

**Statement for the Record  
Testimony  
of  
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 Cybersecurity, Infrastructure Protection, and Security  
Technologies  
Washington, DC**

**July 24, 2012**

Thank you Chairman Lungren, Ranking Member Clarke, and the distinguished members of the Subcommittee. My name is Eric Patterson, and I am the Director of the Federal Protective Service (FPS) within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD).

I am honored to appear before you today to discuss NPPD/FPS's progress in utilizing key protection and risk management practices such as allocation of resources, leveraging technology, and enhancing information sharing and coordination.

The GAO has raised several areas that have historically represented challenges for FPS including:

1. Absence of a risk management program;
2. Addressing key human capital issues through a strategic human capital plan;
3. Contract Guard workforce management and oversight; and
4. Need for a review of FPS's fee design

Today's hearing is an opportunity to address the progress FPS has made during the past year in working to address these challenges, and to also provide information on the topics addressed in GAO's new report related to risk assessment and Protective Security Officer (PSO) program management and oversight.

**FPS Background**

FPS's mission is to protect more than 9,000 Federal buildings and the 1.4 million Federal employees and visitors who occupy them throughout the country every day by leveraging the intelligence and information resources of its network of public and private sector partners. Specifically, FPS executes its mission by providing proactive law enforcement, investigation and protective intelligence and information sharing services, incident response, security planning, and stakeholder engagement. Prior to its transfer to NPPD

in 2009, FPS was organized under Immigration and Customs Enforcement and prior to that, under the General Services Administration (GSA).

Part of our core mission is to assess the threat picture for the Government Facilities Sector (GFS) and share that information with stakeholders as appropriate. For example, FPS leverages the Homeland Security Information Network (HSIN), a secure, trusted web-based portal to share information with our more than 900 government and industry partners. One of the recent information-sharing initiatives FPS has implemented to assist in the protection of facilities and their occupants is the Federal Facility Threat Picture (FFTP), which is an unclassified assessment of the current known threats to the facilities FPS protects. Produced quarterly, the FFTP supports the threat component of a Federal Security Assessments (FSA) and informs our stakeholders of potential threats to government facilities. The FFTP focuses on the threats posed by a variety of actors that may seek to attack or exploit elements of the GFS. The information used in the FFTP comes from intelligence and law enforcement community reporting.

During Fiscal Year (FY) 2011, FPS:

- Investigated and mitigated more than 1,300 threats and assaults directed towards Federal facilities and their occupants;
- Disseminated 331 threat and intelligence-based products to our stakeholders, 142 of which were FPS-produced;
- Conducted 81,125 post inspections;
- Interdicted more than 680,000 weapons/prohibited items including knives, brass knuckles, pepper spray, and other items that could be used as weapons or are contraband such as illegal drugs, at Federal facility entrances during routine checks;
- Made 1,975 arrests;
- Responded to 53,000 incidents involving people or property; and
- Conducted more than 1,800 high-visibility operations under Operation Shield and 150 risk-based Covert Test operations, ensuring the protection of Federal buildings and infrastructure.

### **FPS Is Developing a Risk Management Program**

In terms of a risk management program, FPS's operational activities are organized by the National Infrastructure Protection Plan's (NIPP) Risk Management Framework, which calls for the following steps: Set Security Goals, Identify Assets and Functions, Assess Risks, Prioritize, Implement Protective Programs, and Measure Effectiveness. One area of recent significant progress related to risk assessment and the implementation of a risk management program is the ongoing implementation of FPS's solution for conducting FSAs using an automated assessment tool. In May 2011, the decision was made to cease development of the legacy application known as the Risk Assessment and Management Program (RAMP) and to pursue a standalone assessment tool, in order to provide completed FSAs to customers. That decision has since been affirmed by the Department's Office of Inspector General (OIG).

In the interim period, our employees have continued their daily interactions with tenant agencies and oversight of facility security. Our personnel have been completing Pre-Modified Infrastructure Survey Tool (MIST) worksheets to enable complete FSA reports, and are constantly assessing risks to Federal facilities. Specifically, the pre-MIST worksheet allows the inspector to collect key information that will be populated into MIST and used in generating a final FSA report. Such data includes facility information, vulnerability assessments, and existing protective measures.

After consideration of several alternatives, FPS partnered with NPPD's Office of Infrastructure Protection (IP) to leverage a proven assessment methodology called the Infrastructure Survey Tool (IST). In October 2011, NPPD issued a task order to Argonne National Laboratory (ANL) through the Department of Energy to modify the existing Link Encrypted Network System (LENS) and IST for FPS use to conduct FSAs. Because this project leveraged existing tools and had limited resources and time constraints, the acquisition lifecycle was tailored to meet delivery deadlines.

I am pleased to note that in its draft report, GAO noted FPS's use of project management principles in the development of MIST. Throughout the project, the MIST Users Working Group has remained engaged to ensure user involvement in the process. User feedback from field testing was uniformly positive about MIST and the FPS Gateway, confirming suitability to support the FPS mission. The MIST and FPS Gateway development efforts were completed on schedule, with ANL delivering the system to the Government on March 30, 2012. In April 2012, the decision was made to proceed and deploy MIST. It is important to note that throughout the development and testing of MIST, field employees and our union were involved and actively participated as subject matter experts in the process.

FPS developed and is currently implementing a distance learning-based training program for each MIST user, as GAO commended in its draft report. Supervisors completed this training in April 2012 and Inspectors began their virtual training in May 2012, with completion of all training anticipated for late September 2012. This provides a hands-on learning environment for our inspectors; they will receive virtual instruction as they use the tool in the learning environment. Once an Inspector completes the training and successfully briefs his or her supervisor on a completed FSA, that Inspector will be able to proceed with conducting FSAs and reporting the results to a Facility Security Committee.

In leveraging existing technology in developing MIST, FPS was able to incorporate the ability to illustrate the impact of alternative countermeasures on a particular vulnerability. MIST will also show how a facility is or is not meeting the baseline level of protection for its Facility Security Level as set forth in the ISC's Physical Security Criteria for Federal Facilities standard and the ISC's Design Basis Threat report. This will lead to a more informed and better dialogue with tenants and Facility Security committees as FSA results are discussed and alternatives are explored. Additionally, FPS recently disseminated guidance nationwide on the commencement of the use of MIST to generate FSAs upon completion of inspector training. The anticipated results of the use of MIST

are consistent assessment results nationwide and informed decision-making regarding security investments on the part of tenant agencies.

### **FPS is Addressing Key Human Capital Issues through Development of a Strategic Human Capital Plan**

In order to ensure that human resource requirements are aligned appropriately with FPS's overall mission, a Strategic Human Capital Plan is being developed in conjunction with NPPD's Human Capital Office. We are working to finalize the document; we intend to provide the plan and brief the Committee when it is finalized.

### **FPS is Working to Improve Its Protective Security Officer Management and Oversight**

FPS is working to improve management and oversight of our over 13,000 Protective Security Officer (PSO) force. We have reviewed our operations nationwide and have taken steps at the national program level to ensure that performances under contracts are advantageous to the Government. We are actively working to implement the recommendations resulting from GAO and OIG reviews across the organization. Additionally, an Integrated Project Team (IPT) conducted a comprehensive review of how FPS resources the PSO oversight function and our current oversight policy.

FPS is also working with DHS's Science and Technology Directorate to develop a system for contract guard oversight and explore means of leveraging technology to ensure effective oversight of PSOs, such as automated tracking of guard post staff levels and PSO possession of the necessary credentials to stand post. Additionally, our training team is working closely with industry and Federal partners in developing a more effective training strategy for our PSOs.

### **FPS is Examining Its Fee Structure in order to Review Current Fee Design**

FPS operates through fee-based funding revenue, which is calculated based on the Federal-facility tenant's square footage of occupancy and on the collection of services associated with the provisioning of reimbursable protective countermeasures. This fee-based financial structure is unique among Federal law-enforcement agencies and requires a greater degree of understanding internal operations to ensure it is properly aligned with FPS's costs.

To address this challenge, FPS is implementing a two-pronged strategy to better understand its activities and costs and recommend options for a new revenue structure. In January 2012, FPS collaborated with the Department's Systems Engineering and Design Institute (SEDI), a Federally Funded Research and Development Center managed by the DHS Science and Technology Directorate, to produce a full mapping of FPS activities and then align them with costs. That work will be used to produce Activity-Based Cost (ABC) models for FPS. Both of these efforts are designed to result in a more

efficient revenue structure for FPS and greater transparency in security costs for FPS stakeholders.

### **Conclusion**

Thank you again for the opportunity to provide you with an update on the progress FPS is making on a number of fronts. FPS aspires to be an exemplary law enforcement and strategic critical-infrastructure protection organization. This is a vision uniformly shared by FPS leadership and operational staff, both at headquarters and in the field. I would be happy to answer any questions you might have.