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

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 12, 2016

Serial No. 114–81

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE

25–264 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
KATIE RASHID, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable John Ratcliffe, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies:
Oral Statement 1
Prepared Statement 3
The Honorable Cedric L. Richmond, a Representative in Congress From the State of Louisiana, and Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies:
Oral Statement 4
Prepared Statement 5

WITNESSES

Mr. Chris P. Currie, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office:
Oral Statement 6
Prepared Statement 7
Mr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security:
Oral Statement 17
Joint Prepared Statement 19
Ms. Caitlin Durkovich, Assistant Secretary, Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security:
Oral Statement 25
Joint Prepared Statement 19
Mr. Marcus L. Brown, Homeland Security Advisor, Director of the Office of Homeland Security, Commonwealth of Pennsylvania:
Oral Statement 27
Prepared Statement 29

APPENDIX

Questions From Chairman John Ratcliffe for Chris P. Currie 43
Questions From Chairman John Ratcliffe for Andy Ozment 45
Questions From Ranking Member Cedric L. Richmond for Andy Ozment 52
Questions From Chairman John Ratcliffe for Caitlin Durkovich 54
Questions From Chairman John Ratcliffe for Marcus Brown 60

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

Tuesday, July 12, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 311, Cannon House Office Building, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, Perry, Donovan, Richmond, Sanchez, and Langevin.

Also present: Representative Payne.

Mr. RATCLIFFE. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

The subcommittee is meeting 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 and conducting physical and cybersecurity vulnerability assessments. The critical systems that are essential and 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 are interested in learning about the strategy that DHS efforts is being guided by 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 in training.

For 12 years, the primary mission of the Office of Infrastructure Protection's Protective Security Advisor Program has been the protection of our critical infrastructure. Protective Security Advisors, or PSAs, are regionally based in alignment with the 10 FEMA regions. PSAs execute their primary mission through the planning, coordination, and performance of security survey 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 or SEAR level 1 and level 2 events and re-

sponse to incidents. The mission I have just described is enormous. Because it is voluntary in nature, its success really hinges on stakeholder buy-in. Such buy-in requires strategic outreach and real value added for owners and operators of critical infrastructure.

I'm 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 have to 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 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 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's vulnerability assessment programs for critical infrastructure and identified challenges within DHS in 2013, in 2014, and, again, in 2015. These reports included a number of recommendations to increase the use, and to 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 voluntarily participation.

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

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 the lessons learned from the PSA Program are, in fact, 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 you in this critical mission.

[The statement of Mr. Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

The subcommittee meets today to examine how the Department of Homeland Security is fulfilling its important mission of protecting our Nation's critical infrastructure by conducting vulnerability assessments. Everyday terrorists, nation states and criminals are targeting the critical systems that run our everyday lives. I want to thank our panel of experts for joining us today 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 Office of Infrastructure Protection's Protective Security Advisor Program's primary mission has been the protection of critical infrastructure. Protective Security Advisors (PSAs) are regionally based in alignment with the 10 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. I am curious to hear today what strategy is guiding this vitally important program for homeland security and what metrics are being used to measure the value it has brought to the owners and operators of critical infrastructure.

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 raising 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 passed unanimously 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 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 these DHS programs depend on voluntary participation.

Just last week, a review of the DHS's website for critical infrastructure vulnerability assessments found conflicting and outdated programs. While errors like these appear insignificant, it's important to remember that these programs are voluntary in nature, and if DHS cannot clearly and effectively promote and market the value of these programs, private-sector entities are unlikely to participate and seek assistance.

The subcommittee believes that both the CSA and PSA programs can be of great value for the protection of our Nation's critical infrastructure, but it's vital that there be effective management of them.

It is the hope of this subcommittee that this hearing will bring some clarity on how DHS has resolved some of these out-standing 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.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of our subcommittee, the gentleman from Louisiana, Mr. Richmond, for his opening statement.

Mr. RICHMOND. Thank you, Mr. Chairman. Thank you for holding this hearing to examine how the Department conducts vulnerability assessments for our Nation's critical infrastructure.

Whether it's going about our daily lives, running a business, or a local government, we all rely on the security of resiliency of our critical infrastructure. As we have seen after disasters like Katrina, Rita, Sandy, or the recent devastation in West Virginia, the ability to recover quickly is crucial.

In my district, as in many districts across the country, multiple DHS components and a range of other agencies conduct vulnerability assessments—The Coast Guard and the ports in my district, TSA and airports and for pipelines and transportation corridors, and DOE and FERC for electrical grid vulnerabilities. Risk assessment involves integrating threats, vulnerabilities, and consequence information and then deciding which protective measures—measure to take based on an agreed upon risk reduction and recovery strategy.

Within DHS, the National Infrastructure Protection Program, or NIPP, outlines how Government and the privately-owned critical infrastructure community can work together to manage risk and achieve physical and cybersecurity resiliency. It is important to remember that these are voluntary, nonregulatory assessments, and they represent the foundation of the NIPP risk-based programs designed to prevent, deter, and mitigate the risk of a terrorist attack or a natural disaster.

The DHS protective security advisors, or PSAs, and cybersecurity advisors, CSAs, conduct these assessments and focus on coordination, training, and building existing relationships with State, local, Tribal, territorial, and private-sector partners.

This year, President Obama requested additional funds to expand the PSA and CSA Programs in hopes of melding physical security with cybersecurity and in line with the Secretary's DHS Unity of Effort initiative.

The critical infrastructure vulnerability assessments present DHS and the current NPPD directorate with one of their most complex challenges. As GAO has suggested in their testimony, it is not clear that the directorate has had a consistent and systematic approach for identifying Nationally critical assets, assessing the risk they pose, and using that information for cost-effective allocation of resources.

Thank you, Mr. Chairman. I look forward to the testimony and yield back.

[The statement of Mr. Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

JULY 12, 2016

Mr. Chairman, thank you for holding this hearing to examine how the Department conducts vulnerability assessments for our Nation's critical infrastructure.

Whether it's going about our daily lives, running a business, or a local government, we all rely on the security and resiliency of our critical infrastructure. As we have seen after disasters like Katrina, Rita, Sandy, or the recent devastation in West Virginia, the ability to recover quickly is crucial.

In my district, as in many districts across the country, multiple DHS components, and a range of other agencies conduct vulnerability assessments—the Coast Guard in the ports in my district, the TSA in airports and for pipelines and transportation corridors, and DOE and FERC for electric grid vulnerabilities.

Risk assessment involves integrating threats, vulnerabilities, and consequence information, and then deciding which protective measures to take based on an agreed-upon risk reduction and recovery strategy.

Within DHS, the National Infrastructure Protection Plan (or NIPP) outlines how Government and the privately-owned critical infrastructure community can work together to manage risks and achieve physical and cyber security and resiliency.

It is important to remember that these are voluntary, non-regulatory assessments, and they represent the foundation of the NIPP risk-based programs designed to prevent, deter, and mitigate the risk of a terrorist attack, or natural disaster.

The DHS Protective Security Advisors (or PSAs), and Cybersecurity Advisors (or CSAs), conduct these assessments and focus on coordination, training, and building existing relationships with State, local, Tribal, territorial, and private-sector partners.

This year, President Obama requested additional funds to expand the PSA and the CSA programs, in hopes of melding physical security with cybersecurity, and in line with the Secretary's DHS Unity of Effort initiative.

Critical infrastructure vulnerability assessments present DHS and the current NPPD Directorate with one of their most complex challenges and, as GAO has suggested in their testimony, it is not clear that the Directorate has had a consistent and systematic approach for identifying Nationally-critical assets, assessing the risks they pose, and using that information for cost-effective allocation of resources.

Thank you Mr. Chairman, I look forward to the testimony today and yield back.

Mr. RATCLIFFE. I thank the gentleman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have with us today a very distinguished panel of witnesses on this critically important topic.

With us today, Mr. Christopher Currie, is the director for homeland security and justice at the Government Accountability Office. Thanks for being with us.

Dr. Andy Ozment is the assistant secretary for the Office of Cybersecurity and Communications within the National Protection and Programs Directorate at the Department of Homeland Security. Andy, good to have you back with this subcommittee.

Ms. Caitlin Durkovich is the assistant secretary for the Office of Infrastructure Protection within the National Protection and Programs Directorate at the Department of Homeland Security. Ms. Durkovich, again, it's great to have you back in front of this committee as well.

Finally, Mr. Marcus Brown, is the homeland security advisor and director for the Office of Homeland Security at the Commonwealth of Pennsylvania.

Welcome to Washington, DC. Thanks for being here at this committee hearing.

I now would like to ask all the witnesses to stand and raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that the witnesses have answered in the affirmative. You all may be seated. The witnesses' full written statements will appear in the record.

The Chair now recognizes Mr. Currie for 5 minutes for his opening statement.

STATEMENT OF CHRIS P. CURRIE, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CURRIE. Thank you, Chairman Ratcliffe, Ranking Member Richmond, Congressman Donovan. Thank you for having me here today.

Today, I would like to talk about DHS's important but equally difficult mission of assessing vulnerabilities across all 16 critical infrastructure sectors. This is a challenge for many reasons, as you know.

Each sector is very different but many are also interconnected. Also, some sectors are heavily regulated and not—and very accustomed to Federal oversight, others are not. Voluntary collaboration is absolutely critical, as you both mentioned in your opening statements. Most infrastructure is owned and operated by the private sector or State and local governments.

DHS needs to collect information to assess Nation-wide risks. But, they must also earn the trust of these partners by using the information effectively and protecting it, too.

Sharing and trust are also increased when DHS returns the favor and gives information back to owners and operators they can use.

In late 2014, we evaluated 10 different DHS vulnerability assessment tools across all 16 sectors. We found that from 2010 to 2013, DHS was involved in almost 13,000 assessments of different assets or systems. These varied from multi-day onsite assessments of chemical facilities to voluntary on-line surveys used by shopping malls and other commercial facilities. We also found that these assessment tools overlapped across sectors and collected different information and levels of detail.

For example, some of the 10 assessment tools collected information on vulnerabilities to all hazards like earthquakes and hurricanes while others didn't. We also found that asset names and addresses were recorded differently across assessments, and this simple difference made it difficult for DHS officials and us, for that matter, to analyze whether assessments duplicated one another across sectors.

DHS also lacked mechanisms at the time for sharing assessment data across its own components like NPPD, TSA, Coast Guard, as well as with other Federal departments. For example, non-DHS agencies like EPA also provide self-assessments to facilities to assess their risk, like waste water treatment facilities, for example. However, DHS did not have mechanisms in place to better integrate those assessments and avoid potential duplication.

So we made a number of recommendations in that particular report. First was that DHS identified the most important areas and the detail necessary to integrate assessment efforts, first of all.

Second of all, we recommended that DHS consistently collect and maintain assessment data and share it across components and other Federal departments. This could help them better identify duplication or on the other end gaps in the coverage that these assessments do.

DHS agreed with all of our recommendations, and I want to give them credit, because they have taken action to address them. For example, it's established working groups among components and other departments. It's also considering actual guidance within the Department to better coordinate assessment efforts, and begun to inventory what other departments are doing. While this is progress, there's still much more work needed to institutionalize these efforts into DHS policies that components must follow.

Strengthening how DHS manages and coordinates its assessments won't just benefit DHS but also the infrastructure owners and operators that must use these assessments. When surveyed, they told us—and you mentioned this, Mr. Chairman, and DHS officials told us, too—that there is Federal fatigue or weariness in conducting numerous assessments. To this end, we have recommended that DHS could really do more to understand why asset owners and operators decline to participate in voluntary assessments. We also found that DHS should more quickly provide assessment results back to owners and operators, which could encourage trust and participation.

To be clear, DHS has made much progress in this area since our report. For example, they are now using web-based systems to more quickly deliver results and have cut down on these delays.

Last, better coordination among components and agencies and sharing of data, as I discussed before, could also help reduce burden on operators. For example, if a DHS protective security adviser has access to all Federal assessment data on a particular facility, they have a head start in assessing that facility as well as information to build credibility with the owner or the operator.

This concludes my statement. I look forward to the Q&A.

[The prepared statement of Mr. Currie follows:]

PREPARED STATEMENT OF CHRIS P. CURRIE

JULY 12, 2016

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.

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 on-going 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, 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 6 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 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

---

[1] See 42 U.S.C. § 5195c(e).

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

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

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

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

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

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

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

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

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 on-going recommendation follow-up activities.

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

---

[10] GAO, *National Protection and Programs Directorate: Factors to Consider When Reorganizing,* GAO–16–140T (Washington, DC: Oct. 7, 2015); *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach,* GAO–14–464T (Washington, DC: Mar. 26, 2014); *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program,* GAO–13–616 (Washington, DC: 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, DC: Mar. 25, 2013); and *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments,* GAO–12–378 (Washington, DC: May 31, 2012).

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

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.

PROGRESS MADE ADDRESSING BARRIERS TO CONDUCTING VOLUNTARY ASSESSMENTS AND SHARING INFORMATION

DHS 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 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 own-

---

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

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

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

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

[16] GAO–12–378.

ers 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 time frames 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 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 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:

---

[17] GAO–12–378.
[18] GAO–13–616.
[19] A protective security advisor is a DHS field representative. Among other things, they conduct RRAP projects.
[20] GAO–13–296.

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 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 on-line 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.

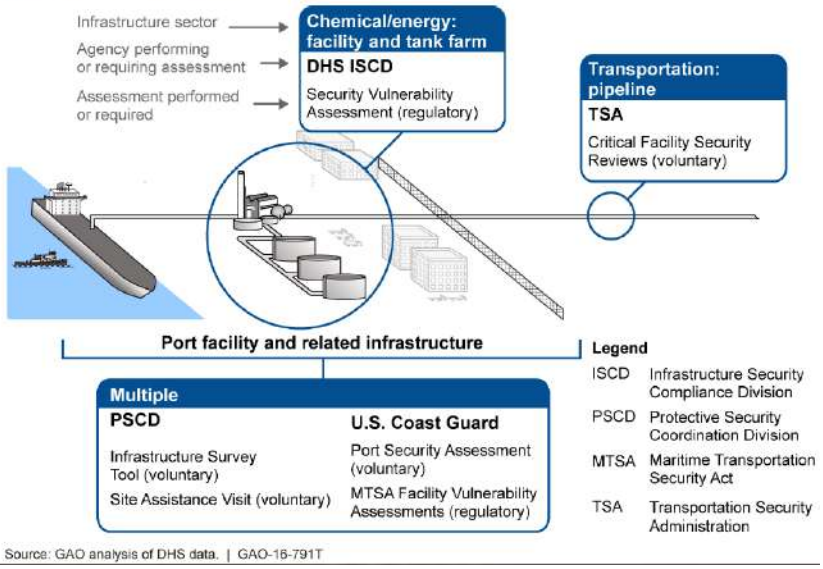
We recommended that DHS review its vulnerability assessments to identify the most important areas to be assessed, and determine the areas and level of detail that are necessary to integrate assessments and enable comparisons, and establish guidance, among other things. DHS agreed with our recommendation, and established a working group in August 2015 to address this recommendation and others we made. As of March 2016 these efforts are on-going 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

[21] GAO–14–507.

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

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 infra-

[22] GAO–14–507.

structure 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 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 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 on-going 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

---

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

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

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.

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).* 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) [1]
Food and agriculture	Department of Agriculture [2] and the Department of Health and Human Services [3]
Defense industrial base [4]	Department of Defense
Energy [5]	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 [6]
Water and wastewater systems [7]	Environmental Protection Agency
Commercial facilities	Department of Homeland Security
Critical manufacturing	Office of Infrastructure Protection [8]
Emergency services	
Nuclear reactors, materials, and waste	
Dams	
Chemical	
Information technology	
Communications	Office of Cyber Security and Communications [9]

Source: Presidential Policy Directive/PPD–21/GAO–16–791T.

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

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

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

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

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

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

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

[7] The water sector includes drinking water.

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

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

Mr. RATCLIFFE. Thank you, Mr. Currie.

The Chair now recognizes Dr. Ozment for 5 minutes for his opening statement.

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

Mr. OZMENT. Thank you.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to appear before you today.

My organization within NPPD has three sets of cybersecurity customers; Federal civilian agencies, private-sector companies, and State, local, Tribal, and territorial governments.

Today, I will focus on the Cybersecurity Advisors Program, or CSA Program. Our CSA's focus is on the latter two customers, private-sector companies and State and local governments. The CSA Program is modeled after the Protective Security Advisor, or PSA Program that you will hear from my colleague, Assistant Secretary Durkovich.

Although the CSA Program does reflect several differences to account for its focus on cybersecurity. Importantly, the CSA Program, as you noted, Chairman, is more nascent than the PSA Program. While there are over 100 PSAs, as of last weekend, there were only 5 regionally-deployed Cybersecurity Advisors. I say last weekend, because yesterday, our sixth CSA started work, a nice milestone for us.

Our customers have demonstrated a significant demand for the resources and support provided by our CSAs. For this reason, we expect to deploy 13 CSAs in the field by the end of this fiscal year. The President's 2017 budget requests a total of 24 field-deployed CSAs. As you know, the vast majority of our Nation's critical infrastructure is owned and operated by the private sector or by State and local governments. To protect that infrastructure, we must help those owners and operators improve their cybersecurity.

Now, people who work in Washington, DC, are sometimes criticized for thinking that only of Washington, DC. Our Nation cannot afford for NPPD to think that way. We must work across the

United States helping private-sector and State and local government customers where they live.

For critical infrastructure owned by small businesses, there's often no other way to reach them. Our Cybersecurity Advisors are thus NPPD's deployed cyber work force who live across the United States helping critical infrastructure where it is located and where the owners and operators live. Our Cybersecurity Advisors have 4 areas in which they support our customers. They help our customers adopt best practices, they share information, respond to incidents, and support special National security and other events. I'll speak to each of those in turn.

First, we help our customers adopt cybersecurity and best practices as exemplified by the NIST cybersecurity framework. We do that by advising them on risk management. One of the more concrete and visible ways we advise on risk management is by performing risk assessments.

We offer a wide range of cyber risk assessments starting at the most strategic level and then going down into more technical areas depending on what a company or other customer needs.

For example, our most strategic cyber risk assessment is a questionnaire that could take a full day, working with many different leaders within an organization to complete to get a full picture of their risk management methodology.

With our current work force, we average about 80 assessments a year. A few months after the assessments, we survey the companies to see, did the company or State and local organization make a major change based on the assessment?

So far, 96 percent of the respondees to our post-assessment survey have made at least one major security improvement as a consequence of our assessment.

CSAs also link critical infrastructure owners and operators to more technical hands-on assessment teams based in the NCCIC. For example, the NCCIC can actually try to break into a company, that is, we can try to hack them. I'll emphasize that we do this only at the invitation of the company.

Second, CSAs connect companies to our information-sharing activities. For example, the Cybersecurity Information Sharing Act of 2015 has passed, and CSAs are helping us to recruit companies to share machine-to-machine data at real time, in our automated indicator sharing program. Let me thank you and the committee, again, for your help in passing that very important legislation.

Third, CSAs can provide support to our customers who experience a cybersecurity incident. When an incident occurs, our customers can work with CSAs to obtain incident response and to coordinate resources and information coming out of the NCCIC.

Finally, CSAs provide support to officials responsible for planning and leading special events, sometimes known as National security events. Examples of special events supported by the CSAs include major sporting events such as the Super Bowl and major league baseball all-star game and upcoming conventions.

These are the 4 major lines of effort by which CSAs support customers—best practices and risk assessments, information sharing, incident response, and special events. But CSAs have an additional role, which is to aid and inform our National efforts. For example,

a local perspective could be critical to identify which infrastructure matters the most. CSAs use their local knowledge to identify the most critical infrastructure in a given region.

Increasingly, they are also asked to bring their expertise into close collaboration as trusted advisers, planners, and emergency management executives who report to the State Homeland Security Advisor. Ultimately, CSAs are also the voice of individual companies in the development of National plans and programs.

CSAs provide a local point of connection to help their customers manage their cyber risk and brings their insight into this National conversation. Although we only have 6 CSAs in the field today, I ask your support in passing the fiscal year President's budget to bring us to a total of 24 CSAs in the field.

Thank you again for the opportunity to appear before you today, and I look forward to your questions.

[The joint prepared statement of Mr. Ozment and Ms. Durkovich follows:]

JOINT PREPARED STATEMENT OF ANDY OZMENT AND CAITLIN DURKOVICH

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 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 cyber space is also changing. Threat actors in cyber space 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 cyber attack 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 fiscal year 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 5 regionally-deployed CSAs. By the end of this fiscal year, we expect to deploy 13 total CSAs in the field. The President's fiscal year 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 3 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 4 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 10 U.S. cities and 2 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 10 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 5 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 Nation-wide 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 10 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 3-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 3 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.

Mr. RATCLIFFE. Thank you, Dr. Ozment.

I now would like to recognize Ms. Durkovich for 5 minutes for her opening statement.

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

Ms. DURKOVICH. Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for the opportunity to appear before you today to discuss the crucial role that Protective Security Advisors and Cybersecurity Advisors, or PSAs and CSAs, respectively, serve in supporting critical infrastructure owners and operators in their efforts to manage an increasingly complex and dynamic risk environment.

NPPD's mission is derived from the recognition that critical infrastructure is essential to the Nation's security, economic prosperity, the resilience of our communities, and our way of life. However, the majority of our Nation's infrastructure is owned and operated by the private sector and by State and localities. As such, the Federal Government shares responsibility in helping them navigate a risk landscape that has become multi-dimensional, covering physical, cyber, and even space-based threats and hazards.

To that end, we appreciate your support for establishing a cyber and infrastructure protection operational component within the Department and for authorizing the PSA and CSA Program.

The Department's approach to critical infrastructure security and resilience is predicated on building trusted, value-added partnerships with owners and operators of critical infrastructure. We build partnerships at the National level with the 16 sectors to identify requirements and gaps, develop tools, build capacity, and promulgate best practices to manage threats and hazards specific to their sectors while recognizing the important dependencies and interdependencies that are created by their interception.

But equally important we build partnerships at the regional, State, and local level beyond the Beltway, where owners and operators are living the daily reality of this dynamic risk environment. The PSAs and CSAs are responsible for developing and sustaining these trusted relationships and bringing resources to bear to help owners and operators put appropriate security and resilience measures in place. And in the event of a bad day, help mitigate the consequences so we can not only limit the loss of life but the economic impact and disruption to our communities.

We fielded the first PSA cohort in 2004 with the goal of putting at least one PSA in every State. Today, it is a mature program with 102 regionally-based personnel, and we've done more than just putting a PSA in every State. Larger States and urban areas are home to several PSAs. In the President's fiscal year 2017 budget request, we have been asked for an additional 17 PSAs.

No week for a PSA is the same. I have had the opportunity to witness first-hand what they accomplish each day in our communities. It ranges from conducting the vulnerability assessments we are here today to discuss, to organizing security campaigns on evolving threats, such as violent extremism or substation attacks. It may include active-shooter training and counterimprovised explosive device workshops or planning for special events such as the upcoming political conventions.

Equally important, as I expect you will hear today from Director Brown, they support State and local critical infrastructure protection activities and provide critical decision support information about disruptions to infrastructure and cascading impacts during an incident.

Recent events demonstrate why critical infrastructure must be secure and able to rapidly recover from all hazards. Terrorist attacks and active-shooter incidents both here and abroad highlight the continuing interest that adversaries have shown in targeting critical infrastructure, the vulnerability of public gathering sites, and they underscore the persistence of those who wish to cause harm, whatever their motive.

In addition, the last several months highlight the convergence of the cyber and physical domains. The disruption to the Ukrainian power grid is the first known example of a remote cyber attack that had physical consequences. We know that nation-States are looking to gain footholds into our infrastructure to use in times of conflict. To meet the threat head-on, CSAs and PSAs have already begun to coordinate their efforts, conducting joint physical and cyber as-

sessments of critical infrastructure and aligning analytical resources and assessment methods.

In fiscal year 2015, more than 20 percent of CSA evaluations were initiated as a result of direct referrals from the PSAs. The Office of Infrastructure Protection is working to develop a 3-year strategic plan for assessments as required by Congress, which we expect to be completed by the second quarter of fiscal year 2017. This plan will enable us to clarify the strategic intent behind IPs conduct of assessments, expand the value derived by our stakeholders, and will further guide how the assessments are prioritized and measured.

In closing, protecting the Nation, our critical infrastructure, our communities, and our way of life is a shared responsibility. PSAs and CSAs provide the local point of connection between DHS programs and our critical infrastructure stakeholders. They are the primary bottom-up capability to help owners and operators better manage their risks and consequently are the basis for the trusted relationships that have resulted in a National critical infrastructure program that is a model around the world.

Thank you, again, for the opportunity to appear before you today. I look forward to your questions and to working with you to ensure NPPD or cyber and infrastructure protection is appropriately organized and positioned to carry out this critical mission.

Mr. RICHMOND. Mr. Chairman, I would ask unanimous consent that Mr. Payne be allowed to participate in today's hearing.

Mr. RATCLIFFE. Without objection.

I would like to welcome the gentleman from New Jersey to our subcommittee today. Glad to have you.

Thank you, Ms. Durkovich. The Chair now recognizes Mr. Brown for 5 minutes for his opening statement.

STATEMENT OF MARCUS L. BROWN, HOMELAND SECURITY ADVISOR, DIRECTOR OF THE OFFICE OF HOMELAND SECURITY, COMMONWEALTH OF PENNSYLVANIA

Mr. BROWN. Good morning, committee Members, Chairman, Ranking Member. I appreciate the opportunity to be here today to discuss our partnership with the Department of Homeland Security's Office of Infrastructure Protection.

A significant aspect of our mission relates to 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 advisers and our 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, and we have developed and implemented a State critical infrastructure 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, 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 the PSAs accomplish this is by conducting vulnerability assessments, surveys, active-shooter protection walkthroughs of facilities and assets. My staff has accompanied the PSAs in many of these facilities when they are conducting vulnerability assessments. From our observations, having the owners and operators of these facilities in a room with law enforcement, with emergency medical services, and with other public safety officials always provided one-of-a-kind opportunities for everyone involved to identify the complexities of a facility in terms of physical and cybersecurity.

The main tools the PSA uses in their vulnerability surveys is called an Infrastructure Survey Tool, or an IST. The IST is used to capture information about a facility in order to identify the areas where the facility is most vulnerable. After that data is collected and analyzed, a report containing a comparative analysis known as the 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 of consideration, meaning that these specific actions taken by a facility will reduce its vulnerability and, therefore, reduce its risk against man-made or natural disasters.

Additionally, this information gives 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 specific event such as the upcoming Democratic National Convention in Pennsylvania. The tool used for this purpose is called the Special Event or Domestic Incident Tracker tool. During the upcoming Democratic National Convention in Philadelphia, the PSAs will share the information in this tool with all of the members of our State Emergency Operation Center. Then the EOC will be able to provide me with situational awareness reports that I can then feed to public safety leadership and the Governor.

From the perspective of my office and the citizens of Pennsylvania, the PSAs and the Cybersecurity Advisors 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 my office, especially during times when my staff has to report to our State EOC during an activation. We value their input and assistance when they are participants with us in our tabletop exercises and training events. What they offer our office is immeasurable to our mission of protecting the citizens of Pennsylvania.

We have provided in an Appendix a list of the assessments, that have been done by our PSAs in advance of the Democratic National Convention. So once again, I would just like to thank the com-

mittee for having me here, and I'm more than willing to answer any questions.

[The prepared statement of Mr. Brown follows:]

PREPARED STATEMENT OF MARCUS L. BROWN

JULY 12, 2016

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 3 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 (SEDIT) 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)

Mr. RATCLIFFE. Thank you, Mr. Brown.

I now recognize myself for 5 minutes for questions.

Dr. Ozment, I want to start with you. We talked about the fact that, as you said, the CSA program that hopefully, you'll be able to leverage and learn from some of the lessons of the PSA's 12-year history.

One of the questions that I have for you is can you advise us on the developmental and training programs for the CSAs to ensure that the field-based personnel out there have a diverse cyber experience that includes computer engineering skills, that includes a well-versed knowledge of cyber incident response and a solid working knowledge of the NCCIC and its capabilities and services?

Mr. OZMENT. Thank you, Chairman. Let me, first, highlight what we are looking for in a Cybersecurity Advisor.

Cybersecurity Advisors are the risk advisors in organizations. So if you look at a typical chief information security officer office, the chief cybersecurity office of a customer, they usually have a CISO, chief information security officer, a policy office, a risk management office, an operations office, and maybe an information-sharing office.

The CSAs bring in that high-level risk management knowledge. So we do not expect them to put hands on a keyboard and be able to do a technical risk assessment. We want them to bring that strategic perspective. Risk management is really the chassis upon which we build cyber programs, and so it's really core.

So right now, let me tell you, in fact, about our 6 CSAs, because I think we have a really impressive group of folks. We have one individual who is a former State CISO. We have a National lab expert on cybersecurity. We have a long-time Navy cyber individual who is also the CISO of a private-sector company. We are about to bring on to Houston in the next month a person who is an executive in an oil and natural gas company to be our Cybersecurity Advisor in Houston. So, and that's just an example of the great talent we've got in this program. So we are bringing in the right people.

To your point, we then have to continue to train them. So one of the things that we do is we actually look to existing training programs such as—well actually, I won't mention certification programs by name, but there are existing private-sector-led certification programs that you use to really ensure that your people have the best risk management knowledge, and so we use those certification programs plus bringing them in back to headquarters to train them on what's available from the headquarters organization and the NCCIC itself.

Mr. RATCLIFFE. Thank you, Dr. Ozment.

Ms. Durkovich, let me turn to you. As I understand, the Protective Security Advisor Program has developed a new public outreach initiative, "Homeland Security Starts With Hometown Security." You and I talked about that. I've got this handout that you gave me. This sounds like a great initiative. My question to you is, have you determined any benchmarks or metrics to determine the success of programs like these or other PSA outreach? Then depending on your answer, Mr. Currie, I would like to have you weigh in on your experience with respect to whether there are any best practices for determining or reporting measurable metrics in areas that are activity-based?

Ms. DURKOVICH. Thank you very much, Chairman, for that question. It is a great question. I want to begin by acknowledging that we are continuing to look at how we enhance and improve our metrics.

As you know, most of what we do within the Office of Infrastructure Protection is voluntary. So owners and operators are not required to participate in our assessments, nor are they required to report back to us what options or considerations they accept. However, we have, over the course of the last several years, begun to do a better job in terms of tracking those options or considerations that are recommended, and we know, for instance, that at least 90

percent of owners and operators at least adopt one of our options for consideration.

We are working to go through the Information Collection Request process, which will allow us to provide surveys and questionnaires, to our owners and operators, to more effectively understand how useful the value that campaigns such as the connect-plan-train-report initiative are bringing.

Once we have that information collection request completed, again, we will be able to actually hand out surveys and get their direct input. We do this right now for the Office of Bombing Protection within IP, and many of the counter-improvised explosive device training courses that we offer, and we know, for example, that our owners and operators rate most of our trainings 4.7 out of 5 stars. So that's an encouraging statistic.

Some of the metrics is anecdotal or qualitative, I should say, and it is based on the participants that come to our workshops. We have recently rolled out an updated version of our active-shooter workshop that is focused on developing an emergency action plan for owners and operators in the event of an active-shooter incident. I will tell you, having participated in one in Philadelphia a month ago, the room is overflowing. I will—again, some of this is just based on the feedback that we get directly whether it is from homeland security advisers, from owners and operators, in terms of the value that we have brought in helping them understand the range of threats and hazards and the measures that are appropriate for their operating environment.

Not every business, shopping mall, movie theater, can put mags in, can do the things that you have here when you enter into this building. So part of what we do is working with them over time to develop that plan and to ensure that the appropriate measures are in place.

But it is an area that we recognize that we have to continue to work on, and it is why we are working diligently to complete the 3-year strategic assessment which will, again, give us a better foundation for the metrics that we collect.

Mr. CURRIE. Yes, sir. So I agree with everything Ms. Durkovich said at the end. I would sort of make two points. No. 1, and, you know, data sharing and data collection is not an exciting topic, but I think that that is the key first step, is that there are so many assessments that have already been done and so many tools out there and so much data that has been collected, first looking across all of this data to see what we first have.

One of the problems we identified when we actually tried to look across all that information was that there may have been similar information collected in different assessments but just asked in a different way. So it wasn't consistently collected, and you could not compare it across sectors, across facilities and all that type of thing. That makes it really, really difficult to identify priorities across the country. But I also want to make the point that—I mean, this is really difficult, you are dealing with 16 individual unique sectors; each sector has to have unique tailored questions to it. But there is a way to collectively do this.

I do want to make the other point, though that, there are certain programs where DHS is a little bit more involved in the actual as-

sessment and follow-up, like the Regional Resiliency Assessment Program, where DHS goes out with local partners and other Federal agencies and assesses regional risk and resiliency. One of our past recommendations is they better follow up on that to see what mitigation actions were taken and how that actually decreased vulnerabilities. So you can quantitatively look at that issue, too.

Mr. RATCLIFFE. Thank you, Mr. Currie and Ms. Durkovich.

My time has expired. The Chair now recognizes my friend from Louisiana, the Ranking Member, Mr. Richmond.

Mr. RICHMOND. Thank you very much.

This is to Director Brown, and it's also a follow-up of some things that you mentioned in your testimony.

In your experience in Pennsylvania, and especially in light of the upcoming Democratic convention, how are critical infrastructure owners and operators taking advantage of the vulnerability assessments performed by PSAs and CSAs, and are they actually adopting the recommended countermeasures and security controls, No. 1?

Then, No. 2, in your opinion, have these assessment programs been noticeably beneficial? If not, what would you suggest improving?

Mr. BROWN. First, I would like to take a step back from the DNC last year. We had the papal visit in Philadelphia, also. Again probably the largest a NSSC event that the country has ever seen. And, again, I sat on the Executive Steering Committee for that, and so, oversaw a great deal of the security planning for the event at all levels—local, State, and Federal. The PSAs played a very important role in what we were doing there. You know, they—and that was in several ways. No. 1, the assessments that they did, they had done a significant number of assessments in the Philadelphia area for that event, leading up to that event, and then again prior to the DNC. Those facilities, when we did table-top exercises, many of those facilities came into a component of the exercise. The fact that we had security assessments done and more importantly, actions taken as a result of those security assessments to make those facilities safer, I think, played a big role in the level of protection everybody expected at those locations and then how we felt about our preparation for the events.

You know, in each one of those events also leading up to them, including the DNC, you know, our PSAs also assisted greatly in training preparation for those events. They had active-shooter training, they had vulnerability facility training, they had IED training, they had surveillance protection training. So it goes beyond just the assessments themselves. When they do the assessments, they see that there are certain vulnerabilities, and then their training comes in behind that to ensure that we're looking at those things and trying to solve some of those problems.

So my thought is that, that they play an important role working with public safety to ensure that the facility and the location and the events that we are putting on, especially in the ones coming up here in Philadelphia for the DNC, I think we are in a much safer position now as a result of their work.

Mr. RICHMOND. Thank you. I would direct this question to the panel, and I think that—I would be interested in the response.

GAO reported that Coast Guard Protective Service Security Advisors and TSA field personnel, have reported observing Federal fatigue or a perceived weariness among critical infrastructure owners and operators that have repeatedly been approached by different Federal agencies and offices. What's being done to address this, both, within the Office of Infrastructure Protection and Cybersecurity and Communications, and externally in regards to other agencies and is it something you all notice and see?

Ms. DURKOVICH. I'm happy to start with that question. Thank you. It is a great one.

I do want to begin by mentioning that we have moved to a single assessment methodology within the Office of Infrastructure Protection, in part because of the work that the GAO has done in identifying some of the challenges behind having multiple assessments.

So over the course of the last several years, we have, again, moved to a single assessment methodology. That assessment methodology is housed in something called the IP Gateway, which really serves as the chassis that underpins our entire suite of assessment tools, our integrated situational awareness, and our integrated planning tools.

The IP Gateway now is used not only by DHS but by many of our Federal partners across the departments and agencies, and equally important, it is used by every State and often in urban areas to conduct these assessments.

But I think that your question raises why our efforts to continue to move toward operationalization, and to enhance our efforts out in the field in the regions is so important.

Part the reason that we have established an IP senior leader in every region is to ensure that we are coordinating, more closely than ever before, with our Federal partners, with our State partners not only in the conduct of assessments to ensure that we are not duplicating efforts, but equally important that we are coordinated in support of special events and incident response.

We have seen the dividends already play out in the regions. I think that we, again, are doing a much better job in limiting duplication.

So as we continue to move in, you know, move to getting additional resources out there, I think that we will continue to see the benefits from this.

Mr. RICHMOND. Anyone else wanted to comment?

Mr. OZMENT. I'll just chime in and highlight that this is one of the strengths of having the PSA Program and the CSA Program closely coupled. The CSAs cybersecurity advisers coordinate with the PSAs, Protective Security Advisors to make sure that their activities are in line, and really look to the PSAs to be the core relationship manager in a given region.

Mr. BROWN. If I could just make one final comment. You know, I think the security assessments that are done play an important role. But when we couple them, our office has—a huge part of what we do is put on table-top exercises. So, when we can couple that assessment with an actual exercise, we all of a sudden now—the facility is now testing what they got in their assessment in an exercise to ensure that the implementation of it, that the surrounding

public safety officials are all on-board with what the assessment is saying and then how best to protect the facility.

So I really think the coordination of both of those things has played an important role in Pennsylvania, especially for some of the large events that we've had.

Mr. RICHMOND. Thank you, Mr. Chairman.

I yield back.

Mr. DONOVAN [presiding]. The gentleman yields back. I don't want you to think that your testimony caused the Chairman to lose his hair, to get a little bit older. He had another commitment, and he's asked me to assume his role.

The Chair is going to recognize other Members of the subcommittee for 5 minutes of questions they may wish to ask the witnesses. In accordance with the committee's rules and practice, I plan to recognize Members would were present at the start of the hearing by seniority on the subcommittee. Those coming in later will be recognized in the order of arrival. We alternate Republican and Democrat. Since I'm the only Republican left, I will ask you questions for 5 minutes.

Mr. Currie, you have testified before this committee before; I thank you for coming again. You had many suggestions during your testimony on how DHS can gain the trust of the private sector, the private owners, and how your suggestions can decrease Federal fatigue that these people are experiencing. Why haven't we done anything about it? You had great suggestions. I thought your testimony was wonderful. Why haven't we done it?

Mr. CURRIE. Well, I think we have done a better job in recent years, no doubt. I think there's two keys to this, and I mean—and the folks talk about it. I mean, one is local relationships. There has to be local relationships in these areas, and that's really important. It's also really difficult to measure how good that is, but it's key.

One of our key points, and, again, not the most exciting topic, but data sharing and data consistency across so many different assessments is critical. If a PSA has reviewed information on assessments that have already been done of a facility, they go in not just informed for their own jobs, but they go in and it lends credibility with the owner and operator.

If there's consistency across questions, especially in the same area, they also don't have to ask the same question a different way that the person may have been asked 3 months ago by the EPA, for example. So I think both things are absolutely critical.

Mr. DONOVAN. Do you think that—you're seeing results, increase, a change? I mean, the program has been going on for 12 years now.

Mr. CURRIE. Sir, to be fair. So we issued our report in 2014, and DHS has done a lot since that time. She mentioned the IP Gateway, which is basically, you know, a web-based tool where people don't have to hand out paper assessments and read them. Everyone can go in and have access to certain information. We think that's good progress. But what we don't know, because our work is a little bit dated is, you know, we surveyed owners and operators at the time. We would have to go back and actually talk to them to get their perspectives, and we haven't done that. So that may be a better question for Mr. Brown.

Mr. DONOVAN. Mr. Brown? It's tough when another witness passes the ball.

Mr. BROWN. You know, I would say one thing about the number of different assessments that are done. You know the agencies that are doing those assessments have very, very high expertise in that certain area, so they are assessing a location or a facility where that type of assessment is probably very important, whether it's the Coast Guard, whether it's environment. You know, they are assessing a certain business or facility where that part is critical.

So, you know, the concern for us always is the last thing we would like to see is a watered-down assessment that sort-of fits everybody. So I think there's sort-of a balance in, you know, what's been reported here compared to exactly what's going to work out in the field.

You know, if it's a maritime facility, we would like to see specialists in the maritime arena be the ones doing the assessment.

So I would caution there should be some balance as we move forward on this to try and make a single assessment that fits everybody or ensuring that we have a comprehensive assessments for each individual sector, because when we have had exercises where multiple assessments have been done, you know, we do get some specific input from each of those assessments that helps us sort of move forward in the security plan.

Mr. CURRIE. Sir, I would absolutely agree with that, too. Then we're not suggesting that there be one single assessment to apply to all 16 different sectors. I think—you know, I absolutely agree. I think what we noticed in our work is that there was a lot of information collected across a lot of different assessments and sectors that was the same, but different. It was collected differently. It could have been used differently if it was collected consistently and analyzed across sectors.

Of course, there has to be subject-matter expertise. That's why the Coast Guard, for example, does port security inspections instead of NPPD, for example.

Mr. DONOVAN. Just for all of you, is this well-spent money?

I know, Ms. Durkovich, you said that it's a voluntary program, people have to, because their private sector, have to volunteer to participate. We're spending a lot of taxpayer dollars on this. Do you feel, each of you, that this is a worthwhile effort, and we're achieving the goal that we set out to achieve when the program began?

Ms. DURKOVICH. Thank you, sir, and I'm happy to start with that question. My answer is unequivocally, yes. As I alluded to in my opening remarks, we are living in a very dynamic and complex risk environment. At the end of the day, our reliance on critical infrastructure is really what, you know, drives our way of life and helping owners, and operators navigate this environment and manage the risk is really the essence behind our program.

So our ability to do these assessments, to share information with them, to make recommendations on how they can improve their security. The reality is you cannot operate in this day and age without having some sort of security plan and some plan for how you are going to bounce back in the event of an incident.

So that is the value that we bring to them, a no-cost assessment that helps them understand where they compare to others in their

sector or subsector, and the return on investment that they will get if they make certain enhancements in security and resilience. So I will tell you, absolutely, it is taxpayer money well spent. We have saved lives. We have limited disruptions to critical infrastructure.

I do want to just speak briefly to the different types of assessments. We have this, you know, this reality in the Office of Infrastructure Protection where we actually have the authority to regulate high-risk chemical facilities. There are about 3,400 facilities that we have deemed high-risk because of quantities, threshold quantities, that they have of chemicals of interest. So we have a special program and chemical security inspectors who are responsible for helping that facility develop a Sites Security Plan and ensure that those chemicals are well-protected.

Our chemical inspectors work closely with our PSAs to ensure that we're not duplicating efforts. Then in addition to a CSI showing up on-site that you don't have a PSA then knocking on the door and saying, hey, do you want an assessment?

We have learned, though—and this is where the work we are doing in the field, to better serve their activity is so important—that even though you may be a high-risk chemical facility, you still have the need for some of our other voluntary services, whether it be active-shooter training, many of, again, the kind of voluntary, the voluntary programs that we do participating in exercises at the State and local level, ensuring that we are accounting for you in NSSCs and the such.

So I think that the earlier comments about the need for specialized assessments is true as well. Thank you.

Mr. DONOVAN. Thank you very much. My time has expired.

The Chair now recognizes the gentlewoman from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman. Thank you, all, for the incredible difficulty of the work that you do.

I believe that both Mr. Langevin and I have been working on this both from the Armed Services Committee and from the Homeland Security Committee. He has ranked for a while with respect to cybersecurity on the Armed Services, and I ranked earlier on that, and of course, we have been very involved here on this issue on homeland.

It's at times just overwhelming, as you know, trying to figure out how we safeguard what we need to safeguard. So I have only one question. Because we have really, and I believed in this, sort-of kept a hands-off method in ensuring with our third parties, those who own our very critical infrastructure, and 90 percent of which really sits in these third parties' hands, we've really attempted to stay short of regulations and playing on red tape and in an effort to keep costs down so that they might be able to better use those funds, that they would otherwise spend to enhance the security of these structures.

We have had both small businesses who have been—who are contractors to some of these larger infrastructure pieces very engaged. We've had, of course, many larger companies engaged. But we've also had a set that have declined to even tell us what they are doing or what they might have, asked us to come in and take a look from an expert standpoint and maybe help them.

What can we do to engage those who are still outside of what we are doing? That would be my only question.

Mr. OZMENT. Thank you, Representative Sanchez.

I think that's really a fundamental question for us all, and I really appreciate your putting your finger on it. The key question here is in a world where we work voluntarily with companies, how do we get them to engage?

I'll tell you, on the cyber side, and I think the same is true on the all-hazards side, having a local regionally-deployed presence is critical, because ultimately, companies work—or small and medium businesses, or State and local governments, they work with the Federal Government when they have a trust in the Federal Government. We build that trust through having people who are living where they live, working where they work, and really providing value to them, making it real that the Federal Government has services to improve your company's security, your local government security. We do have those services.

So having these cybersecurity advisers on the cyber side living and working with our customers has been incredibly important. As you know, I mentioned earlier right now we only have 6, and we are really looking for the Congress' support to increase the number of field-deployed cybersecurity advisers in the 2017 budget.

Ms. DURKOVICH. I would agree with my colleague, but I would like to add one thing, and I think it is an important component of the assessments that we do. But when we work with owners and operators to evaluate their security posture, one of our claims is you are kind-of only secure—you are only as resilient as your weakest link. We encourage them to look across their entire supply chain, to have conversations with their suppliers, to recognize where their key dependencies are, whether it is power, whether it is water, whether it is communications, and to, at a minimum, have conversations with those key dependencies, with those key third-party providers about what their security plans are.

But, equally important, and I think we are seeing this more in the cyber realm than we are in the physical realm, but is ensuring that as you develop relationships and contracts, with those third-party providers, with those in your supply chain, that you are making security, that you are making resilient a key part of that agreement between your organizations, that in some ways, we are pushing the need for security into that supply chain.

Mr. OZMENT. Congresswoman, I apologize. Can I add one additional point? My apologies.

I think one other key aspect of this is actually the legislative protections that you, the Congress, has given us for protecting the information our customers share with us.

I'd highlight two in particular—protected critical infrastructure information, which means that when a company shares vulnerabilities or their risk profile with us, statutorily we protect that information. We cannot give it to a regulator. It cannot be accessed through a Freedom of Information Act or other State Sunshine Act Laws and it cannot be disclosed in civil litigation. That protection is critical. We treat information we receive under that protection extraordinarily carefully.

Then obviously the Cybersecurity Information Sharing Act of 2015 also gave us additional statutory protections for cybersecurity indicator information and those protects are also extremely important.

Mr. BROWN. If I could just weigh in, you know, from the field what we found out is that the more of assessments and the training is done, the more you have other facilities wanting the training. So when you have several hospitals in a city or a locale that have done the assessment, the next thing you realize is you start getting calls from the third hospital saying, hey, I understand these assessments were done, we would like that to have happen.

Now the same thing is happening with the minor league baseball stadiums in the State of Pennsylvania. You know we've done the Philly stadium now, several of their minor league stadiums are asking for an assessment done, followed by a table-top exercise. It is sort of a snowballing effect. The more we are doing these types of things, I think the more the industry is asking for them.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. DONOVAN. The Chair now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chair. Also I thank the Ranking Member for allowing me to sit in today on a very important topic. In my work as Ranking Member on my subcommittee, that deals with resilience and communications, this is something that I've been very interested in and have advocated the administration on. In 2013 the National Infrastructure Protection Plan focuses not only on the security of the Nation's critical infrastructure, but also its resilience, which is something that I've dealt with a great deal.

What training and technical assistance is DHS providing through the PSA and CSA programs to increase resiliency of our critical infrastructure?

Ms. DURKOVICH. I am happy to start with that question, Congressman Payne, and thank you very much. Over the course of the evolution, of our program, we have moved from a security focus to a security and resilience focus because of our recognition of the importance to work with owners and operators, to be able to return to normal operations in the event of an incident.

Resiliency has become a very key part of the vulnerability assessments that we do. Of the 1,400 questions that are part of the infrastructure survey tool, that Director Brown alluded to, a number of them cover resilience-related measures.

Again, that ranges everything from do you have a business continuity plan in place? Do you have route diversity when it comes to your communications? Do you understand who is providing your electricity, your water in the event of a power outage? Do you have a generator? Do you have enough fuel to fuel that generator for at least 72 hours, if not longer?

So again, those types of questions are considered in the IST and we give an owner and operator the ability to see where they stand from a resiliency index compared to others. If for example they didn't have a business continuity plan but they developed one, how that score would improve.

Equally important, a cornerstone of the office of infrastructure protection has become our regional resilience assessment program.

This is where we look at a key industry, a key critical infrastructure asset. In New Jersey, for example, one of our first regional resilience assessment programs projects was focused on exit 14 and the concentration of petrochemical plants, that you find at that exit, and their dependency on water, on electricity, on communications, the importance of the port in the area. We both evaluated what were the threats and hazards that could disrupt or cause some sort of incident at that port.

But equally important, how do we work very closely, not only with the owners and operators, but the State and the local authorities to improve the resilience of all of those underlying systems and assets? It is a Regional Resilience Assessment Program that continues to see value. It has been the basis for a number of different exercises. The State of New Jersey actually created an app based on that RRAP, it is the foundation.

Recently we looked at a category 1 hurricane coming up the southern tip of New Jersey and really the relationships that exist in that region were because of this RRAP that we did in 2009. So resiliency has become a key piece of what we do in the Office of Infrastructure Protection.

Mr. PAYNE. Good old exit 14. I live 4 minutes from there. You know that area has been called the 2 most dangerous miles in the country based on the airport and the seaport, the chemical and the infrastructure, so these issues are very important to me.

How has DHS incorporated the concept of resilience into their vulnerability assessments?

Ms. DURKOVICH. Again, it is both through some of the questions that I alluded to, but looking at really at an organization's, or an industry's, or a particular region's, kind of operational capability, and what is a minimal time of disruption that that particular organization, that particular community can sustain? That's really kind-of what drives our concept of resiliency.

Mr. PAYNE. Thank you.

Mr. OZMENT. I would just note, sir, that our cybersecurity most strategic risk assessments are in fact resiliency assessments.

Mr. PAYNE. OK. Thank you. I appreciate your indulgence and yield back the balance of my time.

Mr. DONOVAN. The gentleman yields back.

I would just like to recognize that I live 10 minutes from that exit, so keep up the good work.

The Chair now recognizes Mr. Langevin from Rhode Island.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank the Chair and the Ranking Member for holding this hearing. I want to thank our witnesses for your testimony here today, and the work you're doing to protect the country.

For Secretary Ozment and Durkovich—so I appreciate the desire to incorporate cybersecurity in your risk assessments, particularly as more and more systems are connected to the internet.

So as a Member of the Armed Services Committee I recognize that today's conflict and really all future ones for that matter are going to contain some type of a cyber component to it going forward. It seems prudent to extend that mindset to critical infrastructure.

So with that in mind, Secretary Ozment and Secretary Durkovich, can you talk about the training required for PSAs to provide these assessments, while Chairman Ratcliffe asked about CSA training, it seems that since they are outnumbered by 20 to 1, at the moment, I imagine PSAs are required to do the baseline assessments and basically it would seem that much of the expertise is different from the physical security that traditionally has been at the domain of PSAs?

Ms. DURKOVICH. Thank you very much for that question. As you alluded to, we see the Protective Security Advisors as force multipliers in this effort to secure critical infrastructure from cyber threats. As I alluded to in my opening statement, over 20 percent of the referrals to the CSAs actually come from the Protective Security Advisors, this is because we have these long-standing relationships that we have developed with owners and operators. In addition to being worried about natural hazards and terrorist threats, they are also dealing with, again, the range of cyber actors.

So at a minimum what our PSAs do is connect them with the other NPPD, cybersecurity security expertise, that may be the NCCIC, that may by the Cybersecurity Advisors, but we also are bringing tools and capabilities. We have a number self assessments that are available to owners and operators on the cyber side of the House and, as well, can articulate kind of that basic cyber hygiene.

So, to ensure that our PSAs at least know enough to be dangerous on the cyber front. This is something that in my role I've had do as well. Right, it is hard for me to go out and talk about this dynamic risk environment and not include cyber in that conversation.

Mr. LANGEVIN. So I just want to ask to clarify, so are they just doing referrals to CSA, or to other entities, or do they actually have training in that area on the site?

Ms. DURKOVICH. So they are largely doing referrals. They do do kind-of general awareness about the threat. They can talk about kind-of basic cyber hygiene, the importance of multifactor authentication of segmenting systems. But, to answer your question, we have sent all of them down to Hoover and the Secret Service cybersecurity campus there to get a basic level of training. There are some Protected Security Advisors who have spent time at Idaho National Labs, with our industrial control system team, getting kind-of a higher level of training. We have only a few, but this is while Andy works to build up his work force, that are actually certified to conduct our cyber infrastructure survey tools. So it's a mix of——

Mr. LANGEVIN. So where do you see the work force going on the CSA side? Because it seems to be that you'd almost want the two to be co-assessing or collocating in conducting these assessments.

Mr. OZMENT. Sir, I think of this as a sort-of three-tiered system. We have the PSAs who can do—advertise our cyber programs, connect people with our other cyber resources and do basic—for example, as part of their basic infrastructure survey tool they do have strategic cyber questions there. They can give high-level advice on cyber hygiene.

When we have a problem that demands more cyber knowledge than that, and a lot of our customers are demanding more cyber

knowledge than that, we go to the CSAs, and the CSAs provide—are cybersecurity specialists but they are not hands-on technical operators, they are cybersecurity executives, if you will.

So then at the next and final tier when a customer needs more technical specialized assistance we draw then upon our different technical groups within the NCCIC, whether it be the industrial control systems team, or an instant response team, or a hacking team if you will.

So we start with that broad base of PSAs who, as you note, there are far more of them and they have these relationships. When we are in a region the CSA and the PSA have to be very tightly coupled and they are very tightly coupled so that the CSA can draw upon that PSA's knowledge and relationships.

Mr. LANGEVIN. So where do we see the CSA work force going? Is that—are you working to increase that, so you have more of balance with the PSAs?

Mr. OZMENT. Yes, sir. We do very much need that CSA work force. The demand is just huge. So we will absolutely increase it. I don't know that we'll reach as large as PSA work force. I think some of that is we have to see how the demand evolves, but we are very much asking for an increase to 24 CSAs in the field in the fiscal year 2017 budget.

Mr. LANGEVIN. Thank you. I hope we are going to concentrate on that more.

Thank you, Mr. Chairman I yield back.

Mr. DONOVAN. The gentleman yields back. I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the committee may have some additional questions for the witnesses. I would ask that you respond to those in writing.

Pursuant to committee rule 7(e) the hearing record will be held open for 10 days. Without objection the subcommittee now stands adjourned.

[Whereupon, at 11:17 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR CHRIS P. CURRIE

Question 1. Given the focus of some DHS assessments on threats to specific regions, are there any U.S. cities or sectors that are examples of best practices in collaborating with and among DHS offices and components and other Federal partners in participating in assessments and taking actions to address vulnerabilities identified?

Answer. DHS has taken steps in response to a past GAO recommendation that will help officials identify U.S. cities or sectors that have demonstrated best practices in collaborating with and among DHS offices and components and other Federal partners. Specifically, DHS uses follow-up surveys at facilities that have undergone vulnerability assessments and security surveys, including those that participate in Regional Resiliency Assessment Program (RRAP) projects, and has initiated a broader data-gathering effort with its RRAP critical infrastructure stakeholders to explore changes in diverse topics such as partnering and State actions based on RRAP participation in response to a recommendation we made to DHS in 2013.[1] In August 2015, the Office of Infrastructure Protection (IP) provided documentation to address this recommendation, including screen shots of an IP-developed SharePoint capability for tracking RRAP findings. This Tracker Tool contains questions about the status of RRAP principle findings, any action taken by RRAP participants, whether the action was taken due to the RRAP, and identification of the point of contact who can confirm this linkage. The data fields in the Tracker Tool will allow IP to identify the RRAPs and associated regions that were successful at bringing about resiliency improvements and the types of improvements that are more common across RRAPs.

Question 2a. According to the GAO testimony, DHS established a policy in October 2014 to conduct quarterly reviews of programs related to critical infrastructure to better understand the barriers critical infrastructure owners and operators face in improving the security of their assets. What trends has DHS identified in declinations using its tracking system since October 2013?

Has DHS identified barriers that critical infrastructure owners and operators face in making improvements?

Question 2b. If so, what are those barriers?

Answer. According to DHS's 2013 National Infrastructure Protection Plan, our Nation's well-being relies upon secure and resilient critical infrastructure. To achieve this, the National Plan calls for critical infrastructure partners to collectively identify priorities, measure progress, and adapt based on feedback and the changing environment, among other things. Therefore, it is imperative that DHS conduct regular reviews of its programs. In 2012, we reported that DHS could be missing an opportunity to measure performance associated with planned and in-process enhancements, and could better understand why certain improvements to securing critical infrastructure were, or were not made, following assessments.[2] We reported that this information could help DHS to better understand what barriers owners and operators face in making improvements to the security of their assets. DHS began tracking additional information in response to our recommendations. Table 1 provides a snapshot of common reasons why facilities refused or were not selected to participate in an assessment from October 2013 through September 2014—the last date for which DHS provided GAO data on this issue—which could

---

[1] GAO, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program,* GAO–13–616 (Washington, DC: July 30, 2013).

[2] GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments,* GAO–12–378 (Washington, DC: May 31, 2012).

prevent owners and operators of critical infrastructure from identifying and making needed improvements.

TABLE 1.—COMMON REASONS WHY FACILITIES REFUSED OR WERE NOT SELECTED TO PARTICIPATE IN A DEPARTMENT OF HOMELAND SECURITY VOLUNTARY ASSESSMENT FROM OCTOBER 2013 THROUGH SEPTEMBER 2014

	Facility Count
Stakeholder believes the threat risk is low	20
Facility is confident in its security posture	43
Facility point of contact requires coordination with corporate office	172
Defense Industrial Base site—no data collection allowed	47
Regulated facility—no data collection allowed	18
Nuclear site—no data collection allowed	5
Facility does not want to share its information with the Government	34
Facility lacks a budget for implementing potential recommended security improvements	24
Facility point of contact lacks time to commit to an assessment	29
Facility not selected by Protective Security Advisor (PSA) for assessment due to resource constraints	577
Facility not selected by PSA for assessment due to regional priorities	94
PSA performed a security assessment at the facility recently	188
Facility received a different vulnerability assessment recently	55
Facility not interested in assessment at this time but would consider future assessment	349
Other	249

Source: DHS data.

Table 2 provides a snapshot of additional information DHS gathered from participants in its voluntary vulnerability surveys from October 2013 through September 2014, the last date for which we received an update from DHS.

TABLE 2.—DEPARTMENT OF HOMELAND SECURITY VOLUNTARY ASSESSMENT FOLLOW-UP SURVEY RESPONSES, OCTOBER 2013 THROUGH SEPTEMBER 2014 NUMBER OF FACILITIES

Number of Facilities	Information Provided Through The Assessment Was Beneficial To My Organization	My Organization Is Likely To Integrate The Information Provided By The Assessment Into Its Future Security Or Resilience Enhancements
Strongly Disagree	54	38
Disagree	5	5
Neither Agree or Disagree	22	37
Agree	287	399
Strongly Agree	473	357
Not Applicable	11	16

Source: DHS data.

In addition, 851 facility owners and operators responded to the question (checking all applicable responses), What are your organization's primary challenges with respect to implementing security or resilience enhancements?:

- Lack of budget (651 responses)
- Lack of project management resources (181 responses)
- Differing strategic priorities (239 responses)
- Plans to move or significantly change the facility (23 responses)
- Local ordinances (28 responses)
- Other (90 responses).

According to a 2014 IP quarterly performance review document we reviewed, IP has plans that could address some of these barriers, including plans to update IP's web architecture to capture, report, and prioritize the technical assistance, training, and education needs of IP and its partners within the critical infrastructure community by the end of fiscal year 2020.

Question 3a. One of the recommendations from your agency's work in 2014 and 2015 stressed the need for DHS to develop an approach to ensure that vulnerability data gathered on critical infrastructure is consistently collected and maintained across DHS to identify gaps and prevent duplication of efforts.

Do you have any recommendations on how to best standardize this data?

Question 3b. Are there any "best-in-class" examples that can be leveraged to accelerate the achievement of the recommendation?

Answer. According to the National Infrastructure Protection Plan managing risk, among other things, entails efficient information exchange through defined data standards and requirements, including an information-sharing environment that has common data requirements and information flow and exchange across entities. However, we reported that the lack of consistent, standardized data on the names and addresses of assets already assessed by DHS's offices and components inhibited the Department's ability to identify whether a given asset had been previously assessed by one office or component. Without consistent, standardized data, DHS was not positioned to readily identify potential duplication or overlap among assessments already conducted. Within DHS, the Office of Infrastructure Protection (IP) has begun, in response to GAO recommendations, some notable efforts to address data quality. These efforts include, among other things, a two-phased automated quality assurance process that confirms that certain data elements have appropriate data, to include but not limited to: Ensuring phone numbers are 10 digits, geocoordinates and zip codes correlate to the associated county and State, and the assignment of unique identifiers. Accurately capturing this basic information in a standardized manner is an important first step in addressing gaps and to prevent duplication of effort. In addition, IP officials told us the office is planning pilot projects with a limited number of Sector-Specific Agencies to identify critical infrastructure data elements that each agency may have a need for, after which appropriate policies for sharing those data elements can be established. With regard to "best-in-class" examples that could be leveraged, in a January 2016 report,[3] we reported on leading practices for well-constructed data definitions derived from standards developed by the International Organization for Standardization (ISO).[4] While not "best-in-class", these practices would be helpful for DHS to review in its efforts to identify "best-in-class" examples it could leverage as it standardizes its data.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR ANDY OZMENT

Question 1. Given the focus of some DHS assessments on threats to specific regions, are there any U.S. cities or sectors that are examples of best practices in collaborating with and among DHS offices and components and other Federal partners in participating in assessments and taking actions to address vulnerabilities identified?

Answer. There are many examples of best practices in collaboration at all levels. A few illustrative examples include the State of New Jersey, Salt Lake City, and the Energy Sector.

State Partnerships—New Jersey.—The State of New Jersey's Office of Homeland Security and Preparedness (OHSP) has been a strong partner on a variety of infrastructure assessment activities. In 2009, the State participated in one of the first Regional Resiliency Assessment Program (RRAP) projects. The 2009 RRAP examined vulnerabilities and dependencies of a cluster of critical lifeline infrastructure located near Exit 14 of the New Jersey Turnpike in Newark. As part of the project, the State was provided with detailed modeling of interconnected water systems in northern New Jersey. Using the water model, New Jersey took steps to develop combined analytical products for the electrical and water systems to look at regional

---

[3] GAO, *DATA Act: Data Standards Established, but More Complete and Timely Guidance Is Needed to Ensure Effective Implementation,* GAO–16–261 (Washington, DC: Jan. 29, 2016).

[4] The ISO is an independent, nongovernmental membership organization and the world's largest developer of voluntary international standards. It has published more than 20,500 international standards covering a wide range of industries including technology, agriculture, and health care. For access to the ISO leading practices for the formulation of data definitions, published July 15, 2004, see: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c035346_ISO_IEC_11179-4_2004(E).zip.*

interdependencies between electricity and water, thereby strengthening the resilience of the Energy and Water Sectors. It also utilized the model to support information-sharing and exercise activities with the Water Sector. New Jersey is currently increasing security systems at two major water treatment plants. As a direct result of the RRAP project, the North District Water Supply Commission initiated a project to improve the resilience of the northern New Jersey water system infrastructure.

Within this RRAP, DHS conducted its first 7 Cyber Resilience Reviews (CRR) ever, focusing on critical information technology services that underpinned these lifeline-sector partner's operations. The results of these cyber evaluations provided cybersecurity-focused options for improvement to each participating organization.

Since 2009, the State has requested 3 additional RRAP projects. The first, in 2014, focused on complex infrastructure supporting the production and transportation of petroleum fuel. The findings were used to drive the New Jersey 2015 Hurricane Season Rehearsal Tabletop Exercise. Using the RRAP-provided information as its basis, the exercise explored improvements for information sharing between the State and the energy sector. In addition, the project delivered to the State and the Federal Emergency Management Agency's (FEMA) Region II office extensive geographic information system (GIS) products depicting petroleum and related infrastructure. The results support emergency response and recovery operations and planning.

The second additional RRAP project, in 2015, is a collaborative effort with State partners from Delaware and Pennsylvania, and is focused on the resilience of ports along the Delaware River, specifically landside terminal operations and inter-modal distribution networks for these ports and marine terminals. The Resiliency Assessment report for the Delaware River project is with stakeholders for review at this time. Preliminary findings were presented to stakeholders in May 2016.

The final additional RRAP project, started in 2016, is focused on the 6 largest wastewater treatment plants, the disruption of which could have cascading impacts across the State and into New York and Pennsylvania. With each of the RRAP projects, the State will receive Resilience Enhancement Options—actions they can take to improve resilience.

Following the RRAP-related cyber evaluations in 2009, DHS began a continuing set of collaborative engagements with the State Chief Information Security Officer (CISO) and the State's infrastructure planners and preparedness coordinators. In 2011 and 2012, DHS provided a review of the State-wide strategic cybersecurity plan. DHS began participating in public-private partnership meetings and provided advice to the State on cybersecurity. The State requested information on DHS's Cyber Security Advisor (CSA) program. By 2014, the State hired its first State-employed CSA.

City Partnerships—Salt Lake City, Utah.—Salt Lake City, Utah, is another consistently strong and active partner. The city received two RRAP projects in 2013 and 2015. The 2013 RRAP project analyzed the Salt Lake City area's health systems' critical infrastructure dependencies and interdependencies, specifically how they would be impacted by a major earthquake. The findings were used to inform emergency response plans, and prompted more detailed analysis of the region's health system dependencies. The 2015 project will provide Salt Lake City with an improved understanding of the various interconnected water and wastewater systems, and identify critical nodes and vulnerabilities.

Sector Partnerships—Energy Sector.—DHS conducts regular engagements with all Sector-Specific Agencies (SSAs) which provide an opportunity to discuss on-going efforts and share best practices. Many of the findings resulting from the different types of assessments are incorporated as part of best practices and reference resources that are disseminated though multiple outreach mechanisms. The RRAP in particular, given its collaborative approach to assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure, lends itself to capitalizing on sector partnerships. The RRAP team participates in SSA coordination calls to inform them of upcoming projects, and includes the SSAs in its annual RRAP kickoff where they have the opportunity to provide input. SSAs are relied upon by the RRAP team to provide insight into the operations and vulnerabilities of infrastructure, as well as to connect the RRAP project teams to relevant private industry and Government contacts who can assist in the assessment and analysis.

The Department of Energy (DOE) has been a close partner, providing insights into the industry, key contacts, and access to useful DOE resources. DOE and the Transportation Security Administration were both involved in the 2012 regional pipelines RRAP project. The Department of the Interior has been supporting the ongoing 2016 Gulf of Mexico project with oil production information and GIS data.

Through these RRAP projects, DHS is helping the Oil and Natural Gas (ONG) sector better understand operational dependencies and to improve coordination with Government emergency management officials. Federal, State, and local emergency management officials play an important role in responding to incidents affecting the ONG sector.

An additional example can be found in the joint DHS and DOE study on the impacts of electromagnetic pulse (EMP) and Geomagnetic Disturbance Events (GMD) on the electric grid. This study will analyze the hazard environments, impacts, and consequences of different sources of EMP and GMD. Events of concern and potential means of mitigation will be better understood.

Federal Partnerships—Cybersecurity.—The role of cyber emergency preparedness, threat and asset response, risk management and best practice promotion, and information sharing in supporting resilient infrastructure operations cannot be understated. Cyber Security Advisors (CSAs) began working with the Coast Guard through participation in Area Maritime Security Committees (AMSC) starting in 2010, acting in many situations as an architect for AMSC cyber working groups and subcommittees. In 2011, DHS assisted the Coast Guard's Pittsburgh Marine Safety Unit, via its AMSC. The CSA on the AMSC cyber subcommittee helped to draft a 2-year strategic charter, laying out objectives for private-sector partners to develop and test cyber incident notifications, response coordination, and lesson-learned collections. Since 2011, CSAs have worked with nearly 12 AMSCs.

NPPD has helped to amplify the cyber emergency coordination efforts of the Federal Emergency Management Agency (FEMA). In 2015 and 2016, NPPD coordinated with FEMA Regional Interagency Steering Committees and engaged FEMA partners through cyber preparedness workshops and cybersecurity symposiums. Most recently, NPPD supported FEMA Region III with a 2-day, cyber preparedness symposium and DHS personnel moderated and sat for multiple panels alongside Federal, State, and private-sector cybersecurity officials.

As far back as 2009, NPPD began supporting the U.S. Secret Service (USSS) Critical Systems Protection efforts related to National Special Security Events. This coordination added a focus on cyber preparedness, joint IT operations coordination, and asset response coordination (i.e., ensuring the availability of technical mitigation resources for cyber attacks and incidents). In addition, NPPD assisted in the inauguration of several USSS Electronic Crimes Task Forces, to demonstrated not only a unity of effort in Federal preparedness and response but to bridge cyber crime and infrastructure resilience issues, specific to cyber planning, coordination, and best practice adoption.

Question 2a. According to the GAO testimony, DHS established a policy in October 2014 to conduct quarterly reviews of programs related to critical infrastructure to better understand the barriers critical infrastructure owners and operators face in improving the security of their assets. What trends has DHS identified in declinations using its tracking system since October 2013?

Has DHS identified barriers that critical infrastructure owners and operators face in making improvements?

Question 2b. If so, what are those barriers?

Answer. The quarterly program review process collects a broad range of information from across the Office of Infrastructure Protection (IP), and is a mechanism for improving data driven decision making. The assessment portfolio is one area of information collected.

In fiscal year 2015, approximately 88% of facilities where IP conducted an Infrastructure Survey Tool (IST) assessment reported they were likely to integrate, or have integrated, some of the protective measures detailed in the assessment report. This is up from 86% in fiscal year 2014 and 85% in fiscal year 2013. Four thousand four hundred sixteen ISTs have been conducted since fiscal year 2010. The most common improvements include enhancements to electronic security systems, security force, and security management. This kind of action is one important indicator of the impact that our assessments have on the security and resilience of infrastructure, but does not provide a perfect measure of the overall state of preparedness.

When stakeholders are interested in accepting IP's recommendations, the barriers that preclude them from making those changes include:

- Cost-prohibitive capital investments;
- Lack of project management resources;
- Differing strategic priorities;
- Plans to move or significantly change the facility;
- Local ordinances.

When partners decline IP services and capabilities, the most common reasons cited include:

- Facility isn't interested in assessment at the initial time of contact but indicated they would consider future survey;
- The facility has had a recent security assessment, either performed by the PSA or through another vulnerability assessment;
- Point of Contact (POC) requires coordination with corporate;
- POC lacks time to commit to assessment;
- Facility is confident in its security posture;
- Facility does not want to share its information with the Government;
- The facility does not allow data collection because it's a regulated facility, nuclear facility, or defense industrial base facility;
- Facility lacks a budget for implementing potential recommended security improvements; or
- Stakeholder believes the threat risk is low.

To formalize its response to these trends, NPPD is working to develop a 3-year Strategic Plan for Assessments conducted by IP to determine how it can enhance the value of its assessment portfolio for stakeholders, to include addressing physical and cyber convergence in assessments. The 3-year strategic plan will:

- Articulate the strategic intent of IP's assessments;
- Define specific goals to guide prioritization, maturation, management, and use of IP's assessments;
- Clarify opportunities for collaboration between IP assessments and OCIA analyses;
- Articulate mechanisms to assist the Federal Emergency Management Agency (FEMA) and other agencies in risk assessments supporting grant allocation decisions; and
- Provide a plan to develop and use performance metrics for program management and reporting processes.

This plan will guide how PSA-led assessments support stakeholders, contribute to a National understanding of risk, and support National preparedness planning. The CSA program will identify improvements by drawing upon this plan and its lessons learned.

Question 3. According to President Policy Directive 41 (PPD–41) Section V, "The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, shall be the Federal lead agency for asset response activities," as defined by the PPD. Do CSAs have any other cyber-related responsibilities that are not included in PPD–41 that are carried out by the NCCIC?

Answer. Presidential Policy Directive 41 (PPD–41) sets forth principles governing the Federal Government's response to any cyber incident and, for significant incidents, establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. The Department of Homeland Security, through our experts at the National Cybersecurity and Communications Integration Center (NCCIC), act as the Federal lead agency for asset response. Asset response includes helping a victim find the bad actor on its system, repair its system, patching the vulnerability, reducing the risks of future incidents, and preventing the incident from spreading to others.

Cyber Security Advisors (CSAs) do not themselves typically engage in asset response activities, especially asset response activities beyond those related to coordinating with relevant entities and providing advice on how to best use Federal resources. While CSAs may support the NCCIC role in cyber incident response by serving as field-based support elements, CSAs focus most of their resources on cyber preparedness and protective activities. CSAs engage private-sector companies and State, local, Tribal, and territorial (SLTT) governments prior to an incident to help them develop and assess their cyber incident response plan. In an incident, the primary role of a CSA is to connect the victim or potential targets with the resources of the NCCIC.

Question 4a. Dr. Ozment, can you advise us on the developmental and training plans for the CSAs to ensure that field-based personnel have a diverse cyber experience with computer engineering skills and are well-versed in cyber incident response activities with a solid working knowledge of the NCCIC and its capabilities, services and personnel?

Answer. Cyber Security Advisors (CSAs) are hired based on subject-matter expertise in Information Technology (IT) Security, Operations, and Management—to include proficiency with IT security program and project management, evaluation and assessment, technical communications and presentation, and system and network administration skills. Each CSA has unique training needs identified as they onboard and progress through their career. This includes an orientation and regular information on National Cybersecurity and Communications Integration Center (NCCIC) services available to customers.

Cybersecurity skills underlying CSA activities are identified, mapped to, and managed against workforce education initiatives and opportunities for cybersecurity awareness, training, and education. Additionally, a robust training and certification program is available to CSAs. This includes training in Information Security, Ethical Hacking and Penetration Testing, Networking, Industrial Control Systems Cybersecurity, and Risk Management.

Question 4b. How are you ensuring the CSAs are fully integrated with both the NCCIC and US–CERT? Are there plans to rotate the CSAs through the NCCIC and US–CERT to ensure they have the technical and incident response expertise?

Answer. Cyber Security Advisors (CSAs) are critical, field-based personnel with a sound understanding of the National Cybersecurity and Communications Integration Center (NCCIC). CSAs are a local resource for private-sector companies and SLTT partners. As such, CSAs often become the first element of NCCIC customer management: Coordinating incident response requests, facilitating requests for information, such as best practices and technical evaluations, routing requests for operational partnership, or access to technical threat analysis and vulnerability mitigation products. As the CSA program adds additional personnel, we will explore the possibility of rotations back to headquarters, to include rotations the NCCIC.

However, the CSAs are not hired for the skillset of technical incident response, nor should they be. There are many different skillsets in cybersecurity. The CSA skillset is intended to match more closely the skillset of a Chief Information Security Officer (CISO) or a CISO's policy, compliance, and metrics team. A CSA should be able to help a company develop a security program, identify gaps, provide strategic advice, and connect that company with services available from the Federal Government, particularly the NCCIC.

Question 4c. How will you ensure that CSAs and their cyber outreach and engagement activities are fully integrated into the rest of CS&C's cyber efforts before, during, and after cyber incidents?

Answer. CSAs are not focused on cyber incident response: Their primary role is on prevention and preparedness.

There have been very few instances, due to the small number of Cyber Security Advisors (CSAs), where a CSA had a prior engagement with a private-sector company or State, local, Tribal, and territorial (SLTT) partner, and that same partner experienced a cyber incident. In these few cases, CSAs were generally the first point of notification by the victim. CSAs determined the situational information surrounding the event and the victim's basic needs for assistance.

Under these limited instances, after an incident, CSAs also provided direct process improvement guidance on the cyber incident process and worked to identify cyber preparedness and best practice efforts for consideration by the victim's cyber program planning, operations procedures, and resource allocations.

Question 5. Has DHS identified any best practices in assessing and addressing vulnerabilities from threats and hazards that our Nation's critical infrastructure owners and operators face, and if so, has DHS shared these practices with other critical infrastructure partners to help them be more prepared?

Answer. The National Protection and Programs Directorate (NPPD) is a clearing house for best practices and lessons learned, which are continuously gathered through Protective Security Advisor (PSA) and Cyber Security Advisor (CSA) engagements and then shared with critical infrastructure partners.

PSA-led and CSA-led assessments produce a dashboard and/or a report that assist stakeholders in identifying key considerations for enhancing the security and resilience. The dashboards provide a comparative analysis an entity's security and resilience, including a high, low, and median score comparison. The reports contain a written analysis of the assessments key findings. This includes documenting vulnerabilities and identifying corresponding options for owner and operators. These options are, in effect, best practices that have been observed and compiled since 2009. Reports also document "commendable" items when an entity has already implemented best practices.

As a result of PSA and CSA support to special events and domestic incidents, we collect after-action reports and lessons learned. In addition, DHS is drafting an "Effective Practice" document that will identify documented best protective measure practices.

NPPD works with critical infrastructure partners to assess areas of concern and potential vulnerability gaps. These findings inform the development of best practices for consideration by owners and operators. A sampling includes:

Suspicious Activity Videos.—(https://www.dhs.gov/gallery/infrastructure-protection) provide information on identifying and reporting suspicious activity and threats in different environments and scenarios, including:

- Check It! (Bag search procedures for public venues);

- What's in Store: Ordinary People/Extraordinary Events (Retail);
- No Reservations: Suspicious Behavior in Hotels (Lodging); and
- Options for Consideration (Active Shooter).

On-line Training Courses.—Self-paced courses (offered through the Federal Emergency Management Agency's (FEMA) Emergency Management Institute (EMI) *https://training.fema.gov/emi.aspx)* designed for both people who have emergency management responsibilities and for the general public. All are offered free-of-charge. DHS has partnered to produce courses in active shooter, surveillance awareness, and more. Each course, listed below, takes approximately 45 minutes to complete.

- IS–906 Workplace Security Awareness;
- IS–907 Active Shooter: What You Can Do;
- IS–912 Retail Security Awareness—Understanding the Hidden Hazards;
- IS–914 Surveillance Awareness: What You Can Do;
- IS–915 Protecting Critical Infrastructure Against Insider Threats; and
- IS–916 Critical Infrastructure Security: Theft and Diversion—What You Can Do.

For those involved in the security of industrial control systems, the National Cybersecurity and Communications Integration Center offers several cybersecurity courses. These courses can be accessed at: *https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT*.

Through our Federal Virtual Training Environment (FedVTE) we offer more than 800 hours of on-line, on-demand training on cybersecurity topics such as ethical hacking and surveillance, risk management, and malware analysis. Course proficiency ranges from beginner to advanced levels, and several of the courses align with Information Technology certifications such as Network+, Security+, and Certified Information Systems Security Professional. FedVTE has been available to Federal, State, local, Tribal, and territorial Government employees. Additionally, we've teamed up with the non-profit organization Hire Our Heroes to provide U.S. veterans with free access to FedVTE.

Hands-on Training.—In addition to on-line training courses, EMI provides two Integrated Emergency Management Courses (IEMC) that provide exercised-based training events to local and county communities, based upon the community's Threat and Hazard Identification and Risk Assessment (THIRA) and Emergency Operations Plan. IEMCs are a combination of classroom lectures, discussions, small-group planning sessions, and functional exercises which expose participants to new ideas, and increase their awareness of the necessary coordination among other agencies and organizations. For the exercises, each participant is assigned a role similar to their real-life position in an emergency operations center (EOC).

- *E0912*.—Preparing Communities for a Complex Coordinated Attack IEMC: Community-Specific; and
- *E0930*.—IEMC: Community-Specific.

NPPD provides hands-on training to private-sector critical infrastructure partners. For example, the National Cybersecurity and Communications Integration Center provides intermediate and advanced training classes on cybersecurity for industrial control systems through regional classroom training on a quarterly basis. Notably, these offerings include an advanced training offered at our facility in Idaho Falls. This 1-week course includes a two-team activity that lasts for half a day. The red team attacks and the blue team defends a small critical infrastructure facility we built.

Protective Measures Guides: FOUO guides that assist owners and operators in planning and managing security at their facilities. Guides exist for:

- Sports Leagues (2008—being updated);
- Lodging (2010);
- Outdoor Venues (2011); and
- Commercial Real Estate (2013).

Evacuation Planning Guides for Stadiums and Major Events.—Assists stadium owners and operators with preparing evacuation plans and helping to determine when and how to evacuate, shelter-in-place, or relocate stadium spectators and participants.

Patron Screening Best Practices Guide.—Provides suggestions and best practices for developing and implementing patron screening procedures at public assembly venues.

Sports Venue Bag Search Procedures Guide.—Provides suggestions for developing and implementing bag search procedures at sporting event venues hosting major sporting events. The purpose for establishing bag search procedures is to control items that are hand-carried into the sports venue. The bag search procedures should be a part of the venue's overall security plan and should be tested and evaluated

as outlined in the security plan. The actual implementation of bag search procedures and level of search detail will depend upon the threat to the venue as determined by the venue's security manager.

Sports Venue Credentialing Guide.—Provides suggestions for developing and implementing credentialing procedures at sporting event venues that host professional sporting events. The purpose for establishing a credentialing program is to control and restrict access to a sports venue, and to provide venue management with information on those who have access. Credentialing can also be used to control and restrict vehicle movement within a venue.

Additionally, IP offers information and resources founded in best practices to support critical infrastructure partners in the identification and assessment of vulnerabilities and the adoption of mitigating measures through the IP Digital Library, which is offered through the IP Gateway. Through the IP Digital Library, Federal, State, and local critical infrastructure partners can access sector-specific materials relating to various industry best practices; Information-sharing resources, practices, and protocols; applicable Standards; sector-specific resilience reports; and other research and analytic materials relating to critical infrastructure protection and resilience. The Digital Library also features the Infrastructure Protection Report Series (IPRS) which highlight common vulnerabilities and potential indicators for specific subsets of critical infrastructure systems, clusters, and assets.

On the cyber side, DHS participated in the development of the National Institute for Standards and Technology's (NIST) Cybersecurity Framework, a key resource for best practices. The Critical Infrastructure Cyber Community Voluntary (C3VP) was created to help improve the resiliency of critical infrastructure's cybersecurity systems by promoting the use of the Framework. Reference materials and assessment tools targeted to stakeholder groups can be found on-line: *https://www.us-cert.gov/ccubedvp*. Additionally, DHS shares information among public and private-sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost. For example, the Cyber Resilience Review Implementation Guide series is publicly available at the US–CERT website to help organizations systematically address gaps in management that often lead to vulnerabilities. The ICS–CERT website contains alerts, advisories, and other products for critical infrastructure owners and operators. These resources can be found at: *https://www.us-cert.gov* and *https://ics-cert.us-cert.gov/*.

In fiscal year 2016, IP initiated a "Connect, Plan, Train, and Report" campaign that is rooted in best practices to assist public and private stakeholders proactively think about the role they play in the safety and security their environment. In support of this effort, we consolidated a number of key tools and resources for small and medium venues as well as public-sector partners, on *www.dhs.gov/hometown-security*. PSAs are actively engaged in this messaging campaign, and we have developed a simple information card they can hand out to stakeholders. We have also been able to share this messaging through the Secretary's and other DHS senior leadership engagements.

Question 6. Dr. Ozment, how do the CSAs currently leverage, or plan to leverage, the existing field relationships that already exist between the private sector and Secret Service or the FBI?

Answer. Cyber Security Advisors (CSAs) regularly engage with a number of Federal field offices, including: The Federal Bureau of Investigation, U.S. Secret Service, Homeland Security Investigations, U.S. Coast Guard, Federal Emergency Management Agency (FEMA), and other partners in the field. In the case of FEMA, as noted in the Department's response to Congressman Ratcliffe's QFR No. 1, CSAs work with several FEMA Regions to help jurisdictions prepare for potential physical consequences during and after a cyber incident. In addition, CSAs leverage their relationships to assist with introductions to owners and operators of critical infrastructure. However, each of these agencies have relationships with the private sector that differ from those created by a CSA. CSA engagements with private-sector companies are voluntary, not law enforcement or regulatory. CSAs focus on cyber preparedness, best practice promulgations, and incident planning. While CSAs leverage those existing mechanisms, for instance to prepare cybersecurity practitioners to work with cyber threat and incident response partners, the CSA mission has a focus not currently replicated within the Federal Government.

Question 7. Can you walk us through a day in the life of a CSA? At this stage in the program's evolution, I think it will be helpful for us to understand how much of their time is focused on making new connections, following-up on existing relationships, conducting assessments, etc.

Answer. Upon initial assignment to a region, new Cyber Security Advisors (CSAs) spend significant time forming relationships with existing Federal, State, and infra-

structure sector partners, and building holistic approaches to cyber infrastructure protection and resilience. CSAs look for opportunities to augment what are typically general cyber threat, incident response, and crisis management activities, with a full spectrum of cyber preparedness, risk mitigation, and incident planning activities—covering cyber asset identification, protection, detection, response, and recovery practices. As CSAs build competence with partner and individual engagement activities, CSAs lead cybersecurity evaluation activities; deliver cyber process improvement and best practice adoption activities; deliver cyber preparedness and planning workshops and presentations; attend meetings to advise cybersecurity leaders in State, local, Tribal, and territorial (SLTT) agencies and private-sector companies; augment cybersecurity awareness, education, and exercise programs; support cyber threat and vulnerability-focused outreach initiatives; work to enhance operational capabilities and capacity within cyber communities-of-interest; advising on SLTT cyber policy and resource activities; and supporting other Federal agency and Sector-Specific Agency cyber engagements.

Question 8. When a cyber incident occurs on an entity that previously engaged with a CSA, what are the roles and responsibilities of that CSA during and after an incident? How is that CSAs previous relationship leveraged during and after an incident?

Answer. Cyber Security Advisors (CSAs) are not focused on cyber incident response: Their primary role is on prevention and preparedness.

There have been very few instances, due to the small number of CSAs, where a CSA had a prior engagement with a private-sector company or State, local, Tribal, and territorial (SLTT) partner, and that same partner experienced a cyber incident. In these few cases, CSAs were generally the first point of notification by the victim. CSAs determined the situational information surrounding the event and the victim's basic needs for assistance.

Under these limited instances, after an incident, CSAs also provided direct process improvement guidance on the cyber incident process and worked to identify cyber preparedness and best practice efforts for consideration by the victim's cyber program planning, operations procedures, and resource allocations.

Preparedness Data—Cyber Security: In the Threat and Hazard Identification and Risk Assessment (THIRA) process, States, territories, urban areas, and Tribes identify their threats and hazards of greatest concern and set capability targets that define success in each core capability. States and territories then complete a State Preparedness Report (SPR) to assess their current capabilities relative to their THIRA targets.

In the 2015 THIRA, 80 percent of States and territories included a cyber attack as a threat or hazard of primary concern, the highest percentage of all threats and hazards. In the SPR, States and territories identified cybersecurity as their lowest-rated capability; Only 13 percent of State and territory responses were identified as proficient (4 or 5 rating on 5-point scale). States and territories have identified cybersecurity as their lowest-rated capability for 5 consecutive years.

Question 9. What are the specific metrics by which the effectiveness of the CSA program and the assessment tools used by a CSA are (or will be) measured?

Answer. Due to the small number of Cyber Security Advisors (CSAs) at this time (less than 5), program effectiveness is currently measured against limited factors. These include qualitative factors such as how partners engaged in CSA outreach, working groups, and assessments. CSAs report on levels of community planning toward best practices and produce yearly analysis of partner cyber readiness, to include factors based upon capability, capacity, and maturity. Measures and metrics for cyber assessment effectiveness are based upon the direct solicitation and receipt of feedback from evaluation.

QUESTIONS FROM RANKING MEMBER CEDRIC L. RICHMOND FOR ANDY OZMENT

Question 1. DHS has issued a Notice of Suspension and Modification of Certain Submission Requirements for Chemical Facilities of Interest and Covered Chemical Facilities Under Agency Regulations (81 FR 47001) to inform the public that the requirement to submit vulnerability assessments and other applications would be suspended until October 1, 2016 to allow the Infrastructure Security Compliance Division (ISCD) an opportunity to transition to "CSAT 2.0"—an updated risk-tiering tool that will make much-needed improvements to the existing risk assessment methodology. The Notice provides that, once implemented, facilities will be individually notified to re-submit applications using CSAT 2.0. Notification will be phased. Which facilities will be notified first, and how will facilities be staggered (i.e., by Tier? Location? Date of original submission?)

When does ISCD expect to complete these notifications?

Answer. The Department intends to notify a broad cross-section of the regulated community during the initial batch notification in order to allow us to more quickly assess the actual impacts of the updated tiering methodology and CSAT Top-Screen application on all portions of the regulated community. The initial notification batch will include both tiered and untiered facilities, across the country. Subsequent notification batches are expected to include a cross-section of the regulated community although batch composition may be adjusted, as lessons are learned, during the review of the initial Top-Screen submissions. The Department currently envisions notifying batches consisting of between 500 to 1,000 facilities every 2 weeks, with all chemical facilities of interest anticipated to have received notification by the end of fiscal year 2018.

Question 2. The planned roll-out of CSAT 2.0 will necessarily involve a high volume of facilities re-submitting applications within a very short time frame. Does ISCD have systems, processes, and personnel in place to review these resubmissions expeditiously and in a way that does not result in administrative backlog (as seen in past years)?

Answer. DHS is implementing a phased approach for reaching out to the facilities. The phased approach decision was made in part to reduce the likelihood of an administrative backlog, and was based on existing Infrastructure Security Compliance Division resource levels and information technology capabilities. Additionally, as DHS receives and reviews Top-Screens and issues high-risk determinations, DHS will evaluate the length of time for each step and make adjustments, as needed, to help prevent an administrative backlog.

Question 3. On page 47002, the Notice explains that chemical facilities of interest, including facilities previously determined not to be high-risk, will be among the facilities notified of the requirement to re-submit applications using CSAT 2.0. Another section provides that un-tiered facilities will not be notified or subject to the re-submission requirement. Please provide more clarity on which facilities will be notified, particularly with regard to facilities that may have been found not to present a high level of risk in the past but should be reconsidered against the updated tiering methodology.

Answer. All chemical facilities of interest, including facilities previously determined not to be high-risk, will be required to submit a Top-Screen using the revised CSAT 2.0 Top-Screen application unless they fall into 1 of the 4 categories of facilities enumerated in Section IV of the Department's *Federal Register* Notice. 81 FR 47002. The 4 categories enumerated in Section IV are as follows:

- Agricultural Production Facilities, as defined in 73 FR 1640, or any facility subject to a similar extension issued by the Department for submitting a Top-Screen;
- Chemical facilities of interest whose only reportable chemical of interest is present in a gasoline mixture;
- Facilities that are statutorily excluded from CFATS which include: (A) Facilities regulated under the Maritime Transportation Security Act of 2002 (Pub. L. 107–295; 116 Stat. 2064); (B) public water systems, as that term is defined in section 1401 of the Safe Drinking Water Act (42 U.S.C. § 300f); (C) Treatment Works, as that term is defined in section 212 of the Federal Water Pollution Control Act (33 U.S.C. § 1292); (D) facilities owned or operated by the Department of Defense or the Department of Energy; or (E) facilities subject to regulation by the Nuclear Regulatory Commission, or by a State that has entered into an agreement with the Nuclear Regulatory Commission under section 274(b) of the Atomic Energy Act of 1954 (42 U.S.C. § 2021(b)) to protect against unauthorized access of any material, activity, or structure licensed by the Nuclear Regulatory Commission); and
- Untiered facilities that previously submitted a Top-Screen with no Chemicals of Interest (COI) selected (i.e., facilities that have informed the Department they no longer possess a reportable amount of any COI), so long as the facility has not come into possession of a reportable amount of COI since submitting their previous Top-Screen.

Question 4. Months before the July 20, 2016 notice in the *Federal Register,* ISCD circulated a statement about the suspension to "the regulated population and industry associations to ensure maximum dissemination." Why was the committee not included in this correspondence? How will ISCD ensure that the committee is kept apprised of the status and progress of the CSAT 2.0 transition?

Answer. In this case, the Department notified the committee separately of the forthcoming suspension rather than include committee Members or staff on the communication to the regulated population and industry associations. The Department provided this notice to the committee, via e-mail to multiple committee staff members, on June 21, 2016, 1 day after telephonically informing the Chemical and Oil

and Natural Gas Sector Coordinating Councils (SCCs) of the forthcoming suspension, and prior to providing written notification to the SCCs. In the future, the Department will ensure that it informs the committee via phone or e-mail of any major programmatic activities, such as the decision to temporarily suspend Top-Screen submission requirements, and, as always, the Department is able to provide briefings to the committee on any aspect of CFATS, including the CSAT 2.0 transition, upon request.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR CAITLIN DURKOVICH

Question 1. Ms. Durkovich, we are all aware that the majority of the programs provided by the Office of Infrastructure Protection to owners and operators of critical infrastructure are voluntary in nature. Because of this it is incumbent on DHS to promote and market the value of its services. As I mentioned in my statement, the DHS website for critical infrastructure vulnerability assessments has conflicting and outdated programs.

While a few minor corrections can remediate a website, those errors lead to a larger question of how NPPD is communicating the value-added proposition to critical infrastructure owners and operators. Can you please discuss how NPPD currently communicates the value of these voluntary programs to the private sector?

Answer. Through the National Protection and Programs Directorate's (NPPD) strategic engagement efforts, we take a proactive approach to ensure that the full range of available tools, capabilities, and resources are well understood by our customers, including the Federal Government; State, local, Tribal, and territorial governments; and private-sector entities. Our customer engagements include outreach by our field-based Protective Security Advisors and Cyber Security Advisors. At the National level, NPPD collaborates through the National Infrastructure Protection Plan (NIPP) Council, consisting of public and private-sector entities to identify requirements and build capabilities for mitigating risks. Examples include assessments, intelligence products, and information-sharing platforms.

In addition, NPPD works with organizations across the country to disseminate targeted information on voluntary programs available to critical infrastructure owners and operators. Recent examples include keynotes and panel participation at events such as the National Sports Safety and Security Conference, Retail Industry Leaders Association Forum, National Homeland Security Conference, Corporate Security Symposiums, the National Conference on Building Resilience through Public-Private Partnerships, and the Domestic Security Alliance Council conference.

NPPD also hosts forums with our many partners utilizing the Critical Infrastructure Partnership Advisory Council (CIPAC) where stakeholders provide direct feedback. This translates into actionable capabilities available at the regional, State, and local levels to include assessments, exercises, and workshops. These include the Active-Shooter Preparedness Program, the Homeland Security Information Network-Critical Infrastructure portals, the Private-Sector Clearance Program, and education and training resources.

These capabilities are actively represented by the Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) who work directly with critical infrastructure owners and operators every day. In fiscal year 2015, PSAs conducted 2,131 Enhanced Critical Infrastructure Protection visits. These visits provide critical infrastructure owners and operators with information on their facility, explain how their facility fits into its critical infrastructure sector, and provide an overview of resources available to enhance the facility's security and resilience. Similar information is delivered during PSA speaking engagements, panels, webinars, and meetings.

In fiscal year 2015, the 5 CSAs conducted 468 cybersecurity engagements. On-average 90 were conducted by each CSA within their assigned region and 13 were performed by a CSA outside of their assigned region. These engagements encompass all evaluations, cyber protective visits, workshops, resource briefings, and speaking engagements. Engagements focus on assessment, planning, and promotion of cyber preparedness, risk mitigation, and asset response coordination.

Question 2. In responding to an incident, what are the roles and responsibilities of a PSA and how do they engage with the lead agency as the situation is developing and post-incident?

Answer. As part of the National Planning Frameworks and Federal Interagency Operational Plans, the Protective Security Advisors (PSAs) support response, recovery, and reconstitution efforts during incidents. During an incident, the PSAs deploy to the Joint Field Offices; National and Regional Response Coordination Centers (RRCC); and regional, State, and county Emergency Operations Centers (EOCs) as necessary to support Federal and State emergency response officials, to include the

Federal Coordinating Officer and the Unified Command Group. They serve as Infrastructure Liaisons by providing expert knowledge of the impacted infrastructure; maintaining communications and information sharing with owners and operators of critical infrastructure; and prioritizing and coordinating response, recovery, and reconstitution efforts. Specific to Emergency Support Functions (ESFs), PSAs provide direct support to lead agencies by leveraging established relationships with owners and operators of critical infrastructure. For example, under ESF–12, a PSA would support the Department of Energy with reestablishment of damaged energy systems and components. PSAs often assist with connecting owners and operators with appropriate agencies.

Question 3. What are the specific metrics by which the effectiveness of the PSA program and the various assessment tools are measured?

Answer. Quarterly and end-of-year performance measures are submitted under the Government Performance and Results Act (GPRA). One of these measures includes the percentage of critical infrastructure facilities that are likely to enhance their security and resilience by integrating Infrastructure Protection (IP) vulnerability assessments or survey information. Providing facilities with vulnerability information allows them to understand and reduce their risk. In fiscal year 2016 Q3, 90% of facilities reported they were likely to integrate, or have integrated, some of the protective measures detailed in their assessment report.

For fiscal year 2016, IP has delivered 507 Infrastructure Survey Tool (IST) dashboards to owners and operators. The IST provides Protective and Resilience Measures Indices for facility owners and operators and identifies physical security, security management, protective measures, information sharing, dependencies, and capabilities related to preparedness, mitigation, response, resilience, and recovery. Performance is measured against a delivery of 600 IST surveys by September 30, 2016.

The Regional Resiliency Assessment Program (RRAP) is measured by primary stakeholders that have implemented, planned to implement, or are in the process of implementing at least one security or resilience enhancement related to RRAP Key Findings within 3 years following the publication of the final RRAP report. This metric stands at 50%.

The PSAs support National Special Security Events (NSSE) and Special Events Assessment Rating (SEAR) Level 1 & 2 events with on-site critical infrastructure expertise, products, and analysis. Performance is measured by supporting 100% of the NSSEs and SEAR 1& 2 level events in fiscal year 2016. Some of the events include Super Bowl 50, and the Republican National Convention and Democratic National Convention. This metric stands at 100%.

PSAs support Federal, State, local, Tribal, and territorial partners, and owners and operators of critical infrastructure during man-made or natural incident response. In fiscal year 2016, PSAs have responded to 201 incidents.

Question 4. Since 2004, DHS has maintained infrastructure protection field operations throughout the Protective Security Advisory (PSA) program. PSAs are trained critical infrastructure protection and vulnerability subject-matter experts. Given the complexity of critical infrastructure protection and the largely private ownership, what barriers, if any, impede DHS's ability to partner with facility owners and operators through the PSA program?

Answer. The most common barriers are:

- The point of contact (POC) requires coordination with their corporate office,
- POC lacks the amount of time to commit to an assessment,
- Facility is already confident in its security posture,
- Facility does not allow data collection as it is a regulated facility (nuclear or defense industrial base),
- Facility lacks a budget for implementing potential security improvements,
- Facility does not want to share its information with the Government.

In addition to these concerns, DHS is working to address the logistical challenge of placing sufficient staff in the field to meet the needs of our diverse and disparate stakeholders. The PSA program has been successful in large part because it provides trained staff across the Nation, reaching outside of Washington, DC, to form trusted relationships. In fiscal year 2016, DHS began a disciplined shift to build on this model and emphasize regional activities. Support for this regionalization initiative is one of the most important ways to improve DHS's ability to partner with facility owners and operators.

Since its inception, the PSA program has focused on supporting partners in hardening and securing existing infrastructure. As the program has matured, the partner needs have evolved, and the PSA program is adapting to support a broad range of risk management and resilience activities across infrastructure sectors, stakeholder groups, threats, and hazards.

Question 5. Dr. Ozment, how is the CSA program engaging with the critical infrastructure community in light of the fact that most critical infrastructure is privately owned and operated?

Answer. Engagements with critical infrastructure owners and operators are voluntary-based. Our Cyber Security Advisors (CSAs) focus on building trusted relationships with owners and operators, demonstrating the value we bring through risk assessments and connecting customers to our services, sharing best practices, and sharing the current threat landscape. One way we reach this community is through existing fora, such as InfraGard, Electronic Crime Task Forces, Cyber Working Groups, Area Maritime Security Committee Meetings, and industry conferences. Additionally, our CSAs leverage existing relationships within the Department, including those that have been developed by Protective Security Advisors and the National Cybersecurity and Communications Integration Center (NCCIC).

CSAs work with State cybersecurity leaders, including Homeland Security Advisors, Chief Information Security Officers, and cyber infrastructure protection and emergency management planners, to engage critical infrastructure owners and operators through State-led cyber working groups, information-sharing and analysis centers, fusion centers, and law enforcement outreach groups.

Question 6. GAO reported that DHS has conducted thousands of assessments of critical infrastructure in the last few years using at least 10 different tools. These tools do not all cover the same vulnerabilities, they vary in detail and complexity, and some overlap. GAO made recommendations that DHS should address the overlap to avoid potentially unnecessary duplication and gaps. According to the GAO, DHS established a working group to address the overlapping assessments and potential duplication and gaps. What is the status of fulfilling GAO recommendation?

Answer. The Department of Homeland Security (DHS) concurred with GAO's recommendations and has moved forward to harmonize critical infrastructure security vulnerability assessments across Federal departments and agencies. Over the past couple of years, the National Protection and Programs Directorate's (NPPD's) Office of Infrastructure Protection has worked with the Transportation Security Administration (TSA), the Federal Protective Service (FPS), the United States Coast Guard (USCG), the Office of Cybersecurity and Communications (CS&C), and other DHS agencies to collaboratively identify a core set of questions and anticipated response options from the single assessment methodology.

The Cross-Agency Vulnerability Assessment Working Group, consisting of members from Federal departments and agencies with relevant vulnerability assessments, was charged to:

- Identify key critical infrastructure security-related assessment tools and methods used or offered by Federal departments and agencies;
- Analyze the key critical infrastructure security-related assessment tools and methods to understand areas each assessment captures;
- Develop and disseminate guidance for areas that should be included in vulnerability assessments of critical infrastructure to enable a more coordinated and integrated approach.

To support the working group, NPPD established a portal for departments and agencies to upload documentation to include vulnerability assessment questionnaires, methodology, user guides, fact sheets, and other technical documentation.

NPPD completed an analysis of tools and methodologies across approximately 5,000 assessments, the findings of which identified that core questions in 6 Key Security Areas have the greatest impact on infrastructure security, while covering the range of security areas envisioned by GAO. Consequently, NPPD has provided these core questions to Federal partners and has recommended inclusion of the questions in the next update or modification to respective Assessment questions and/or tools. With respect to DHS assessment tools, these core questions have been and will be continue to be integrated into all assessment tools when appropriate and used across the Department to further enable cross component and agency comparison of assessed assets and risk.

In addition, NPPD/IP has implemented a single assessment methodology that enables the IP mission partners to assess vulnerabilities and risk using the IP Gateway suite of assessment tools and integrated situational awareness and analytic planning and response tools. More than 80 State and Federal Department and agency partners currently use the IP Gateway to support their critical infrastructure protection needs. NPPD is currently working with additional partners to become IP Gateway partners.

Question 7. Given the number of assessments, how prepared are the Nation's most at-risk critical infrastructure to threats from international and domestic terrorists and other high-risk vulnerabilities and hazards?

Answer. NPPD's work has demonstrated that the Nation's most at-risk critical infrastructure is well-prepared—but faces new and continually evolving challenges. In addition to facing increasingly dynamic international and domestic terrorist threats and a wide range of hazards, the demands placed on infrastructure systems are expanding, while the American communities that infrastructure serves and supports have increasingly diverse needs. This environment of change emphasizes the importance of investing in the tools and resources that DHS provides for making security decisions about critical infrastructure. Further compounding these challenges is the underinvestment in critical infrastructure and the reality that the demand on infrastructure in the United States is increasing while investment capital is flagging.

The 2016 National Preparedness Report identified the Infrastructure Systems core capability within the National planning system as 1 of 6 capabilities that remain National areas for improvement. Likewise, based on State Preparedness Report (SPR) data, States and territories reported some of the lowest proficiency in the Protection mission area, which is relevant to critical infrastructure. However, notwithstanding the remaining gaps in reported proficiency, we are seeing improvement over time. For example, based on a review of SPR "proficiency delta data," 71% of core capabilities in the Prevention mission area, 64% in Protection, and 86% in Mitigation were reported as improving in proficiency from 2012–2015. In 2016, the first edition of the Protection Federal Interagency Operational Plan was completed, paving the way for an improved interagency model for coordinating infrastructure security and resilience concerns.

In the area of National preparedness, there are evident areas for growth, and areas where the IP assessment programs can increase their support for that growth. The DHS assessment programs are vital tools for continuing to improve our understanding of risks to infrastructure, providing resources for managing those risks, and encouraging owners and operators to take action. IP assessments contribute to the preparedness of the Nation's infrastructure through a model of continued engagement and evaluation. Because our critical infrastructure is heavily networked, both large and small infrastructure enterprises can be central to security and resilience, and IP's suite of assessment capabilities is tailored to meet the varied needs of our stakeholders.

Corresponding to this networked nature of our critical infrastructure, DHS measures the success of its assessment program both in terms of completing assessments, and in terms of our stakeholders taking action based on the indices and information developed through our assessments. In terms of completing assessments, since fiscal year 2010, 4,416 Infrastructure Survey Tool (IST) assessments have been conducted. In fiscal year 2015, approximately 88% of facilities where DHS conducted an Infrastructure Survey Tool (IST) assessment reported they were likely to integrate, or have integrated, some of the protective measures detailed in the assessment report. This is up from 86% in fiscal year 2014 and 85% in fiscal year 2013. The most common improvements include enhancements to electronic security systems, security force, and security management. This kind of action is one important indicator of the impact that our assessments have on the security and resilience of infrastructure, but does not provide a perfect measure of the overall state of preparedness of the Nation's infrastructure.

Furthermore, the security and resilience of our Nation's critical infrastructure relies on robust sector coordination structures developed under the National Infrastructure Protection Plan, meaning that measuring impact of the IP assessment program on the security and resilience of the Nation's critical infrastructure is tied to measuring the success of these coordination structures. In 2016, all of the Sector-Specific Plans under the NIPP were updated, improving our ability to work within and across infrastructure sectors to set priorities and manage risk. NPPD provides support to owners and operators across the 16 critical infrastructure sectors that have grown due to the increasingly complex and dispersed nature of the threat, including soft targets and cyber dependence.

Measuring the success of IP assessment programs must be a continuous and evolving process to capture the increasingly complex and dispersed nature of threats, as well as other high-risk vulnerabilities and hazards to at-risk infrastructure. Accordingly, at the direction of Congress, NPPD is currently undertaking a 3-year strategic plan for IP's assessments that will strengthen our ability to leverage the data we have collected during assessments to characterize our National understanding of risks, support National preparedness planning, and support our partners. This plan will allow us to better understand how DHS assessment programs inform our National picture of risk, as well as how data from assessment programs can both improve our prioritization efforts and better support National preparedness planning, particularly as it relates to our most at-risk critical infrastructure and physical/cyber convergence in assessments.

In a continually evolving environment, we strive to respond to threats, high-risk vulnerabilities and hazards to our Nation's most at-risk critical infrastructure through the use of DHS assessment programs and continued coordination with both large and small infrastructure enterprises. The DHS assessment programs are one tool that we use that can provide great value for owners and operators to take action. DHS assessment programs, as well as the 3-year strategic plan for assessments are integral mechanisms for understanding the increasingly complex and dispersed nature of threats, improving our prioritization efforts, and better supporting National preparedness planning.

Question 8. How are the PSAs engaging with their counterparts from Sector-Specific Agencies such as the Department of Energy or Environmental Protection Agency, in ensuring our Nation's critical infrastructure is protected?

Dr. Ozment, the same question regarding the CSAs?

Answer. Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) engage with Sector-Specific Agencies (SSAs) during assessments, incident response efforts, and threat-directed outreach.

The National Protection and Programs Directorate (NPPD) serves as the SSA for 6 of the 16 critical infrastructure Sectors and coordinates with the other 10 sectors. Through this voluntary partnership framework consisting of a Government Coordinating Council and a Sector Coordinating Council an effective mechanism has been established for collecting data, sharing information, and advancing collective actions for National critical infrastructure security and resilience. NPPD employs sector liaisons who are responsible for serving as conduits between the Department and external SSAs.

Training.—The Office of Infrastructure Protection (IP) in collaboration with the Environmental Protection Agency (EPA) and Water Sector partners developed an on-line training course, "Risk Management for the Water Sector." The course is designed to provide water and wastewater facility owners and operators with general knowledge of risk management. In addition, the course introduces EPA's Vulnerability Self-Assessment Tool (VSAT).

Threat-Directed Outreach.—During outreach to State, local, Tribal, and territorial (SLTT) Government and private-sector partners, PSAs coordinate activities with appropriate Federal agencies and SSAs. For example, in response to a coordinated attack on an electric substation in Metcalf, CA, on April 18, 2013, the Department of Energy (DOE) and the Department of Homeland Security (DHS), in coordination with the Federal Bureau of Investigation, the Federal Energy Regulatory Commission's Office of Energy Infrastructure Security, the Electricity Sector Information Sharing and Analysis Center partners, and industry experts conducted a series of briefings Nation-wide for owners, operators, and local law enforcement. These briefings provided a threat overview, and information on available tools, resources, and best practices. Additional targeted PSA-led efforts were conducted in partnership with service providers such as Exelon/PECO and ConEdison.

Assessments.—One of the major strengths of the Regional Resiliency Assessment Program (RRAP) is the collaboration that brings together Federal, State, local, Tribal, and territorial governments, and the private sector to work with DHS. Collaboration at the regional level is led by the PSAs assigned to execute the project, with support from CSAs. Interagency coordination occurs between headquarters offices as well. The RRAP team provides project briefings to the SSAs and their Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs). SSAs are relied upon to provide insight into the operations and vulnerabilities of infrastructure, as well as to connect the RRAP project teams, which include PSAs and CSAs, to relevant industry and Government contacts who can assist in the assessment and analysis. Some examples of SSA and interagency involvement include:

- DOE has assisted DHS on numerous oil and natural gas RRAP projects. Current collaboration includes a resilience project for the electric power grid in the Northeast in support of recommended actions from the 2015 Quadrennial Energy Review.
- U.S. Coast Guard (USCG) is a strong SSA partner. The USCG is included in port- or maritime transportation-related RRAP projects. Examples include the 2013 Columbia River Basin project and the 2016 Gulf of Mexico project, in support of the USCG-led Gulf of Mexico Area Maritime Security Committee.
- U.S. Army Corps of Engineers regularly participates in dam-related projects. They are currently involved in a 2015 project in Louisville, Kentucky, and a 2016 project in Branson, Missouri.
- Department of Transportation regularly participates in transportation disruption-focused projects, including the 2013 Cajon Pass (California) and 2014 Alaska projects.

- U.S. Department of Agriculture has been involved in the agriculture-focused projects in Texas, California, Alabama, New Mexico, examining issues such as biosecurity of the cattle industry and the milk supply chain.

In addition to the SSAs, the RRAP team also works with other Federal agencies, including the Federal Emergency Management Agency (FEMA), the National Oceanic and Atmospheric Administration (NOAA), U.S. Geological Survey (USGS), and other Emergency Support Function (ESF) and Recovery Support Function (RSF) leads. FEMA contributes hazard information and insight into regional disaster planning and capabilities. In turn, RRAP analyses improve planning factors related to infrastructure dependencies and hazard impacts. NOAA and USGS provide very specific, useful hazard information and models (e.g., earthquakes, tsunamis, overland flooding/storm surge) that the RRAP uses to inform analyses of infrastructure impacts. The many ESF and RSF agencies provide insight into their response and recovery roles, capabilities, and plans.

Incident Response.—PSAs engage the agencies designated as Emergency Support Function (ESF) and Recovery Support Function (RSF) leads, which include SSAs.

Under the Recovery Support Functions for infrastructure systems, the U.S. Army Corps of Engineers is the National Coordinating Agency for the Federal Government's efforts to support recovery goals related to the public engineering of the Nation's infrastructure systems. NPPD is a Primary Agency in this effort, along with a number of other SSAs who serve as Primary Agencies or Supporting Organizations. In this role, PSAs may deploy to Joint Field Offices (JFO) or Regional Field Offices (RFO) to assist with infrastructure recovery operations.

Cyber Security Advisors.—CSAs engage with SSAs to raise awareness and improve readiness. For example, CSAs work with SSAs to identify sector-based, critical cyber services. CSAs then focus voluntary cybersecurity evaluations at these services. Additionally, the CSAs assisted DOE with developing the Electricity Subsector—Cybersecurity Capability Maturity Model (ES–C2M2) assessment, which is derived from the Cyber Resilience Review. ES–C2M2 is a sector-specific maturity model that guides electricity companies in implementing best practices. In the field, CSAs have coordinated with the Environmental Protection Agency on water engagements, the Coast Guard on maritime engagements, the Transportation Security Administration on mass transit engagements, and Treasury on financial service engagements.

Question 9. The National Critical Infrastructure Prioritization Program (NCIPP) identifies a list of Nationally-significant critical infrastructure each year that is used to, among other things, prioritize voluntary vulnerability assessments that will be conducted by PSAs. According to GAO's testimony, as of August 2014, DHS officials reported that they are exploring options to streamline the process and limit the delay of dissemination of the NCIPP list among those who have a need-to-know.

What is the status of efforts to streamline the NCIPP process and limit to delays in disseminating this list?

Answer. The Department (DHS) has streamlined the NCIPP process in a number of ways:

- DHS has eliminated the requirement of States and sectors to re-nominate the same infrastructure every year by automatically approving infrastructure already on the Level 1 and Level 2 List. This has significantly decreased the time and manpower requirements on partners.
- The consequence criteria threshold used for the Level 1 and Level 2 List has remained largely stable for more than 5 years. This stability has allowed partners to better understand how the criteria may be applied to various infrastructure and focus their efforts on those assets, systems, and clusters whose consequences are most likely to reach the established criteria.
- DHS has increased the assistance and outreach provided to State and local partners prior to and during the data call including on specific nominations and guidance on approaches nominators might take to maximize the probability of approval.
- The system used to make nominations for the Level 1 and Level 2 List is available to States and sectors year round enabling partners to work on nomination justifications at their own pace.

DHS continues to work with State and Territorial Homeland Security Advisors, through the PSAs, to make delivery of the completed list as efficient as possible. This includes the increased use of electronic dissemination of the lists through State and Local Fusion Centers. The overall stability of the List has also decreased the time required to finalize and prepare the list for dissemination. The average dissemination time has been reduced by approximately 2 months.

As of August 2014, GAO closed out all recommendations associated with GAO 13–296 *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress.*

Question 10. Background material provided to the committee in preparation for this hearing regarding the PSAs notes that in 2015, the PSAs conducted 949 "Cyber Enhancement" engagements. Can you please go into more detail on what those engagements entail and how do they overlap with or differ from engagement by CSAs?

Answer. The evolving risk landscape associated with cybersecurity highlights the increasingly close connection between cyber and physical systems, including the potential for physical impacts associated with the exploitation of cyber vulnerabilities. For this reason, Protective Security Advisors (PSAs) conduct cyber enhancement events that include the Office of Cybersecurity and Communications. These cybersecurity and resiliency meetings, cyber-related assessments, special event support, and engagements with stakeholders provide opportunities for addressing cyber and physical risks in a holistic and coordinated fashion. As reflected in State Preparedness Reports, cybersecurity continues to be one of the top concerns at the State and local level. PSAs are trained to communicate the Department's cybersecurity services available to stakeholders. In many cases, PSAs and Cyber Security Advisors (CSAs) work together on identifying stakeholder needs.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR MARCUS BROWN

Question 1. Given the focus of some assessments on threats to specific regions, are there any U.S. cities or sector that are examples of best practices in collaborating with and among DHS offices and components and other Federal partners in participating in assessments and taking actions to address vulnerabilities identified?

Answer. There has been extremely good collaboration among Federal agencies (including various DHS elements) in conducting assessments and assisting owners and operators of critical infrastructure, and a good example would be the Greater Philadelphia area. DHS entities such as NPPD, FEMA, Coast Guard, Customs and Border Protection, the U.S. Secret Service, etc. have worked together with the Federal Bureau of Investigation, National Park Service, Health and Human Services, Environmental Protection Agency, Department of Energy, etc. to conduct/participate in assessments of all types. There have been cyber and physical vulnerabilities identified and protective measures implemented in many sectors, including: Commercial Facilities; Energy; Water/Wastewater; Health Care; etc. These protective measures have included: Access control (barriers, CCTV, electronic access control systems, fencing, etc.), security and emergency planning, security management practices, resilience of lifeline dependencies, cybersecurity, and a host of others.

Question 2a. According to the GAO testimony, DHS established a policy in October 2014 to conduct quarterly reviews of programs related to critical infrastructure to better understand the barriers critical infrastructure owners and operators face in improving the security of their assets. What trends has DHS identified in declinations using its tracking system since October 2013?

Has DHS identified barriers that critical infrastructure owners and operators face in making improvements?

Question 2b. If so, what are those barriers?

Answer. We believe that many of the barriers that owners and operators face in making improvements to critical infrastructure are a result of trade-offs that have to be made in a fiscally-constrained environment. Owners and operators in the State have benefitted from the voluntary surveys that DHS conducts on critical infrastructure using the Infrastructure Survey Tool (IST), a web-based vulnerability survey conducted by DHS's Protective Security Advisors (PSAs) to identify and document the overall security and resilience of a facility. Based on information from our local PSA, the resulting survey information is provided to owners and operators through the interactive Dashboards. The Dashboards highlight areas of potential concern and feature options to view the impact of potential enhancements to protection and resilience measures. The written report, developed from the IST data, contains a description of the facility and its vulnerabilities as well as recommendations to mitigate identified vulnerabilities. The PSAs follow-up with the facility approximately 1 year after the Dashboard is provided to better understand the value of the survey and potential enhancements that were made as a result of the survey. Feedback is quantified and analysis conducted on the responses to determine if security and resilience enhancements are being implemented, and if there are impediments to incorporating recommended enhancements. Based on the feedback we have received from the PSA, approximately 90% of facilities are likely to integrate, or have integrated, some of the protective measures detailed in the assessment report. The most

common improvements include enhancements to electronic security systems, security force, and security management. The PSA indicated that barriers for making changes include cost-prohibitive capital investments, lack of project management resources, differing strategic priorities, plans to move or significantly change the facility, and local ordinances.