TESTIMONY

OF

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

And

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

BEFORE
THE

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

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

STAKEHOLDER ENGAGEMENT:
PROTECTIVE SECURITY ADVISORS AND CYBERSECURITY ADVISORS

JULY 12, 2016

I. Introduction

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

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

II. Risk Management

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

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

III. Threat landscape

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

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

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

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

IV. Critical Infrastructure Security and Resilience

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

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

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

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

V. PSA and CSA Value Proposition

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

In existence since 2004, the PSA program is a mature initiative that presently fields 102 regionally-based personnel. The President's FY2017 Budget requests further growth to 119 regionally-based PSAs to meet demand. As field-based representatives, the PSAs work closely with private sector companies and with State Homeland Security Advisers. SLTT stakeholders from every region served by the PSA programs have consistently identified PSAs as a highly valued source of support for their critical infrastructure protection responsibilities. While PSAs focus principally on physical security, they are beginning to provide customers with targeted information based on the existing NPPD portfolio of cybersecurity services to maximize the breadth of outreach for both cyber and physical risk management activities.

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

VI. PSA Program

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

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

1. Conduct Assessments to Foster Risk Management Best Practices

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

The resulting survey information is provided to owners and operators and highlights areas of potential concern, recommendations to mitigate identified vulnerabilities, and options to view the impact of potential enhancements to protection and resilience measures. Over 85 percent of the assessed facilities indicate that they will use the feedback from the PSA to guide their security or resilience enhancements.

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

2. Information Sharing

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

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

An additional example followed the mass shooting at the Emanuel AME church in Charleston, SC on June 17, 2015. Our local PSA offered around 20 security briefings and conducted active shooter briefings for companies, schools, and churches. All briefings were well received and some recipients requested further training. On February 17, the PSA also supported holding a DHS Interfaith Town Hall in Charleston, South Carolina where we brought public and private sector partners together and discussed protective security resources for faith-based and non-profit community stakeholders.

3. Incident Response

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

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

4. Special Events

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

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

5. Risk Mitigation Training

To reduce risk to the Nation’s critical infrastructure, NPPD develops and delivers a diverse curriculum of training to build nationwide counter-improvised explosive device (IED) core capabilities and enhance awareness of terrorist threats. Coordinated by PSAs, the courses educate SLTT participants such as municipal officials and emergency managers, State and local law enforcement and other emergency services, critical infrastructure owners and operators, and security staff on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

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

VII. CSA Program

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

1. Conduct Assessments to Foster Risk Management Best Practices

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

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

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

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

2. Information Sharing

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

3. Incident Response

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

4. Special Events

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

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

VIII. The Way Forward

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

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

1. Way Forward for the PSA Program

i. Three Year Strategic Plan:

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

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

Once completed, this project will guide how the PSA assessment portfolio supports stakeholders across the nation, contributes to a national understanding of risk, and supports national preparedness planning, as well as grants decision making. The CSA program will identify improvements by drawing upon the analysis in this plan and its lessons learned.

ii. Regionalization:

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

2. Way Forward for the CSA Program:

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

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

IX. Closing

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

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