Statement for the Record

Caitlin Durkovich
Assistant Secretary for Infrastructure Protection
National Protection and Programs Directorate

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
Washington, DC

December 17, 2013

Thank you Chairman Carper, Ranking Member Coburn, and the distinguished members of the Committee. I am pleased to appear before the Committee today to discuss the efforts by the Interagency Security Committee to increase security and resilience at our Nation's Federal facilities.

Ensuring the Security and Resilience of Critical Infrastructure

The Office of Infrastructure Protection (IP) works with public and private sector partners to increase the security and resilience of critical infrastructure and protect the individuals relying on that infrastructure. This includes programs to support critical infrastructure owners and operators in enhancing their facilities' security and resilience and coordinating critical infrastructure sectors. These efforts not only prepare our partners for day-to-day activity, but also for large-scale and complex incidents. The National Protection and Programs Directorate (NPPD) builds capabilities among our stakeholders and enhances coordination and planning efforts, so when an incident occurs, our employees and stakeholders are prepared to respond and mitigate future incidents.

IP is also responsible for overall coordination of the Nation's critical infrastructure security and resilience efforts, including development and implementation of the National Infrastructure Protection Plan (NIPP). The NIPP establishes the framework for integrating the Nation's various critical infrastructure security and resilience initiatives into a coordinated effort. The NIPP provides the structure through which the Department of Homeland Security (DHS), in partnership with government and industry, implements programs and activities to protect critical infrastructure, promote national preparedness, and enhance incident response. This plan is regularly updated to capture evolution in the critical infrastructure risk environment and DHS is currently updating the NIPP based on requirements set forth in Presidential Policy Directive (PPD) 21[1].

[1] In February 2013, President Obama issued Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience. PPD-21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. One of the requirements set forth in the policy was for DHS to update the NIPP.

IP conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local, and private sector partners. In addition to helping critical infrastructure owners and operators become more aware of the risks, hazards, and mitigation strategies, we're also helping them measure and compare their levels of security and resilience and identifying methods for how they can improve. Since December 2012, we have conducted more than 900 vulnerability assessments and security surveys on critical infrastructure to identify potential gaps and provide the owners and operators with options to mitigate those gaps and strengthen security and resilience. In addition to serving owners and operators and government officials directly, I serve as Chair of the Interagency Security Committee (ISC) and oversee the development of standards, reports, guidelines, and best practices for civilian Federal facilities through the ISC.

Interagency Security Committee

The mission of the ISC is to safeguard U.S. civilian facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners. The ISC was created following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995—the deadliest domestic-based terrorist attack in U.S. history. Following the attack, Executive Order 12977 created the ISC to address "continuing government-wide security" for Federal facilities in the United States.

ISC standards apply to all civilian Federal facilities in the United States. These include facilities that are Government-owned, leased or managed, to be constructed or modernized, or to be purchased, accounting for more than 399,000 federally owned and leased assets and over 3.35 billion square feet nationwide[2]. The ISC is truly an interagency body exhibiting collaboration and communication among 53 Federal agencies and departments[3]. When agencies cannot solve security-related problems on their own, the ISC brings chief security officers and senior executives together to solve continuing government–wide security concerns. The ISC is responsible for the creation and implementation of numerous standards, guidelines, and best practices for the protection of over 300,000 nonmilitary Federal facilities across the country. This work is based on real-world, present-day conditions and challenges and allows for cost savings by focusing on specific security needs of the agencies.

The ISC is a permanent body with appointed members who often serve multi-year terms. Leadership of the ISC is provided by the Assistant Secretary for Infrastructure Protection, an Executive Director, as well as eight standing subcommittees: Steering, Standards, Technology, Convergence, Training, Countermeasures, Design-Basis Threat, and the Chair Roundtable.

Standards and Best Practices for Secure Facilities

The ISC issues standards, reports, guidelines, and best practices to protect approximately 1.2 million federally owned buildings, structures, land parcels, and more than 2.5 million tenant employees, and millions of visitors each day from harm. The documents developed by the ISC

[2] The Federal Real Property Council's FY 2010 Federal Real Property Report, An Overview of the U.S. Federal Government's Real Property Assets.
[3] Additional information on ISC membership is located in the Appendix.

affect all civilian Federal facilities—regardless of whether they are government-owned, leased, to be constructed, modernized, or purchased.

Examples of ISC Standards and Guidelines:

- ***The Risk Management Process for Federal Facilities Standard-*** Issued August 2013, this ISC Standard defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, single source of physical security countermeasures for all nonmilitary Federal facilities. The Standard also provides guidance for customization of the countermeasures for Federal facilities and encompasses the following documents:

    1. *Facility Security Level Determinations (FSL)* 2008
    2. *Physical Security Criteria for Federal Facilities* 2010
    3. *Design-Basis Threat* 2013
    4. *Facility Security Committees* 2012
    5. *Use of Physical Security Performance Measures* 2009
    6. *Child-Care Centers- Level of Protection Template* 2010

- ***Violence in the Federal Workplace: A Guide for Prevention and Response-*** Issued April 2013, these government-wide procedures for threat assessment, intervention, and response to incidents of workplace violence were developed by the ISC, in conjunction with the Chief Human Capital Officers Council and the National Institutes of Occupational Safety and Health.

- ***Occupant Emergency Programs: An ISC Guide-*** Issued March 2013, this guidance outlines the components of an Occupant Emergency Program, including those items that comprise an emergency plan, and defines the basic guidelines/procedures to be used for establishing and implementing an effective occupant emergency program.

- ***Items Prohibited from Federal Facilities: An ISC Standard-*** Issued February 2013, this standard establishes a guideline process for detailing control of prohibited items into Federal facilities, and identifies responsibilities for denying entry to those individuals who attempt to enter with such items.

- ***Best Practices for Armed Security Officers in Federal Facilities, 2nd Edition-*** Issued February 2013, this best practice document recommends a set of baseline standards to be applied to all contract armed security officers working in Federal facilities.

- ***Security Specialist Competencies: An ISC Guideline-*** Issued January 2012, this document provides the range of core competencies Federal Security Specialists should possess to perform their basic duties and responsibilities.

- ***Best Practices for Mail Screening and Handling-*** Issued September 2011, this joint ISC-Department of Defense Combating Terrorism Technical Support Office/Technical Support Working Group document provides mail center managers, supervisors, and security personnel with a framework for mitigating risks posed by mail and packages.

The scope and focus of these new initiatives may change as the ISC continues its work. The ISC continues to identify new initiatives based on current and emerging threats as well as revise policies which may become outdated. Currently the ISC is working on several new initiatives:

- ***Active Shooter- Prevention and Response:*** Streamlining existing Federal guidance and ISC policy on Active Shooter into one cohesive guidance document that agencies housed in nonmilitary Federal facilities can use as a reference to enhance preparedness for an active shooter incident.

- ***Facility Security Planning:*** Utilizing the ISC's Risk Management Process to develop guidance agencies can use to develop a Facility Security Plan.

- ***Security Office Staffing:*** Establishing criteria and policies which will inform agencies' staffing of Security Offices.

- ***Resource Management:*** Developing guidance to help agencies make the most effective use of resources available for physical security across their portfolio of facilities and examine the use of organizational practices for resource management purposes.

- ***Presidential Policy Directive 21 and Compliance:*** Developing security criteria for critical infrastructure supporting mission-essential functions to account for PPD-21 requirements and to create a strategy for compliance.

- ***Best Practices for Federal Mobile Workplace Security:*** Analyzing the future impact on physical and cyber security policy and practices.

Active Shooter Preparedness

Recent events have demonstrated the need to identify measures that can be taken to reduce the risk of mass casualty shootings, improve preparedness, and expand and strengthen ongoing efforts intended to prevent future incidents. DHS aims to enhance preparedness through a "whole community" approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness, incident response, and workplace violence. Working with partners in the private sector, DHS developed training and other awareness materials to assist owners and operators of critical infrastructure to better train their staff and coordinate with local law enforcement. We have hosted workshops and developed an online training tool targeted at preparing those that work in Federal facilities. These efforts and resources have been well-received and are applicable to Federal facilities as well as commercial spaces and other government buildings.

To date, over 9,700 individuals have viewed DHS's active shooter webinar, over 7,900attendees have participated in over 100 active shooter workshops and exercises nationwide, and over 290,000 Americans have taken DHS's "Active Shooter: What You Can Do" course. Each workshop allows participants to "live" an emergency incident and analyze the situation to work through concerns, actions, and decisions. DHS also launched an active shooter webpage in January 2013, which includes active shooter training resources for Federal, state, and local

partners, as well as the public. Since its launch, the page has been accessed more than 300,000 times.

Cognizant of this threat and need for resources, the ISC formed a Federal Active Shooter Working Group this past spring. While a number of Federal guidance documents[4] previously existed on active shooter preparedness and response, this Working Group was formed to streamline the existing ISC policy into a single cohesive document. To date, the Working Group has met five times and has reviewed numerous publications and guidance documents including training and materials developed by the Department for commercial facilities. It will also leverage lessons learned from real-world incidents, such as the Navy Yard shooting. It is our intention that the resulting work will serve as a resource for agencies to enhance preparedness for an active shooter incident in a Federal facility.

Commitment to Securing Federal Facilities

Threats to our critical infrastructure, including Federal facilities, are wide-ranging. Not only are there terrorist threats, like the bombing at the Boston Marathon this past Spring or the complex shopping mall attack in Kenya, but there are also threats from weather-related events such as Hurricane Sandy, as well as threats to our cyber infrastructure that may have a direct impact on the security of our Federal buildings. While it's impossible to anticipate every threat, the Department is taking a holistic approach to create a more secure and resilient infrastructure environment to better handle these challenges, and the work of the ISC exemplifies these efforts.

The shooting at the Navy Yard on September 16 served as a reminder of the need to ensure our infrastructure is secure and resilient so we can protect our communities, regardless of the threat. We must maintain our partnerships and continue to seek new opportunities to enhance the security and resiliency of our Nation while providing our first responders with the resources and tools they need. Ensuring our Federal facilities are secure and resilient is a large undertaking, but the work of our member departments and agencies ensure those responsible for Federal facility security have the tools and resources necessary to mitigate threats.

In closing, I'd like to thank you for the opportunity to appear before you and discuss the important work of the ISC. I look forward to answering any questions you may have.

[4] The Design-Basis Threat Report; the Violence in the Federal Workplace: A Guide for Prevention and Response; and Occupant Emergency Programs: An Interagency Security Committee Guide.

Appendix—Interagency Security Committee Membership

Membership in the ISC consists of over 100 senior level executives from 53 Federal agencies and departments. In accordance with Executive Order 12977, modified by Executive Order 13286, primary members represent 21 Federal agencies. Associate membership is determined at the discretion of the ISC Steering Committee and the ISC Chair. Currently, associate members represent 32 Federal departments.

Primary Members (21)

1. Assistant to the President for National Security Affairs
2. Central Intelligence Agency
3. Department of Agriculture
4. Department of Commerce
5. Department of Defense
6. Department of Education
7. Department of Energy
8. Department of Health and Human Services
9. Department of Homeland Security
10. Department of Housing and Urban Development
11. Department of the Interior
12. Department of Justice
13. Department of Labor
14. Department of State
15. Department of Transportation
16. Department of the Treasury
17. Department of Veterans Affairs
18. Environmental Protection Agency
19. General Services Administration
20. Office of Management and Budget
21. U.S. Marshals Service

Associate Members (32)

1. Commodity Futures Trading Commission
2. Court Services and Offender Supervision Agency
3. Federal Aviation Administration
4. Federal Bureau of Investigation
5. Federal Communications Commission
6. Federal Deposit Insurance Corporation
7. Federal Emergency Management Agency
8. Federal Protective Service
9. Federal Reserve Board
10. Federal Trade Commission
11. Government Accountability Office
12. Internal Revenue Service
13. National Aeronautics & Space Administration
14. National Archives & Records Administration
15. National Capital Planning Commission
16. National Institute of Building Sciences
17. National Institute of Standards & Technology
18. National Labor Relations Board
19. National Science Foundation
20. Nuclear Regulatory Commission
21. Office of the Director of International Intelligence
22. Office of Personnel Management
23. Office of the U.S. Trade Representative
24. Securities and Exchange Commission
25. Smithsonian Institution
26. Social Security Administration
27. U.S. Army Corps of Engineers
28. U.S. Capitol Police
29. U.S. Coast Guard
30. U.S. Courts
31. U.S. Institute of Peace
32. U.S. Postal Service