



July 12, 2016

Value of DHS' Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, United States House of Representatives, One Hundred Fourteenth Congress, Second Session

HEARING CONTENTS:

Member Statements

John Ratcliffe
Subcommittee Chairman
[View Statement](#)

Witnesses

Chris P. Currie
Director
Homeland Security and Justice Issues
U.S. Government Accountability Office
[View Testimony](#)

Andy Ozment
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
[View Testimony](#)

Caitlin Durkovich
Assistant Secretary
Office of Infrastructure Protection

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.



National Protection and Programs Directorate
U.S. Department of Homeland Security
[View Testimony](#)

Marcus L. Brown
Homeland Security Advisor
Director of the Office of Homeland Security
Commonwealth of Pennsylvania
[View Testimony](#)

Available Webcast(s)*:

The following webcast is a full hearing
[View Webcast](#)

Compiled From*:

<https://homeland.house.gov/hearing/value-dhs-vulnerability-assessments-protecting-nations-critical-infrastructure/>

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



**Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee**

*“Value of DHS’ Vulnerability Assessments in Protecting our Nation’s Critical Infrastructure”
July 12, 2016*

Remarks as Prepared

The Subcommittee meets today to examine how the Department of Homeland Security is fulfilling its important mission of protecting our nation’s critical infrastructure. We look forward to examining DHS’s capabilities in conducting physical and cybersecurity vulnerability assessments. The critical systems that are central to our daily lives are targeted every day by terrorists, nation states, and criminals. Taxpayer funds used to protect these systems must be invested wisely and must add value for owners and operators. Because threats to critical infrastructure are numerous and diverse, we’re interested in learning specifics about the strategy that guides DHS’ efforts in this area.

I want to thank our panel of experts for joining us so Congress can better understand the work being done in this area and the value of DHS’s vulnerability assessments and training.

For 12 years, the primary mission of the Office of Infrastructure Protection’s Protective Security Advisor Program has been the protection of critical infrastructure. Protective Security Advisors (PSAs) are regionally based in alignment with the ten FEMA regions. PSAs execute their primary mission through the planning, coordination and performance of security surveys, assessments and outreach activities to those critical infrastructure owners and operators that elect to participate in these voluntary programs. PSAs also support National Special Security Events, Special Event Activity Rating (SEAR) Level I and II events, and respond to incidents.

The mission I just described is enormous. And because it is voluntary in nature, its success hinges on stakeholder buy-in. Such buy-in requires strategic outreach and real value added for owners and operators of critical infrastructure. I am interested in hearing what strategy is guiding this important program and what metrics DHS is using to track and increase such value.

In 2014, DHS established the Critical Infrastructure Cyber Community Voluntary Program to help organizations address and improve their cybersecurity risk management. Additionally, DHS created the Cybersecurity Advisor Program, or CSA Program, to provide cybersecurity expertise and voluntary cybersecurity programs to critical infrastructure owners and operators. While the CSA Program is still in its infancy compared to the 12-year old PSA Program, the CSA mission of assisting our nation’s critical infrastructure owners and operators in strengthening their cyber hygiene is critically important. With the passage of the Cybersecurity Act of 2015 last December, we must ensure the CSA program is also guided by a strategic plan and is well-positioned to effectively lead DHS’s cyber engagement efforts for critical infrastructure.

Last month, this Committee unanimously passed the Cybersecurity and Infrastructure Protection Agency Act of 2016 (CIPA) to elevate the functions of our nation’s cybersecurity and critical infrastructure

protection into an operational component within DHS. The legislation recognizes the unique expertise required of both the cyber and physical aspects of the Agency's mission while also stressing the importance of enhanced collaboration and coordination between the cyber and physical missions.

The Government Accountability Office has reported extensively on DHS vulnerability assessment programs for critical infrastructure and identified challenges within DHS in 2013, 2014 and 2015. These reports included number of recommendations to increase the use and enhance the participation of stakeholders in these vulnerability assessments.

One particular area of concern found in the report was "federal fatigue," which results from a perceived weariness among the private sector who might be repeatedly approached or required by multiple federal agencies to engage in risk assessments. "Federal fatigue" is particularly alarming, as the PSA and CSA assessment programs at DHS depend entirely on voluntary participation.

Just last week, a review of the DHS's website for critical infrastructure vulnerability assessments found conflicting and outdated information. While errors like these appear insignificant, it's important to remember that these programs are voluntary, and if DHS can't handle basic promotion and marketing of the programs, I have concerns about the likelihood of private sector participation.

The Subcommittee believes both the CSA and PSA programs can be of great value for the protection of our nation's critical infrastructure; but a clear strategy, effective stakeholder outreach, and metrics of success are essential.

It is the hope of the Subcommittee that this hearing will clarify how DHS is working to address these issues. Further, given the relative infancy of the CSA program, the Subcommittee hopes to learn more about CS&C's plan to expand this program and would hope that lessons learned from the PSA Program are being incorporated. This Subcommittee is responsible not only for the oversight of DHS's functions but also for ensuring that it has the tools and necessary authorities to successfully meet its objectives. In that spirit, we welcome input as to how we can assist in this critical mission.

###



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

GAO Highlights

Highlights of [GAO-16-791T](#), a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

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

July 2016

CRITICAL INFRASTRUCTURE PROTECTION

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

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,

¹See 42 U.S.C. § 5195c(e).

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

³See 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.

⁴According 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

⁵According 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.

⁶GAO, Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts, [GAO-14-507](#) (Washington, D.C.: Sept. 15, 2014).

⁷During 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.

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

⁹See 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).

¹⁰GAO, *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.

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

¹²As 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.

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

¹⁴See 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

¹⁵DHS 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](#).

¹⁹A 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.

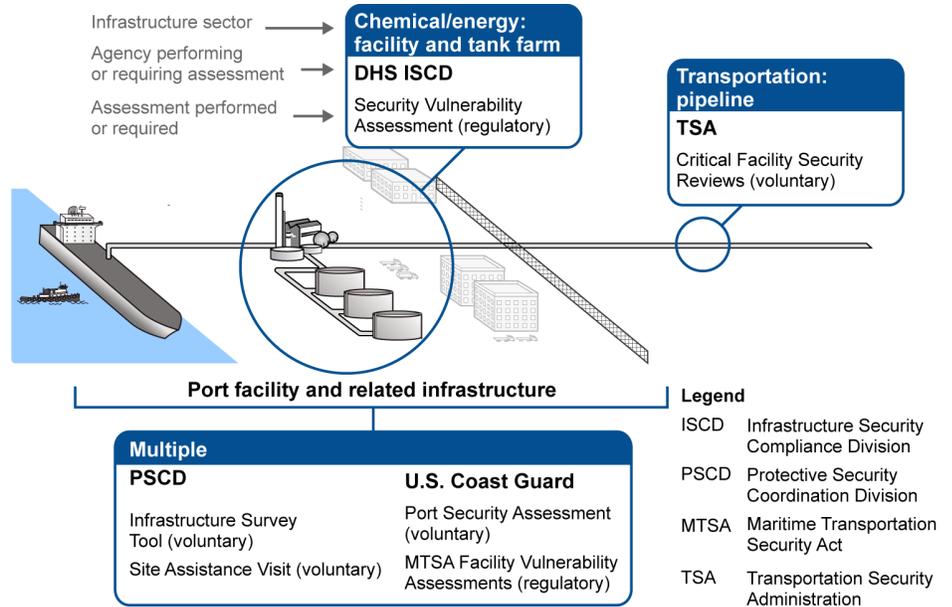
In addition to differences in what areas were included, there were also differences in the detail of information collected for individual areas, making it difficult to determine the extent to which the information collected was comparable and what assumptions and/or judgments were used while gathering 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



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](#).

²³Data 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

²⁴The 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

¹Issued 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.

Appendix I: Critical Infrastructure Sectors

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

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

^aPresidential 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.

^bThe Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

^cThe 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.

^dNothing 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.

^eThe energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

^fPresidential 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.

^gThe water sector includes drinking water.

^hThe 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.

ⁱThe Office of Cyber Security and Communications is the DHS component responsible for the information technology and communications sectors.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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

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



Please Print on Recycled Paper.

TESTIMONY

OF

CAITLIN DURKOVICH
ASSISTANT SECRETARY
OFFICE OF INFRASTRUCTURE PROTECTION
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

And

DR. ANDY OZMENT
ASSISTANT SECRETARY
OFFICE OF CYBERSECURITY AND COMMUNICATIONS
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE

THE

HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND
SECURITY TECHNOLOGIES

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

STAKEHOLDER ENGAGEMENT:
PROTECTIVE SECURITY ADVISORS AND CYBERSECURITY ADVISORS

JULY 12, 2016

I. Introduction

Chairman Ratcliffe, Ranking Member Richmond, thank you for the opportunity to appear before you today to discuss the crucial role that Protective Security Advisors (PSAs) and Cybersecurity Advisors (CSAs) serve in furthering the U.S. Department of Homeland Security's (DHS) mission to enhance the security and resilience of the nation's critical infrastructure in an all-hazards environment. We appreciate Congress' draft legislation that would stand up the National Protection and Programs Directorate (NPPD) as an operational component focused on cyber and infrastructure protection and further our holistic risk management approach.

PSAs and CSAs both support NPPD's operational mission by assisting State, local, territorial, and tribal (SLTT) governments and private sector customers in understanding and mitigating threats, vulnerabilities, and consequences affecting the provision of essential functions, goods, and services. PSAs and CSAs achieve this end through information sharing, capacity building, and direct assistance. The risks that our stakeholders face are cyber and physical, natural and man-made. Some risks blur the distinction between cyber and physical, such as space weather or electromagnetic pulse, while others combine aspects of cyber and physical risk: cyber-attacks causing physical impacts, natural disasters impacting communication networks, or man-made attacks on lifeline critical infrastructure. The proposed realignment, which was included in NPPD's draft reorganization proposal, will further the ability of our cybersecurity experts and physical security experts to work side-by-side, ensuring that risks to critical infrastructure are fully assessed and effectively mitigated and directly supporting our ability to address an emerging risk environment in which cyber and physical boundaries are increasingly meaningless.

II. Risk Management

DHS has an all-hazards mission for protecting the homeland. This means that we must plan for and prioritize a range of risks from natural disasters to terrorism to cyber-attacks. Our mission includes recurring, persistent, and relatively well understood hazards such as hurricanes and earthquakes, as well as threats and hazards such as solar storms where we must continue to understand the likelihood and consequences of a possible event. For this reason, DHS approaches threats and hazards based on an all-hazards analysis of risk and due caution in the face of inherent uncertainty. This risk-informed approach guides our planning efforts and the development of new or enhanced capabilities to address emerging hazards and threats.

Risk is comprised of three variables: *threats* that exploit *vulnerabilities* to cause undesirable *consequences*. In other words, risk is a function of threat, vulnerability, and consequence. DHS recognizes that risk cannot be eliminated and therefore must be managed through proven practices including timely information sharing. Risk management practices include risk acceptance as well as risk mitigation. Risk management can also include risk transfer, such as contractual provisions or insurance coverage. But ultimately, risk cannot be eliminated: there will be incidents, so we must also focus on the resiliency of our infrastructure under all conditions.

III. Threat landscape

NPPD is particularly focused on two threats that are particularly salient in the current risk environment: terrorism and cyber-attacks. Terrorist attacks such as those in France in 2015, Belgium in 2016, and the tragic attacks in Istanbul and Orlando just last month highlight the continuing threat. These attacks underscore the persistence of our adversaries and the vulnerability of public gathering sites.

Terrorist tactics and techniques have transitioned from a complicated attacks such as 9/11 to simple acts of violence using readily-available weapons such as a gun, knife, hatchet, or car. The threats we face today are thus more decentralized than a decade ago and reflect, as Secretary Johnson has said, a new phase of global terrorism. We have moved from a world of directed attacks to one of inspired attacks. Inspired attacks are harder for intelligence and law enforcement communities to detect, can occur with little or no notice, and create a more complex homeland security challenge.

The threat landscape in cyberspace is also changing. Threat actors in cyberspace have highly diverse motivations. Some seek to achieve a political or social aim. Others seek financial benefit and are developing new means to monetize cyber intrusions, as exemplified by the recent wave of “ransomware” attacks. Other adversaries attempt to use strong-arm tactics to advance a goal, such as destroying systems and data to convey a political message, or target sensitive government and private sector systems to steal critical information for espionage purposes.

Perhaps most importantly, the past year saw the use of a cyber attack to achieve a significant disruption of civilian critical infrastructure. In December, several Ukrainian power companies experienced a cyberattack that resulted in power outages lasting around 6 hours that impacted over 200,000 customers. The cyber attack was well-planned, well-coordinated, and used destructive malware to delay recovery efforts. This attack should be a warning to our Nation. Our adversaries have the cyber capabilities to harm our national security, economic security, public health, and safety. This threat environment requires DHS to place renewed focus on providing our customers with risk management tools, information, and support to protect against cyber attacks and mitigate the consequences when a compromise occurs.

IV. Critical Infrastructure Security and Resilience

These trends in the threat landscape require NPPD, as directed by the National Infrastructure Protection Plan (NIPP), to approach risk management from both a top down and bottom up perspective. The majority of the nation’s critical infrastructure is owned and operated by the private sector or by State, local, tribal, and territorial (SLTT) governments. As a result, it is important that government and industry work together to mitigate threats, vulnerabilities, and consequences.

We use a top down approach as we work closely with and across critical infrastructure sectors to understand and address sector- and economy-wide risks. We use a bottom up approach to develop a trusted relationship with owners and operators of the nation's critical infrastructure: for example, a single power plant. PSAs and CSAs are the core of our bottom up approach and serve as the focal point of support to individual critical infrastructure owners and operators. As our stakeholders make challenging decisions about how to manage their own risk, field-based PSAs and CSAs provide advice and connect operators to security capabilities offered across the U.S. Government.

Our PSAs and CSAs operate within a statutory, policy, and doctrinal framework of voluntary partnerships. They conduct vulnerability and consequence assessments, provide information on emerging threats and hazards, and offer tools and training to help critical infrastructure owners and operators and SLTT partners understand and address risks. Finally, they provide on-site critical infrastructure subject-matter expertise during special events and incident responses.

The PSAs have been valuable advisors to local law enforcement. During last year's events in Baltimore, the local PSA received a request from Baltimore Gas and Electric (BGE) to facilitate National Guard Troops at their Spring Gardens facility, fearing that the private security at the main gate may not be able to prevent protestors from entering the plant. The Baltimore PSA advised the Baltimore Police Department Incident Commander of the request and subsequently, the Maryland Army National Guard provided troops near the main entrance, and no incidents took place. This direct, community based security support is precisely the public service that PSAs provide, as highlighted by the recent tragic attacks in Orlando, and the still unfolding events in Dallas last week.

V. PSA and CSA Value Proposition

The Department's approach to critical infrastructure security and resilience is predicated on public-private partnerships. Such partnerships depend on the formation of trusted relationships between public and private sector partners. These trusted partnerships are most effectively formed through regular and meaningful interactions among Federal agencies, private sector owners and operators, and SLTT governments. In turn, such interactions are most effectively enabled by regionally-based Federal representatives. The PSAs and CSAs serve as these regional representatives to establish and mature the relationships with critical infrastructure owners and operators and SLTT governments that are foundational to our voluntary approach to risk management.

In existence since 2004, the PSA program is a mature initiative that presently fields 102 regionally-based personnel. The President's FY2017 Budget requests further growth to 119 regionally-based PSAs to meet demand. As field-based representatives, the PSAs work closely with private sector companies and with State Homeland Security Advisers. SLTT stakeholders from every region served by the PSA programs have consistently identified PSAs as a highly

valued source of support for their critical infrastructure protection responsibilities. While PSAs focus principally on physical security, they are beginning to provide customers with targeted information based on the existing NPPD portfolio of cybersecurity services to maximize the breadth of outreach for both cyber and physical risk management activities.

The CSA program is modeled after the PSA program, although it reflects several differences to account for its focus on cybersecurity. More nascent than the PSA program, there are currently five regionally-deployed CSAs. By the end of this fiscal year, we expect to deploy 13 total CSAs in the field. The President's FY2017 Budget requests a total strength of 24 CSAs. CSAs provide NPPD's most effective mechanism to reach small and medium businesses that may lack the resources to participate in other cybersecurity programs, offer cybersecurity risk assessments to our stakeholders, and provide the Department with invaluable insight into national risk trends that are applicable to the development of new capabilities. CSAs' primary points of contact are private sector and SLTT government Chief Information Officers and Chief Information Security Officers.

VI. PSA Program

The PSA program's primary mission is to proactively engage with Federal and SLTT government mission partners and members of the private sector stakeholder community to protect critical infrastructure. The PSAs have five mission areas that directly support the protection of critical infrastructure:

1. Conduct Assessments to Foster Risk Management Best Practices;
2. Threat and Hazard Outreach;
3. Support to National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) Events;
4. Incident Response; and
5. Coordinate and Support Risk Mitigation Training—particularly active shooter and bombing prevention training.

1. Conduct Assessments to Foster Risk Management Best Practices

One of the central ways that PSAs support critical infrastructure owners and operators is by planning, coordinating and conducting voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions, ranging from houses of worship to major league sports stadiums. Our PSAs offer a range of assessment capabilities including Infrastructure Survey Tool (IST) security surveys, Assist Visits, Infrastructure Visualization Platform imagery captures and broader assessments conducted through the Regional Resiliency Assessment Program (RRAP).

The resulting survey information is provided to owners and operators and highlights areas of potential concern, recommendations to mitigate identified vulnerabilities, and options to view the

impact of potential enhancements to protection and resilience measures. Over 85 percent of the assessed facilities indicate that they will use the feedback from the PSA to guide their security or resilience enhancements.

The increasingly tight coupling and interconnection between cyber and physical systems has required PSA's to begin to conducting joint assessments of cyber and physical security. A principal example of such joint assessment was an RRAP conducted on a Data Center Cluster in Ashburn, VA that assessed cyber and physical risks to a key information technology facility. PSAs serve as a conduit for accessing other DHS cybersecurity resources, and are able to connect stakeholders to resources for encouraging cyber hygiene and information assurance practices. When additional or local cyber expertise is needed, PSAs can connect partners to CSAs.

2. Information Sharing

In the past three years, the PSA program has conducted multiple outreach activities focusing on specific communities of interest and sectors such as faith based organizations, shopping malls, energy/electrical sector entities, sports leagues and venues, and K-12 schools. These engagements were intended to provide an overview of evolving threats, such as active shooter awareness, an understanding of available tools and resources, and best practices designed to enhance information sharing, physical security, and resilience. These efforts often led to customers requesting security/vulnerability assessments from the PSAs. PSAs also encourage businesses to "Connect, Plan, Train, and Report." Applying these four steps in advance of an incident or attack can help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities.

As an example, the Metcalf Electrical Substation, in San Jose, California, was subject to a breach by unknown actors in April 2013. The assailants were able to access the substation and caused significant damage to five transformers and fiber optic cables, which in turn affected telecommunications in Santa Clara County. As a result of this incident and others, the Department of Energy and DHS, in coordination with other Federal agencies and regulatory commissions, conducted an outreach program. The outreach was conducted in ten U.S. cities and two Canadian cities and addressed proactive security measures, threat detection and assessment technologies, and the creation of an incident response plan. Following the completion of the Electrical Substation Outreach, PSAs provided briefings for the ten most critical electrical substations and their stakeholders, and conducted IST security surveys. The data from the security surveys was used to analyze common protective and resilience measures, summarized in a report published April 2015.

An additional example followed the mass shooting at the Emanuel AME church in Charleston, SC on June 17, 2015. Our local PSA offered around 20 security briefings and conducted active shooter briefings for companies, schools, and churches. All briefings were well received and

some recipients requested further training. On February 17, the PSA also supported holding a DHS Interfaith Town Hall in Charleston, South Carolina where we brought public and private sector partners together and discussed protective security resources for faith-based and non-profit community stakeholders.

3. Incident Response

In response to natural or man-made incidents, PSAs deploy to State and local Emergency Operations Centers and, when appropriate, Federal Emergency Management Agency (FEMA) Regional Response Coordination Centers. PSAs provide situational awareness and facilitate information sharing to support the response, recovery, and rapid reconstitution efforts of critical infrastructure. During major incidents and when designated by the Assistant Secretary of the Office of Infrastructure Protection, PSAs serve as Infrastructure Liaisons at Joint Field Offices or Unified Coordination Groups.

In 2015 and 2016, the National Preparedness System went through a “refresh” effort to update the National Preparedness Goal, the five mission area Frameworks and the Federal Interagency Operational Plans for Prevention, Protection, Response and Recovery. These foundational documents further define the role of the PSAs in ensuring that the connection between infrastructure stakeholders and partners across the nation are able to support and engage in national preparedness efforts.

4. Special Events

PSAs provide support to officials responsible for planning and leading special events. This includes providing expert knowledge of local critical infrastructure; participating in planning committees and exercises; conducting security surveys and assessments of event venues and supporting infrastructure; and coordinating the development and delivery of geospatial products. Examples of special events supported by the PSAs include:

- Presidential Inauguration, State of the Union, Papal Visit and Republican and Democratic National Conventions;
- Major sporting events such as the Super Bowl (The Houston PSA is the Deputy Federal Coordinator for Super Bowl 51), World Series, Stanley Cup, and Indianapolis 500;
- Annual United Nations General Assembly; and
- New Year’s Celebration at Times Square in New York City.

5. Risk Mitigation Training

To reduce risk to the Nation’s critical infrastructure, NPPD develops and delivers a diverse curriculum of training to build nationwide counter-improvised explosive device (IED) core capabilities and enhance awareness of terrorist threats. Coordinated by PSAs, the courses

educate SLTT participants such as municipal officials and emergency managers, State and local law enforcement and other emergency services, critical infrastructure owners and operators, and security staff on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

Annually, the PSAs provide active shooter briefings to a diverse audience. These briefings provide an overview and characteristics of an active shooter incident, personal response, and “Active Shooter – How to Respond” materials. PSAs also assist with the coordination of comprehensive Active Shooter Workshops that provide training and detailed information to assist facilities in developing emergency action plans to respond to active shooter threats.

VII. CSA Program

NPPD modeled the CSA program after the PSA program, incorporating appropriate customization to focus on cybersecurity issues. CSAs promulgate best practices and conduct vulnerability assessments, connect stakeholders to information sharing resources, serve as a liaison between critical infrastructure owners and operators and the National Cybersecurity and Communications Integration Center (NCCIC) for incident response and support to special events CSAs function as a regionally-deployed source of subject matter expertise and provide expert consultation on cybersecurity best practices to improve our stakeholders’ cybersecurity risk management.

1. Conduct Assessments to Foster Risk Management Best Practices

Each CSA promotes and assists stakeholders in their implementation of the Cybersecurity Framework, which was jointly developed by the Government and private sector. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps critical infrastructure owners and operators manage their cybersecurity risk. CSAs also provide critical infrastructure owners and operators with tools, guidance, and individualized assistance to help entities use the Framework in a manner that supports their specific risk management needs. CSAs ensure that critical infrastructure stakeholders receive alerts, warnings, and bulletins on cybersecurity vulnerabilities, mitigations and best practices through the NCCIC. These alerts, warnings, and bulletins concern risks to general IT systems as well as specialized risks to industrial control systems—the types of systems used to control power plants, manufacturing assembly lines, and other physical devices.

CSAs also help our customers improve their cybersecurity risk management through voluntary vulnerability assessments. CSAs offer two primary types of assessments to supplement an organization’s existing activities. First, the Cyber Resilience Review (CRR) evaluates an organization’s operational resilience and cybersecurity practices across ten domains including risk management, incident management, and continuity. Second, the Cybersecurity Evaluation

Tool (CSET) is a desktop software program that guides asset owners and operators through a step-by-step process to evaluate their industrial control system and information technology network security practices. Both the CRR and the CSET are now mapped to the Cybersecurity Framework and allow organizations to understand their relative maturity across the Framework's functions. CSAs also offer more specialized risk assessments, such as assessments focused on supply chain risk management.

In addition, CSAs also link critical infrastructure owners and operators and technical penetration testing teams based in the NCCIC. For example, CSAs connect critical infrastructure partners with the National Cybersecurity and Assessment and Technical Services, which provides a variety of technical assessments to identify vulnerabilities in an organization's enterprise, including phishing tests, wireless application assessments, and internal penetration testing.

2. Information Sharing

CSAs connect critical infrastructure entities with the NCCIC's information sharing programs. Pursuant to the Cybersecurity Act of 2015 (Pub. L. 114-113, Division N), DHS serves as the U.S. Government's primary portal for automated cyber threat indicator sharing. By participating in the Automated Indicator Sharing initiative, organizations receive machine-readable cyber threat indicators to immediately detect and block cybersecurity threats. CSAs are leveraging the relationships that they and the PSAs have built to encourage companies to sign up for Automated Indicator Sharing. Additionally, CSAs help stakeholders learn about and join the Cyber Information Sharing and Collaboration Program (CISCP), which provides a trusted forum where vetted partners share threat and incident information with the government and other private sector partners. CISCP also permits participating companies gain access to the NCCIC watch floor for operational collaboration.

3. Incident Response

Cybersecurity is about risk management, and no organization can eliminate all risk. Organizations that implement best practices and share information will increase the cost for adversaries and stop many threats. But ultimately, there exists no perfect cyber defense, and persistent adversaries will at times find ways to infiltrate networks in both government and the private sector. When an incident occurs, private sector and SLTT governments may work with CSAs to obtain incident response and coordination resources from the NCCIC as well as any additional information they need to respond effectively. CSAs provide valuable insight to help the NCCIC coordinate responses to incidents and to enhance senior leaders' situational awareness.

4. Special Events

CSAs also provide support to officials responsible for planning and leading special events. This includes participating in planning committees and exercises and conducting security assessments of event venues and supporting infrastructure. Examples of special events supported by the

CSAs include the Republican and Democratic National Conventions and major sporting events such as the Super Bowl and the Major League Baseball All-Star Game, where adversaries could potentially target the industrial control systems that enable the provision of lighting, crowd control, security measures, and other critical functions to the host venues.

VIII. The Way Forward

As with all of NPPD's programs, we are continuously assessing progress and looking for opportunities to enhance our capability to most effectively serve our customers. As a result of such a continuous improvement effort, NPPD is further integrating the PSAs and CSAs. For example, CSAs frequently leverage the PSA program to identify and initiate stakeholder engagement where a PSA has previously partnered. In fiscal year 2015, more than 20 percent of CSA evaluations were initiated as a result of direct referrals from PSAs. CSAs and PSAs also conduct joint physical and cyber assessments of critical infrastructure entities and coordinate analytical resources and assessment methods. PSAs and CSAs often exchange information regarding interaction with shared partners and stakeholder groups.

In recognition of growing opportunities for joint cyber-physical stakeholder engagement, we asked Congress to authorize the establishment of a new operational component within DHS, the Cyber and Infrastructure Protection Agency. We submitted a plan that will better align the PSAs and CSAs and streamline and strengthen existing functions within the Department to ensure we are prepared for the growing cyber threat and the potential for physical consequences as a result of an attack. We urge Congress to take action so that DHS is best positioned to execute this vital mission.

1. Way Forward for the PSA Program

i. Three Year Strategic Plan:

IP is working with the Office of Cyber and Infrastructure Analysis (OCIA) to develop a three-year Strategic Plan for PSA's Assessments, as required by Congress, to determine how we can enhance the value and impact of its assessment portfolio for its stakeholders over the next three years. The strategic plan will:

1. Clarify the strategic intent behind IP's conduct of assessments;
2. Expand the value derived from assessments for IP's primary stakeholders;
3. Articulate how assessments can better leverage, and be better leveraged by, related efforts from partners such as OCIA and FEMA; and
4. Optimize how assessments are prioritized and measured.

Once completed, this project will guide how the PSA assessment portfolio supports stakeholders across the nation, contributes to a national understanding of risk, and supports national

preparedness planning, as well as grants decision making. The CSA program will identify improvements by drawing upon the analysis in this plan and its lessons learned.

ii. Regionalization:

The owners and operators of critical infrastructure in the United States are not exclusively located in the Washington, DC area. In order to rebalance resources and meet our stakeholders where they operate, the PSA Program and other NPPD programs are regionally- and field-based. These regional programs are so integral to successful delivery of products and assessments to owners and operators that NPPD has begun the process of shifting headquarters-based staff into the field. NPPD will be placing additional staff from IP in each region to supplement the current PSAs. PSAs provide direct support of mission benefactors, tailored and adapted to meet regional, state and local needs, and this disciplined shift toward field based and regionalized operations is designed to optimize the way that PSAs support partners across the nation, both providing more locally tailored support, and managing expanding security challenges. The CSAs will operate in a similar manner and will be tied into this regional construct.

2. Way Forward for the CSA Program:

NPPD is expanding the number of CSAs deployed across the Nation. The allocation of CSAs is based on a risk-informed set of criteria, including:

- **Public Sector Partners:** The presence of public sector partners (e.g., SLTT governments) with strong cybersecurity programs that would benefit from a closer relationship with NPPD.
- **Private Sector Partners:** High concentrations of companies in particular critical infrastructure sectors, particularly entities identified under Section 9(a) of Executive Order 13636 as especially critical.
- **PSA Activity:** Regions with existing PSAs that will provide new CSAs with an existing network of critical infrastructure contacts.
- **FEMA Models:** CSA expansion will also be informed by available FEMA models, such as those utilized in the context of the Urban Areas Security Initiative and Threat and Hazard Identification and Risk Assessment.

IX. Closing

Protecting the Nation, its critical infrastructure, and each community is a shared responsibility. PSAs and CSAs provide an essential local point of connection between DHS and our critical infrastructure stakeholders. They are the primary “bottom up” capability to help individual companies better manage their risks, and consequentially they create trust relationships that can inform the development of top-down programs to manage risks across entire sectors. This local point of connection allows the Department to more effectively accomplish its mission and helps our stakeholders manage their all-hazards risk.

Thank you again for the opportunity to appear before you today. We look forward to your questions.

STATEMENT TO COMMITTEE ON HOMELAND SECURITY'S SUBCOMMITTEE ON
CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

"VALUE OF DHS' VULNERABILITY ASSESSMENTS IN PROTECTING
OUR NATION'S CRITICAL INFRASTRUCTURE"

JULY 12, 2016

DIRECTOR MARCUS BROWN'S TESTIMONY



pennsylvania

GOVERNOR'S OFFICE OF
HOMELAND SECURITY

Good morning committee members. I am Marcus Brown, Director of the Pennsylvania Office of Homeland Security. I appreciate the opportunity to be here today and discuss our partnership with the Department of Homeland Security's Office of Infrastructure Protection.

A significant aspect of our mission relates to the prevention and protection of our citizens and our critical infrastructure in the face of terrorist threats. Many of the ways we maximize our efforts with prevention and protection activities is working with our three protective security advisors (PSAs) and their regional director.

In a joint effort with the PSAs we have developed programs that better prepare our citizens by identifying vulnerabilities and improving capabilities that address the threat of terrorism. We follow the National Infrastructure Protection Plan (NIPP) and have developed and implemented a state critical infrastructure protection plan as a component of the overarching Homeland Security program. Together we have been able to establish a list of the most critical infrastructure in Pennsylvania by collecting,

prioritizing and analyzing facilities and assets through meaningful outreach.

Our three PSAs provide immense value in assisting local, state and federal officials and the private sector in protecting Pennsylvania's critical infrastructure. One of the ways PSAs accomplish this is by conducting vulnerability assessments, surveys and active shooter protection walk-throughs of facilities or assets. My staff has accompanied the PSAs many times to facilities when they conducted vulnerability assessments or surveys. From our observations, having the owners and operators of the facilities in a room with law enforcement, emergency medical services and other public safety officials always provided a one of a kind opportunity for everyone involved to identify the complexities of a facility in terms of physical and cyber security.

The main tool the PSAs use for their vulnerability surveys is called the Infrastructure Survey Tool (IST). The IST is used to capture information about a facility in order to identify the areas where that facility is most vulnerable. After that data is collected

and analyzed a report containing a comparative analysis, known as a dashboard, is provided to the owner of the facility in order to assist in reducing risk. While the interactive dashboard shows how weak or strong that facility is compared to like-facilities around the country, the report also zeros in on vulnerabilities specific to that facility and provides "options for consideration," meaning the actions taken by a facility will reduce its vulnerability and therefore reduce its risk against man-made and natural hazards.

Additionally, this information gives our local, state and federal public safety officials a picture of what is most at risk in their area of operations. For example with this information in hand the PSAs can monitor critical infrastructure that may be vulnerable during a special event, such as the Democratic National Convention (DNC). The tool used for this purpose is called the Special Event and Domestic Incident Tracker (SEEDIT) tool. During the upcoming Democratic National Convention in Philadelphia the PSAs will share the information in this tool with my Infrastructure Protection Specialists, who will be sitting in the

state's Emergency Operations Center (EOC). They will provide me with situational awareness reports that I can share with Governor Wolf.

From the perspective of my office and the citizens of Pennsylvania the PSAs and Cyber Security Advisor (CSA) bring their experience and expertise into play to assist in critical infrastructure protection efforts and their value cannot be overstated. The tools that they use to assist the private sector facilities are most beneficial to our office especially during the times when my staff has to report to the state EOC during activation. We value their input and assistance when we host table top exercises or training events. What they offer our office is immeasurable to our mission of protecting the citizens of Pennsylvania.

I have provided an appendix that lists the assessments that have been completed by our PSAs and CSA in advance of the Democratic National Convention.

Once again, I would like to thank the committee for inviting me here to speak on this matter. To the extent there are questions I will be happy to attempt to answer any inquiries.

APPENDIX

- I. In preparation for the Democratic National Convention, the **Infrastructure Survey Tool** has been used on the following facilities in Philadelphia:
 - Wells Fargo Center (Location for the DNC)
 - PA Convention Center
 - National Constitution Center
 - Lincoln Financial Field
 - Citizens Bank Park
 - Hahnemann Hospital
 - Equinix Data Center
 - One Liberty Place high-rise
 - Multiple Exelon/PECO substations

- II. Other facilities that have been assessed in the past and whose data will be used during the Democratic National Convention include:
 - Philadelphia Gas Works
 - Multiple assets of the Philadelphia Water Department
 - Penn Presbyterian Hospital
 - Transportation assets - Southeastern Pennsylvania Transportation Authority
 - Amtrak
 - Delaware River Port Authority (Walt Whitman and Ben Franklin Bridges)
 - Comcast Center
 - Philadelphia Museum of Art
 - PJM Interconnect

- III. Cyber assessments conducted on Pennsylvania facilities that will have a role in supporting the Democratic National Convention
 - PA Convention Center
 - Samuel Baxter Water Treatment Plant (main water treatment plant of the Philadelphia Water Department)
 - Comcast Center
 - Philadelphia Gas Works
 - PJM Interconnect

IV. Requests for cyber assessments currently in the planning process

- Delaware River Port Authority
- One Liberty Place
- Philadelphia Museum of Art
- National Constitution Center

V. Additional training conducted by DHS and Governor's Office of Homeland Security in advance of the Democratic National Convention

- Active Shooter Workshop (Public & Private Sectors)
 - 29 April 2016 (Independence Visitors Center – 41 N. 6th Street, Philadelphia, PA 19106)
- Surveillance Detection Training (Public and Private Sectors):
 - 10-12 May 2016 (National Park Service HQs – 143 S. 3rd Street, Philadelphia, PA 19106)
 - 07-09 June 2016 (National Park Service HQs – 143 S. 3rd Street, Philadelphia, PA 19106)
- Protective Measures Course and Vehicle Borne IED Search Procedures (Public and Private Sectors):
 - 25 and May 2016 respectively (Delaware Valley Intelligence Center, 2800 S. 20th Street, Philadelphia, PA 19145)