

**Statement for the Record**

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

**Leonard E. Patterson**  
**Director**  
**Federal Protective Service**  
**National Protection and Programs Directorate**  
**Department of Homeland Security**

**Before the**  
**United States House of Representatives**  
**Committee on Homeland Security**  
**Subcommittee on Oversight and Management Efficiency**  
**Washington, DC**

**October 30, 2013**

Thank you Chairman Duncan, Ranking Member Barber, and the distinguished members of the Subcommittee. We are pleased to appear before the Committee today to discuss the efforts by the National Protection and Programs Directorate (NPPD) to increase security and resilience at our nation's federal facilities. The men and women serving in NPPD have wide-ranging responsibilities, from serving on the front lines of law enforcement to developing standards with stakeholders to conducting training nationwide. NPPD works with owners and operators, public safety, and countless others daily to keep the nation secure. These efforts prepare our partners for steady state and day-to-day activity, but also for large-scale and complex incidents. 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.

In addition to working with public and private sector partners to enhancing security across the sectors, NPPD provides daily protection at Federal facilities through the Federal Protective Service (FPS), protecting more than 1.4 million tenants and visitors in the facilities, on the grounds, and on property owned, occupied, or secured by the Federal Government. Across the country FPS provides law enforcement and security management services, which include operations and oversight of approximately 12,000 contract Protective Security Officers (PSO), and security countermeasure services for more than 9,000 General Services Administration-owned, -leased or -operated facilities located across the country and other Federal facilities.

**Ensuring the Security and Resilience of Critical Infrastructure**

Within NPPD, 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 infrastructure. This includes programs to support critical infrastructure owners and operators in enhancing their facilities' security and resilience and coordinating critical infrastructure sectors.

IP is 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. The NIPP 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<sup>1</sup>.

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 how they can improve. In the last year, we 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, IP supports the development of standards, reports, guidelines, and best practices for civilian federal facilities through the Interagency Security Committee (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 attack on U.S. soil before September 11, 2001 and the worst 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

---

<sup>1</sup> 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.

billion square feet nationwide<sup>2</sup>. The ISC is truly an interagency body exhibiting collaboration and communication between 53 Federal agencies and departments<sup>3</sup>. 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. Several have represented their organizations for more than a decade. 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.

FPS is an active participant in the work of the ISC, helping shape standards, guidance and best practices that enable FPS employees to perform their protection mission with consistency and efficiency. FPS sits on the ISC Steering Committee, chairs the Training Subcommittee, and has representatives on a number of other ISC committees and working groups, including the Design Basis Threat group, the Countermeasures subcommittee and others. FPS chaired the working group that authored a “Best Practices for Federal Mobile Workplace Security” document in 2013 that is currently under review, and is also on the Active Shooter-Prevention and Response as well as the PPD-21 and Compliance working groups that are currently meeting. In recent years, FPS has also co-chaired the working groups that produced the *Items Prohibited from Federal Facilities: An ISC Standard and Best Practices for Armed Security officers in Federal Facilities, 2nd Edition* documents. FPS also serves as the Sector Specific Agency for the Government Facilities Sector. In this role FPS is responsible for working with various partners—including other federal agencies; state, local, tribal, and territorial governments as well as other sectors—to develop and implement the government facilities sector-specific plan.

### ***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, and land parcels more than 2.5 million tenant employees, and millions of visitors each day from harm. The documents developed by the ISC affect all civilian federal facilities—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

---

<sup>2</sup> The Federal Real Property Council’s FY 2010 Federal Real Property Report, An Overview of the U.S. Federal Government’s Real Property Assets.

<sup>3</sup> Additional information on ISC membership is located in the Appendix.

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. <i>Facility Security Level Determinations (FSL)</i>	2008
2. <i>Physical Security Criteria for Federal Facilities</i>	2010
3. <i>Design Basis Threat</i>	2013
4. <i>Facility Security Committees</i>	2012
5. <i>Use of Physical Security Performance Measures</i>	2009
6. <i>Child-Care Centers- Level of Protection Template</i>	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, 2<sup>nd</sup> Edition-*** Issued February 2013, this best practice recommends a set of minimum 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 (CTTSO/TSWG) document provides mail center managers, supervisors, and security personnel with a framework for mitigating risks posed by mail and packages.

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 non-military Federal facilities can use as a reference to enhance preparedness for an active shooter incident.
- ***Facility Security Plan:*** 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.

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, but threats from weather-related events, such as Hurricane Sandy, as well as threats to our cyber infrastructure which may have a direct impact on the security of our federal buildings. While it’s impossible to anticipate every threat, NPPD is taking a holistic approach to create a more resilient infrastructure environment to better handle these challenges, and the work of the ISC exemplifies these efforts. Ensuring our Federal facilities are secure and resilient is a large challenge, but by providing our partners with standards and best practices, law enforcement agencies serving at Federal facilities every day, like the Federal Protective Service, have the tools and resources necessary to mitigate threats.

### ***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.

FPS has developed an Active Shooter Tenant Awareness training program and has provided this training to more than 3,300 Federal facility tenants so they may be better equipped to analyze a potential situation and work through concerns, actions, and decisions. In addition, more than

1,000 FPS law enforcement officers and agents have been trained in “Active Shooter Response Tactics.” To date, over 9,700 individuals have viewed DHS’s active shooter webinar, over 7,300 attendees have participated in over 100 active shooter workshops and exercises nationwide, and over 263,400 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 258,000 times. In addition to the training FPS provides to tenants, FPS’s PSOs receive instruction regarding actions to take in special situations, such as a building fire, a report of an active shooter or workplace violence, and other emergency situations or evacuations.

## **Ensuring the Security and Resilience of Federal Facilities**

In the United States government facilities remain a potential target of attacks. The NPPD FPS mission is to protect Federal facilities and their occupants and visitors by providing superior law enforcement and protective security services, leveraging the intelligence and information resources of its network of Federal, state, local, tribal, territorial, and private sector partners. To accomplish our mission and help prevent incidents like the Navy Yard tragedy from occurring at FPS-protected Federal facilities, our inspectors and PSOs work in tandem to attend to daily security needs at Federal facilities, assess individual federal facilities’ vulnerabilities to both natural and man-made events, and effectively respond to security-related activities and threats directed against the facilities or the government personnel working within them.

In performing the mission of protecting Federal facilities and persons thereon, we rely on our law enforcement and security authorities found at 40 U.S.C. § 1315; our ability to enter into agreements with state, local and tribal law enforcement agencies for purposes of protecting Federal property; the enforcement of Federal Management Regulation sections pertinent to conduct on Federal property under 41 C.F.R., Part 102-74 Subpart C; and our responsibility as a recognized “first responder” for all crimes and suspicious circumstances occurring at GSA owned or leased property.

## **FPS Operations**

FPS contracted PSOs are the eyes and ears of our organization. PSOs are responsible for controlling access to federal facilities, conducting screening at access points to federal facilities, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to emergency situations involving facility safety and security. PSOs also ensure prohibited items, such as firearms, explosives, knives, and drugs, do not enter federal facilities. In fact, FPS PSOs stop approximately 700,000 prohibited items from entering federal facilities annually.

### ***Suitability***

All PSOs must undergo preliminary background investigation checks to determine their fitness to begin work on behalf of the government. At FPS, preliminary checks consist of a review of the applicant’s background investigation questionnaire form as well as automated record checks with

the FBI, National Crime Information Center, credit reporting bureaus, and naturalization/citizenship checks, when applicable. If derogatory information cannot be mitigated to allow for a favorable preliminary decision, the background investigation must be completed and favorably adjudicated prior to “Entry On Duty” approval. For PSOs serving in Federal facilities requiring a high-level security clearance, DHS uses the Defense Security Service to adjudicate background investigations.

### ***Training***

FPS partners with private sector guard companies to ensure that PSOs are prepared to accomplish their duties. FPS works with the guard companies to ensure the guards have met the certification, training, and qualification requirements specified in the contracts, covering subject areas such as ethics, crime scene protection, actions to take in special situations such as building evacuations, safety and fire prevention, and public relations. Courses are taught by FPS, by the contract guard company, or by a qualified third party such as the American Red Cross for CPR. PSOs also receive instruction in areas such as X-Ray and magnetometer equipment, firearms training and qualification, baton qualification, and First-Aid certification. PSOs are required to attend refresher training and they must recertify in weapons qualifications in accordance with federal and state regulations.

The FPS training team is working closely with industry and Federal partners in an effort to further standardize the PSO training screening station related training. For example, our trainers work with the U.S. Marshals Service and Transportation Security Administration trainers to incorporate best practices into the base X-Ray, Magnetometer and Hand Held Metal Detector training. Additionally, FPS is working closely with the National Association of Security Companies to develop a National Lesson Plan for PSOs that will establish a basic and national training program for all PSOs; this is important to ensure standards are consistent across the nation. These efforts will further standardize training PSOs receive and will provide for a great capability to validate training and facilitate rapid adjustments to training to account for changes in threat and technological advancements.

### ***Oversight***

FPS is committed to ensuring high performance of its contracted PSO workforce. FPS Law Enforcement personnel conduct PSO post inspections and integrated covert test activities to monitor vendor compliance and countermeasure effectiveness. Additionally, vendor files are audited periodically to validate that PSO certifications and training records reflect compliance with contract requirements. In Fiscal Year 2013, FPS conducted 54,830 PSO post inspections and 17,500 PSO personnel file audits.

In addition, and in accordance with procurement regulation and policy, contract deficiencies and performance issues are documented in the annual Contractor Performance Assessment Report. FPS Headquarters and regional leadership are provided with regular reports to maintain visibility on the status of these important assessments that are also used by Agency source selection officials in the procurement process when awarding new PSO contracts.

As members of the Committee may be aware, the GAO has, in the past, raised some concerns regarding FPS's handling of PSO training and oversight. FPS has taken significant steps to improve oversight of PSO contracts. For example, FPS is currently hiring 39 additional Contracting Officer Representatives in order to improve oversight of vendor contract compliance. FPS has also drafted and implemented an enhanced policy for FPS PSO performance monitoring, security force management, and contractor management functions. Among other improvements, this standardizes nationally the methods and frequencies of PSO post inspections and audits of contractor files.

Due in part to these actions, FPS has made significant progress toward closing GAO and OIG recommendations pertaining to oversight. Since 2011, FPS has successfully closed thirteen GAO and four OIG recommendations and has submitted closure documentation for nine additional recommendations. Of these, two were successfully closed and seven are pending GAO's internal review for closure.

### **Law Enforcement Personnel**

FPS also directly employs over 1,000 federal Law Enforcement Personnel who are trained physical security experts. Law Enforcement Personnel perform a variety of critical functions, including conducting comprehensive security assessments of vulnerabilities at facilities, developing and implementing protective countermeasures, and providing uniformed police response and investigative follow-up. As previously noted, Law Enforcement Personnel also conduct PSO guard post inspections on a daily basis as well as Operation Shield activities, which involve deployments of a highly visible array of law enforcement personnel to validate and augment the effectiveness of FPS countermeasures across the protective inventory<sup>4</sup>.

### ***Facility Security Assessments***

One of the most important responsibilities of FPS Law Enforcement Personnel is conducting Facility Security Assessments (FSAs) at FPS-protected facilities nationwide. FSAs document security related risks to a facility and provide a record of countermeasure recommendations. The process analyzes potential threats toward a facility through a variety of research sources and information. Upon identification of the threats, the process identifies and analyzes vulnerabilities to a particular facility utilizing Protective Measure Indices (PMI). Assessors utilize the Modified Infrastructure Survey Tool (MIST) to document the existing protective posture at a facility and compares how a facility is, or is not, meeting the baseline level of protection for its FSL as set forth in the ISC's Physical Security Criteria for Federal Facilities standard and the ISC's Design Basis Threat report. MIST also compares the disparities identified against the baseline level of protection specified in the ISC standards, thereby operationalizing those standards, and enabling mitigation of the vulnerabilities identified. The FSA report is a

---

<sup>4</sup> This includes providing highly visible law enforcement presence to disrupt terrorist/criminal activity, expand patrol and response operations through increased coverage, demonstrate FPS's commitment to employing the highest standards for the security of Federal facilities and the safety of their occupants; and collect and assimilate data to continually assess and improve FPS's ability to achieve its core mission – to secure facilities and safeguard occupants.

historical record and informative report provided to FPS stakeholders to support their decision making in risk mitigation strategies.

FSA's require collaboration between FPS private sector stakeholders and government stakeholders. Collaboration between these entities is critical to successful implementation of a risk management framework. FPS partners with all of the stakeholders to identify and gather all necessary information for characterizing the risks to each unique facility. FSA is accomplished on a recurring schedule broken down by FSL.

### ***Law Enforcement Response***

FPS officers respond to tens of thousands of calls for service annually, some of which entail responding to criminal activity in progress, others to protect life and property, and still others to respond to national security events or to support other law-enforcement responding to a critical situation, as was the case in the Navy Yard complex on September 16, 2013. In this case, FPS responded to the on-scene Navy Yard Unified Command center in a supporting role and deployed six K9 Explosive Detection Dog teams to be staged at the Navy Yard and sweep the Nationals Park parking lot in response to mutual-aid calls from the District of Columbia Metropolitan Police Department and the FBI. Additionally, given the proximity of the FPS-protected US Department of Transportation (DOT) building to the Navy Yard complex, FPS deployed to the DOT building, coordinated a Shelter in Place for all occupants, established a secure perimeter around the building, conducted K9 sweeps around the perimeter, and increased uniformed patrol activities at other FPS-protected Federal facilities located within the southeast corridor of the District of Columbia.

### **Commitment to Securing Federal Facilities**

In closing, we would like to acknowledge and thank our partners in both the public and private sector, especially members of the law enforcement community who responded the day of the Navy Yard shooting. We are grateful for their continued service. The shooting at the Navy Yard on September 16 provided 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.

DHS is committed to ensuring our Federal facilities remain safe and secure for employees and visitors. Our employees will continue serving on the front lines at Federal facilities and working behind the scenes to develop standards and supporting law enforcement efforts. Thank you again for the opportunity to testify before this committee. We look forward to answering any questions you may have.

## 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