, TSA, and Coast Guard officials identified various assessment tools and methods. We further analyzed these 10 assessment tools and methods because based on our preliminary work, these tools and methods contained two or more areas assessed for vulnerability, such as perimeter security, or the presence of a security force. Tools and methods include the Infrastructure Survey Tool (IST), Site Assistance Visit (SAV), Chemical Security Assessment Tool Security Vulnerability Assessment (CSAT SAV), and Modified Infrastructure Survey Tool (MIST) from NPPD; the Baseline Assessment for Security Enhancements (BASE). Freight Rail Risk Analysis Tool, Pipeline Security Critical Facility Security Reviews (CFSR) and Joint Vulnerability Assessment (JVA) from TSA; and Port Security Assessments and Maritime Transportation Security Act (MTSA)-regulated facility vulnerability assessments performed by the Coast Guard.

Maritime Transportation Security Act (MTSA)[8] and NPPD's Infrastructure Security Compliance Division (ISCD) requirements pursuant to Chemical Facility Anti-Terrorism Standards (CFATS).[9]

My testimony today describes (1) progress made by DHS in addressing barriers to conducting voluntary assessments and sharing information, and (2) the extent to which DHS provided guidance for DHS's CI vulnerability assessment activities and to address potential duplication and gaps in assessment efforts. This statement is based on products we issued from May 2012 to October 2015 on factors to consider when reorganizing, and recommendation follow-up activities conducted through March 2016 related to multiple aspects of DHS's efforts to assess critical infrastructure and provide information to CI owners and operators to help them enhance the security of their facilities.[10] To perform the work for our previous reports, among other things, we reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs to protect critical infrastructure. We interviewed DHS officials responsible for administering these programs and obtained and assessed data on the conduct and management of DHS's security-related programs. We also interviewed and surveyed a range of other stakeholders, including federal officials, industry owners and operators, and CI experts. Further details on the scope and methodology for the previously issued reports are available within each of the published products. In addition, after the issuance of our reports and through March 2016 we contacted DHS to obtain updated information and documentation, as appropriate, on the status of recommendations we made as part of our ongoing recommendation follow up activities.

---

[8]See Pub L. No. 107-295, 116 Stat. 2064 (2002).

[9]See 6 C.F.R. pt. 27; Department of Homeland Security Appropriations Act, 2007. Pub. L. No. 109-295, tit. V. § 550, 120 Stat. 1355, 1388-89 (2006).

[10]GAO, *National Protection and Programs Directorate: Factors to Consider when Reorganizing,* GAO-16-140T (Washington, D.C.: Oct. 7, 2015); *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach,* GAO-14-464T (Washington, D.C.: Mar. 26, 2014); *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*, GAO-13-616 (Washington, D.C.: July 30, 2013); GAO-14-507; *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 (Washington, D.C.: Mar. 25, 2013); and *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

We conducted the work on which this statement is based 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal law and policy have established roles and responsibilities for federal agencies to coordinate with industry in enhancing the security and resilience of critical government and industry infrastructures. According to the Homeland Security Act of 2002, as amended, DHS is to, among other things, carry out comprehensive vulnerability assessments of CI; integrate relevant information, analyses, and assessments from within DHS and from CI partners; and use the information collected to identify priorities for protective and support measures. Assessments include areas that can be assessed for vulnerability (hereinafter referred to as "areas"), such as perimeter security, the presence of a security force, or vulnerabilities to intentional acts, including acts of terrorism. Presidential Policy Directive/PPD-21 directs DHS to, among other things, provide strategic guidance, promote a national unity of effort, and coordinate the overall federal effort to promote the security and resilience of the nation's CI. Related to PPD-21, the NIPP calls for the CI community and associated stakeholders to carry out an integrated approach to (1) identify, deter, detect, disrupt, and prepare for threats and hazards (all hazards); (2) reduce vulnerabilities of critical assets, systems, and networks; and (3) mitigate the potential consequence to CI to incidents or events that do occur. According to the NIPP, CI partners are to identify risk in a coordinated and comprehensive manner across the CI community; minimize duplication; consider interdependencies; and, as appropriate, share information within the CI community.

Within DHS, NPPD is responsible for working with public and industry infrastructure partners and leads the coordinated national effort to mitigate risk to the nation's infrastructure through the development and implementation of the infrastructure security program. NPPD's Office of Infrastructure Protection (IP) has overall responsibility for coordinating implementation of the NIPP across the 16 CI sectors, including providing guidance to SSAs and CI owners and operators on protective measures

to assist in enhancing the security of infrastructure and helping CI sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to the assets.[11] The NIPP also designates other federal agencies, as well as some offices and components within DHS, as SSAs that are responsible for, among other things, coordinating with DHS and other federal departments and agencies and CI owners and operators to identify vulnerabilities, and to help mitigate incidents, as appropriate. DHS offices and components or asset owners and operators have used various assessment tools and methods, some of which are voluntary, while others are required by law or regulation, to gather information about certain aspects of CI. For example, Protective Security Coordination Division (PSCD), within NPPD, relies on Protective Security Advisors (PSA)[12] to offer and conduct voluntary vulnerability assessments to owners and operators of CI to help identify potential security actions; Infrastructure Security Compliance Division, within NPPD, requires regulated chemical facilities to complete a security vulnerability assessment pursuant to CFATS;TSA conducts various assessments of airports, pipelines, and rail and transit systems;[13] and Coast Guard requires facilities it regulates under the Maritime Transportation Security Act of 2002 (MTSA) to complete assessments as part of their security planning process.[14] In addition, SSAs external to DHS also offer vulnerability assessment tools and methods to owners or operators of CI and these assessments include areas such as resilience management or perimeter security. For example, the Environmental Protection Agency, the SSA for the water sector, provides a self-assessment tool for the conduct of voluntary security-related assessments at water and wastewater facilities.

---

[11]A delegation memo to the Undersecretary for NPPD delineates the directorate's roles and responsibilities.

[12]As of July 2016, DHS has deployed 89 PSAs in all 50 states, Puerto Rico, and the nation's capital region to, among other things, conduct outreach with state and local partners and asset owners and operators who participate in DHS's voluntary CI protection and resiliency efforts.

[13]See, e.g., 49 U.S.C. § 44904; Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996).

[14]See Pub L. No. 107-295, 116 Stat. 2064 (2002); 33 C.F.R. §§ 105.300-.310.

Progress Made Addressing Barriers to Conducting Voluntary Assessments and Sharing Information

DHS's took steps to address barriers to conducting critical infrastructure vulnerability assessments and sharing information, in response to findings from our previous work. Specifically, DHS has made progress in the following areas:

Determining why some industry partners do not participate in voluntary assessments. DHS supports the development of the national risk picture by conducting vulnerability assessments and security surveys to identify security gaps and potential vulnerabilities in the nation's high-priority critical infrastructure.[15] In a May 2012 report, we assessed the extent to which DHS had taken action to conduct security surveys using its Infrastructure Survey Tool (IST) and vulnerability assessments among high-priority infrastructure, shared the results of these surveys and assessments with asset owners or operators, and assessed their effectiveness.[16]

We found that various factors influence whether industry owners and operators of assets participate in these voluntary programs, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority assets declined to participate in security surveys or vulnerability assessments. We concluded that collecting data on the reason for declinations could help DHS take steps to enhance the overall protection and resilience of those high-priority critical infrastructure assets crucial to national security, public health and safety, and the economy. We recommended, and DHS concurred, that DHS design and implement a mechanism for systematically assessing why owners and operators of high-priority assets decline to participate.

In response to our recommendations, in October 2013 DHS developed and implemented a tracking system to capture and account for declinations. In addition, in August 2014 DHS established a policy to conduct quarterly reviews to, among other things, track these and other survey and assessment programs and identify gaps and requirements for

---

[15]DHS vulnerability assessments are conducted during site visits at individual assets and are used to identify security gaps and provide options for consideration to mitigate these identified gaps. DHS security surveys are intended to gather information on an asset's current security posture and overall security awareness. Security surveys and vulnerability assessments are generally asset-specific and are conducted at the request of asset owners and operators.

[16]GAO-12-378.

priorities and help DHS better understand what barriers owners and operators of critical infrastructure face in making improvements to the security of their assets.

Sharing of assessment results at the asset level in a timely manner. DHS security surveys and vulnerability assessments can provide valuable insights into the strengths and weaknesses of assets and can help asset owners and operators that participate in these programs make decisions about investments to enhance security and resilience. In our May 2012 report, we found that, among other things, DHS shared the results of security surveys and vulnerability assessments with asset owners or operators.[17] However, we also found that the usefulness of security survey and vulnerability assessment results could be enhanced by the timely delivery of these products to the owners and operators. We reported that the inability to deliver these products in a timely manner could undermine the relationship DHS was attempting to develop with these industry partners. Specifically, we reported that, based on DHS data from fiscal year 2011, DHS was late meeting the 30-day time frame for delivering the results of its security surveys required by DHS guidance 60 percent of the time. DHS officials acknowledged the late delivery of survey and assessment results and said they were working to improve processes and protocols. However, DHS had not established a plan with time frames and milestones for managing this effort. We recommended, and DHS concurred, that it develop time frames and specific milestones for managing its efforts to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners and operators. In response to our recommendation, DHS established timeframes and milestones to ensure the timely delivery of assessment results of the surveys and assessments to CI owners and operators. In addition, in February 2013, DHS transitioned to a web-based delivery system, which, according to DHS, has since resulted in a significant drop in overdue deliveries.

Sharing certain information with critical infrastructure partners at the regional level. Our work has shown that over the past several years, DHS has recognized the importance of and taken actions to examine critical infrastructure asset vulnerabilities, threats, and potential consequences across regions. In a July 2013 report, we examined DHS's

---

[17]GAO-12-378.

management of its Regional Resiliency Assessment Program (RRAP)—a voluntary program intended to assess regional resilience of critical infrastructure by analyzing a region's ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions—and found that DHS has been working with states to improve the process for conducting RRAP projects, including more clearly defining the scope of these projects.[18] We also reported that DHS shares the project results of each RRAP project report, including vulnerabilities identified, with the primary stakeholders—officials representing the state where the RRAP was conducted—and that each report is generally available to SSAs and protective security advisors within DHS.[19]

Sharing information with sector-specific agencies and state and local governments. Federal SSAs and state and local governments are key partners that can provide specific expertise and perspectives in federal efforts to identify and protect critical infrastructure. In a March 2013 report, we reviewed DHS's management of the National Critical Infrastructure Prioritization Program (NCIPP), and how DHS worked with states and SSAs to develop the high-priority CI list.[20] The program identifies a list of nationally significant critical infrastructure each year that is used to, among other things, prioritize voluntary vulnerability assessments conducted by PSAs on high-priority critical infrastructure. We reported that DHS had taken actions to improve its outreach to SSAs and states in an effort to address challenges associated with providing input on nominations and changes to the NCIPP list. However, we also found that most state officials we contacted continued to experience challenges with nominating assets to the NCIPP list using the consequence-based criteria developed by DHS. Among other actions, we recommended that DHS commission an independent, external peer review of the NCIPP with clear project objectives. In November 2013, DHS commissioned a panel that reviewed the NCIPP process, guidance documentation, and process phases to provide an evaluation of the extent to which the process is comprehensive, reproducible, and defensible. The panel made 24 observations about the NCIPP; however, panel members expressed different views regarding the classification of

---

[18]GAO-13-616.

[19]A protective security advisor is a DHS field representative. Among other things, they conduct RRAP projects.

[20]GAO-13-296.

the NCIPP list, and views on whether private sector owners of the assets, systems, and clusters should be notified of inclusion on the list. As of August 2014, DHS officials reported that they are exploring options to streamline the process and limit the delay of dissemination among those who have a need-to-know.

Guidance and Coordination to Address Potential Duplication and Gaps Needed for CI Vulnerability Assessment Activities

Our previous work identified a need for DHS vulnerability assessment guidance and coordination. Specifically, we found:

Establishing guidance for areas of vulnerability covered by assessments. In a September 2014 report examining, among other things, the extent to which DHS is positioned to integrate vulnerability assessments to identify priorities, we found that the vulnerability assessment tools and methods DHS offices and components use vary with respect to the areas assessed depending on which DHS office or component conducts or requires the assessment.[21] As a result, it was not clear what areas DHS believes should be included in a comprehensive vulnerability assessment. Moreover, we found that DHS had not issued guidance to ensure that the areas it deems most important are captured in assessments conducted or required by its offices and components. Our analysis of 10 vulnerability assessment tools and methods showed that DHS vulnerability assessments consistently included some areas that were assessed for vulnerability but included other areas that were not consistently assessed. Our analysis showed that all 10 of the DHS assessment tools and methods we analyzed included areas such as "vulnerabilities from intentional acts"—such as terrorism—and "perimeter security" in the assessment. However, 8 of the 10 assessment tools and methods did not include areas such as "vulnerabilities to all hazards" such as hurricanes or earthquakes while the other 2 did. These differences in areas assessed among the various assessment tools and methods could complicate or hinder DHS's ability to integrate relevant assessments in order to identify priorities for protective and support measures.

We found that the assessments conducted or required by DHS offices and components also varied greatly in their length and the detail of information to be collected. For example, within NPPD, PSCD used its IST to assess high-priority facilities that voluntarily participate and this tool

---

[21]GAO-14-507.

was used across the spectrum of CI sectors. The IST, which contains more than 100 questions and 1,500 variables, is used to gather information on the security posture of CI, and the results of the IST can inform owners and operators of potential vulnerabilities facing their asset or system. In another example from NPPD, ISCD required owners and operators of facilities that possess, store, or manufacture certain chemicals under CFATS to provide data on their facilities using an online tool so that ISCD can assess the risk posed by covered facilities. This tool, ISCD's Chemical Security Assessment Tool Security Vulnerability Assessment contained more than 100 questions based on how owners respond to an initial set of questions. Within DHS, TSA's Office of Security Operations offered or conducted a number of assessments, such as a 205-question assessment of transit systems called the Baseline Assessment for Security Enhancements that contained areas to be assessed for vulnerability, and TSA's 17-question Freight Rail Risk Analysis Tool was used to assess rail bridges.

In addition to differences in what areas were included, there were also differences in the detail of information collected for individual areas, making it difficult to determine the extent to which the information collected was comparable and what assumptions and/or judgments were used while gathering assessment data. We also observed that components used different questions for the same areas assessed. These variations, among others we identified, could impede DHS's ability to integrate relevant information and use it to identify priorities for protective and support measures regarding terrorist and other threats to homeland security. For example, we found that while some components asked open-ended questions such as "describe security personnel," others included drop-down menus or lists of responses to be selected.

We recommended that DHS review its vulnerability assessments to identify the most important areas to be assessed, and determine the areas and level of detail that are necessary to integrate assessments and enable comparisons, and establish guidance, among other things. DHS agreed with our recommendation, and established a working group in August 2015 to address this recommendation and others we made. As of March 2016 these efforts are ongoing and DHS intends to provide an update in the summer of 2016.
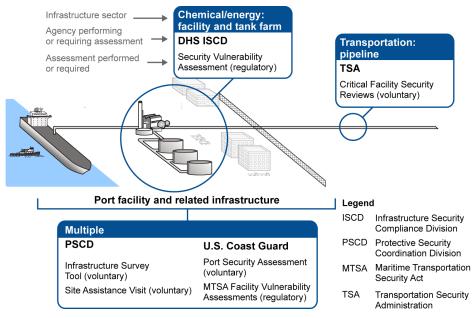
Establishing guidance on common data standards to help reduce assessment fatigue and improve information sharing. As we reported in September 2014, federal assessment fatigue could impede DHS's ability to garner the participation of CI owners and operators in its

voluntary assessment activities. During our review of vulnerability assessments, the Coast Guard, PSCD, and TSA field personnel we contacted reported observing what they called federal fatigue, or a perceived weariness among CI owners and operators who had been repeatedly approached or required by multiple federal agencies and DHS offices and components to participate in or complete assessments. One official who handles security issues for an association representing owners and operators of CI expressed concerns at the time about his members' level of fatigue. Specifically, he shared observations that DHS offices and components do not appear to effectively coordinate with one another on assessment-related activities to share or use information and data that have already been gathered by one of them. The official also noted that, from the association's perspective, the requests and invitations to participate in assessments have exceeded what is necessary to develop relevant and useful information, and information is being collected in a way that is not the best use of the owners' and operators' time. As figure 1 illustrates, depending on a given asset or facility's operations, infrastructure, and location, an owner or operator could be asked or required to participate in multiple separate vulnerability assessments.

Figure 1: Example of a Critical Infrastructure (CI) Asset or Facility Potentially Subject to Multiple Assessment Efforts by Department of Homeland Security (DHS) Offices and Components

Infrastructure sector

Agency performing or requiring assessment

Assessment performed or required

Chemical/energy: facility and tank farm

DHS ISCD

Security Vulnerability Assessment (regulatory)

Transportation: pipeline

TSA

Critical Facility Security Reviews (voluntary)

Port facility and related infrastructure

Multiple

PSCD

Infrastructure Survey Tool (voluntary)

Site Assistance Visit (voluntary)

U.S. Coast Guard

Port Security Assessment (voluntary)

MTSA Facility Vulnerability Assessments (regulatory)

Legend

ISCD — Infrastructure Security Compliance Division

PSCD — Protective Security Coordination Division

MTSA — Maritime Transportation Security Act

TSA — Transportation Security Administration

Source: GAO analysis of DHS data. | GAO-16-791T

Note: Under Chemical Facility Anti-Terrorism Standards (CFATS) implementing regulations, CFATS would not apply to facilities that are regulated by the Coast Guard under MTSA. See 6 C.F.R. § 27.110(b).

DHS officials expressed concern at the time that this "fatigue" may diminish future cooperation from asset owners and operators. We recommended in September 2014 that DHS develop an approach for consistently collecting and maintaining data from assessments conducted across DHS to facilitate the identification of potential duplication and gaps in coverage. Having common data standards would better position DHS offices and components to minimize the aforementioned fatigue, and the resulting declines in CI owner and operator participation, by making it easier for DHS offices and components to use each other's data to determine what CI assets or facilities may have been already visited or assessed by another office or component. They could then plan their assessment efforts and outreach accordingly to minimize the potential for making multiple visits to the same assets or facilities. DHS agreed with our recommendation, and as of March 2016 DHS had established a working group to address the recommendations from our report and planned to provide us with a status update in the summer of 2016.

Addressing the potential for duplication, overlap, or gaps between and among the various efforts. As with the sharing of common assessment data, we found in our 2014 review of vulnerability assessments that DHS also lacks a department-wide process to facilitate coordination among the various offices and components that conduct vulnerability assessments or require assessments on the part of owners and operators.[22] This could hinder the ability to identify gaps or potential duplication in DHS assessments. For example, among 10 different types of DHS vulnerability assessments we compared, we found that DHS assessment activities were overlapping across some of the sectors, but not others. Given the overlap of DHS's assessments among many of the 16 sectors, we attempted to compare data to determine whether DHS had conducted or required vulnerability assessments at the same critical infrastructure within those sectors. However, we were unable to conduct this comparison because of differences in the way data about these activities were captured and maintained.[23] Officials representing DHS acknowledged at the time they encountered challenges with the consistency of assessment data and stated that DHS-wide interoperability standards did not exist for them to follow in recording their assessment activities that would facilitate consistency and enable comparisons among the different data sets.

The NIPP calls for standardized processes to promote integration and coordination of information sharing through, among other things, jointly developed standard operating procedures. However, DHS officials stated at the time that they generally relied on field-based personnel to inform their counterparts at other offices and components about planned assessment activities and share information as needed on what assets may have already been assessed. For example, PSAs may inform and invite CI partners to participate in these assessments, if the owner and operator of the asset agrees. PSAs may also alert their DHS counterparts depending on assets covered and their areas of responsibility. However, we found that absent these field-based coordination or sharing activities, it was unclear whether all facilities in a particular geographic area or

---

[22]GAO-14-507.

[23]Data sets used by DHS offices and components did not share common formats or defined data standards. For example, infrastructure names and addresses generally were not entered in a standardized way or were not available in some cases in a way that would allow us to identify matches across data sets. See GAO-14-507.

sector were covered. For example, after CFATS took effect, in 2007, ISCD officials asked PSCD to stop having PSAs conduct voluntary assessments at CFATS-regulated chemical facilities to reduce potential confusion about DHS authority over chemical facility security and to avoid overlapping assessments. In response, PSCD reduced the number of voluntary vulnerability assessments conducted in the chemical sector. However, one former ISCD official noted that without direct and continuous coordination between PSCD and ISCD on what facilities are being assessed or regulated by each division, this could create a gap in assessment coverage between CFATS-regulated facilities and facilities that could have participated in PSCD assessments given that the number of CFATS-regulated facilities can fluctuate over time.[24]

Without processes for DHS offices and components to share data and coordinate with each other in their CI vulnerability assessment activities, DHS cannot provide reasonable assurance that it can identify potential duplication, overlap, or gaps in coverage that could ultimately affect DHS's ability to work with its partners to enhance national CI security and resilience, consistent with the NIPP. We recommended in September 2014 that DHS develop an approach to ensure that vulnerability data gathered on CI be consistently collected and maintained across DHS to facilitate the identification of potential duplication and gaps in CI coverage. As of March 2016, DHS has begun a process of identifying the appropriate level of guidance to eliminate gaps or duplication in methods and to coordinate vulnerability assessments throughout the department.

We also recommended that DHS identify key CI security-related assessment tools and methods used or offered by SSAs and other federal agencies, analyze them to determine the areas of vulnerability they capture, and develop and provide guidance for what areas should be included in vulnerability assessments of CI that can be used by DHS and other CI partners in an integrated and coordinated manner. DHS concurred with our recommendations and stated that it planned to take a variety of actions to address the issues we identified, including conducting an inventory survey of the security-related assessment tools and methods used by SSAs to address CI vulnerabilities. As of March 2016, DHS has

---

[24]The number of facilities actively regulated under the Chemical Facility Anti-Terrorism Standards requirements can fluctuate over time because of facilities changing their regulated operations or the types and quantities of chemicals handled, new facilities being built, or older facilities being decommissioned, for example.

established a working group, consisting of members from multiple departments and agencies, to enhance the integration and coordination of vulnerability assessment efforts. These efforts are ongoing and we will continue to monitor DHS's progress in implementing these recommendations.

In addition to efforts to address our recommendations, DHS is in the process of reorganizing NPPD to ensure that it is appropriately positioned to carry out its critical mission of cyber and infrastructure security. Key priorities of this effort are to include greater unity of effort across the organization and enhanced operational activity to leverage the expertise, skills, information, and relationships throughout DHS. The NPPD reorganization presents DHS with an opportunity to engage stakeholders in decision-making and may achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation. It also presents DHS with an opportunity to mitigate potential duplication or gaps by consistently capturing and maintaining data from overlapping vulnerability assessments of CI and improving data sharing and coordination among the offices and components involved with these assessments.

Chairman Ratcliffe, Ranking Member Richmond, and members of the sub-committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contacts and Staff Acknowledgments

If you or your staff members have any questions about this testimony, 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 statement. Other individuals making key contributions to this work include Ben Atwater, Assistant Director; Andrew Curry, Analyst-in-Charge; and Peter Haderlein.

Appendix I: Critical Infrastructure Sectors

This appendix provides information on the 16 critical infrastructure (CI) sectors and the federal agencies responsible for sector security. The National Infrastructure Protection Plan (NIPP) outlines the roles and responsibilities of the Department of Homeland Security (DHS) and its partners—including other federal agencies. Within the NIPP framework, DHS is responsible for leading and coordinating the overall national effort to enhance security via 16 critical infrastructure sectors. Consistent with the NIPP, Presidential Decision Directive/PPD-21 assigned responsibility for the critical infrastructure sectors to sector-specific agencies (SSAs).[1] As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of sector partners to protect 10 of the 16 critical infrastructure sectors. Seven other federal agencies have sole or coordinated responsibility for the remaining 6 sectors. Table 1 lists the SSAs and their sectors.

Table 1: Critical Infrastructure Sectors and Sector-Specific Agencies (SSA)

Critical infrastructure sector	SSA(s)[a]
Food and agriculture	Department of Agriculture[b] and the Department of Health and Human Services[c]
Defense industrial base[d]	Department of Defense
Energy[e]	Department of Energy
Government facilities	Department of Homeland Security and the General Services Administration
Health care and public health	Department of Health and Human Services
Financial services	Department of the Treasury
Transportation systems	Department of Homeland Security and the Department of Transportation[f]
Water and wastewater systems[g]	Environmental Protection Agency

[1]Issued on February 12, 2013, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, purports to refine and clarify critical infrastructure related functions, roles, and responsibilities across the federal government, and enhance overall coordination and collaboration, among other things. Pursuant to Homeland Security Presidential Directive/HSPD-7 and the *National Infrastructure Protection Plan*, DHS had established 18 critical infrastructure sectors. PPD-21 subsequently revoked HSPD-7, and incorporated 2 of the sectors into existing sectors, thereby reducing the number of critical infrastructure sectors from 18 to 16. Plans developed pursuant to HSPD-7, however, remain in effect until specifically revoked or superseded.

Critical infrastructure sector	SSA(s)[a]
Commercial facilities Critical manufacturing Emergency services Nuclear reactors, materials, and waste Dams	Department of Homeland Security Office of Infrastructure Protection[h]
Chemical	
Information technology Communications	Office of Cyber Security and Communications[i]

Source: Presidential Policy Directive/PPD-21 | GAO-16-791T

[a]Presidential Policy Directive/PPD-21, released in February 2013, identifies 16 critical infrastructure sectors and designates associated federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA.

[b]The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[c]The Food and Drug Administration is the Department of Health and Human Services component responsible for food other than meat, poultry, and egg products and serves as the co-SSA.

[d]Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commanders of military forces, or military command and control procedures.

[e]The energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[f]Presidential Policy Directive/PPD- 21 establishes the Department of Transportation as co-SSA with the Department of Homeland Security (DHS) for the transportation systems sector. Within DHS, the U.S. Coast Guard and the Transportation Security Administration are the responsible components.

[g]The water sector includes drinking water.

[h]The Office of Infrastructure Protection is the DHS component responsible for the commercial facilities; critical manufacturing; emergency services; nuclear reactors, materials, and waste; dams; and chemical sectors.

[i]The Office of Cyber Security and Communications is the DHS component responsible for the information technology and communications sectors.