Testimony of Stephen Amitay, Esq.
Executive Director and General Counsel

National Association of Security Companies (NASCO)

Before the

Senate Homeland Security and Government Affairs Committee

Hearing on

"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"

December 17, 2013

Testimony of Stephen Amitay, Esq.
Executive Director and General Counsel
National Association of Security Companies (NASCO)
Before the
Senate Homeland Security and Government Affairs Committee
Hearing on
"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"
December 17, 2013

Introduction

The Washington Navy Yard attack raised important issues and challenges related to federal facility security, access control, and personnel background screening. Unfortunately, the Navy Yard attack followed several other shootings at federally protected facilities over the past five years.[1] With such "active shooter" incidents on the rise, federal agencies responsible for federal facility security and their contract security partners who provide security personnel for those facilities must work together to address current federal facility security issues and develop new efficient and effective strategies to reduce the risks of such incidents as well as other threats.

Federal executive branch agencies are responsible for protecting over 370,000 non-military buildings and structures.[2] The Department of Homeland Security's (DHS) Federal Protective Service (FPS) is the primary agency responsible for providing law enforcement and related security services for the approximately 9,600 federal facilities under the control and custody of the General Services Administration (GSA). FPS has about 1,200 full-time employees and about 13,500 contract "Protective Security Officers" (PSO's) deployed at thousands of federal facilities (generally Federal Security Level III and IV facilities) of GSA's 9,600 facilities.[3] The remainder of the federal buildings and structures are protected by some three dozen other federal executive branch agencies. Not including the military services, there are approximately 35,000 private security officers working for various federal agencies.[4]

[1] 2009 Holocaust Museum, 2009 Fort Hood, 2010 Pentagon, 2010 Las Vegas Courthouse, 2012 Long Beach Federal Building, 2012 Birmingham Courthouse, 2013 Wheeling (WV) Federal Building.

[2] GAO:FACILITY SECURITY: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies GAO-13-222, Jan 24, 2013 Page http://www.gao.gov/assets/660/651529.pdf

[3] GAO: FEDERAL PROTECTIVE SERVICE: Challenges with Oversight of Contract Guard Program Still Exist, and Additional Management Controls Are Needed GAO-13-694, Sep 17, 2013 http://www.gao.gov/assets/660/657920.pdf This report claims "FPS has about 1,200 full-time employees and about 13,500 contract security guards deployed at approximately 5,650 (generally level III and IV facilities) of GSA's 9,600 facilities." As to which facilities actually have PSO's onsite, a 2011 GAO Report stated that "FPS provides security personnel to about 2,360 (GSA) facilities…" GAO: FEDERAL FACILITY SECURITY: Staffing Approaches Used by Selected Agencies GAO-11-601 June 2011. http://www.gao.gov/assets/330/320625.pdf

[4] The largest amount of contract security officers work for FPS (approx. 13,500), the United States Marshal Service (approx. 5,000), and the Department of Energy (approx. 5,000). Other federal agencies/instrumentalities that use contact security include: IRS, NASA, FAA, USDA, DOT, DOC, HHS, SSA, NARA, DOL, FDIC, US Coast Guard, State, DIA,

NASCO is the nation's largest contract security trade association, whose member companies employ more than 300,000 security officers across the nation servicing commercial and governmental clients. NASCO member companies and companies in affiliated NASCO "Government Security Contractors Caucus" provide security officers to numerous federal agencies for the protection of federal facilities including the majority of FPS PSO's. Since 2007, NASCO has been working with FPS, as well as Congress and the GAO, to address issues related to the "Protective Service Officer Program (PSOP)" (formerly known as the "Contract Guard Program"). Many of the issues and challenges identified with the PSOP have been laid out in various GAO Reports.

To further ensure the protection of federal facilities and their occupants and visitors, FPS and its security contractors need to continue to work together to make improvements related to training, oversight, recordkeeping, PSO instructions and post orders, and there also needs to be improvement in the lines of communication between FPS headquarters, the regional officials, contract officers, federal tenants, and contractors. FPS is well aware of these issues and there is no doubt that there has been substantial progress being made to address them.

Since the appointment of Director Patterson in 2010, who in turn brought on an Assistant Director for Training, the degree of dialogue and breadth cooperation between FPS and security contractors has been unparalleled. While things might not be moving as fast as GAO and security contractors would like, FPS' commitment to improving the PSO Program at FPS is unquestionable and this commitment is evidenced by its work, often in close partnership with contractors, on numerous activities and initiatives. Currently, NASCO and FPS are working together on a host of issues related to PSO training that will improve the content and delivery of PSO training, standardize PSO training, as well as increase the capability to validate that training. Better and smarter trained PSO's mean better and smarter security at federal facilities. PSO's. Additionally, in the field there have been improvements, driven from headquarters, which have brought greater standardization in the contract process and the treatment of security contractors and PSO's. Much still needs to be done, and can be done, but FPS's management of its contract security force has come a very long way in the past decade. NASCO looks forward to continuing to work closely with Director Patterson and FPS to improve federal facility security through the cost-effective use of contract security officers.

<u>Overview of FPS Activities to Improve the Protective Security Officer Program (PSOP)</u>

Below are highlight of current activities and improvement being made related to the PSOP

In the critically important area of providing x-ray and magnetometer training for PSO's, a deficiency GAO has highlighted on numerous occasions, FPS, working with NASCO, is about to launch a pilot program that will train and certify security contractor instructors so that they can provide the training instead of requiring that PSO's be trained by stretched thin FPS personnel. As GAO has noted, this current situation has resulted in PSO's never receiving the training. And with FPS increasing the PSO screener training to

NRC, Holocaust Museum, and Smithsonian. Private screening companies/personnel are also being utilized successfully at various airports around the United States under the TSA Screening Partnership Program.

16 hours (with an annual 8 hour refresher), the need for its security contractors to be conducting this training is acute.

FPS is also moving to increase "active shooter" training for PSO's. Since the Navy Yard attack, FPS has provided security contractors with new "active shooter instructions" to distribute to PSO's and add to all post orders, and also there will be a new chapter on active shooter in the upcoming revision of the Security Guard Information Manual (SGIM). Nevertheless, it seems clear that actual "active shooter" training is also needed and FPS is also now in the beginning phases of developing such training. We look forward to working with FPS on developing this active shooter training, which is expected to be provided by the security contractors.

While these above FPS training initiatives essentially represent FPS "coming up to speed" with what some other federal agencies that use contract security officers are already doing, these are significant steps in the right direction that will increase training efficiency and effectiveness and lead to better security being provided at federal facilities.

In another training initiative, FPS is working with NASCO and security contractors to revise and standardize the PSO training lesson plans as well working to improve the firearms training and qualifications for PSO's.

FPS also is reaching out to other federal agencies, to see how they are training and managing their contract security officers, and importantly, they are including FPS security contractors in this outreach. Later this month, through an agreement between FPS and DoE, DoE will allow FPS and a group of FPS security contractors attend a DoE "simulated active shooter scenario" that DoE is providing for its contract security officers. The goal is to continue to increase active shooter awareness and response procedures, and share best practices between DoE and FPS on active shooter reaction and response procedures.

FPS is also (finally) coming out with a much needed revision of the "Security Guard Information Manual" (SGIM), the PSO bible. The SGIM governs and instructs PSO's on how to act and not following the SGIM is considered a contract violation. Unfortunately, the degree of contractor input into this revision process was minimal, and certain long-standing issues such as instructions related to a PSO's authority to act (and potentially liability for acting) in extreme situations may not be adequately addressed. However, FPS officials have said that the new version of the SGIM (now called the Security Manual and Resource Tool "SMART" book) will be a version control document that is founded on a quality management process that will allow for incorporating improvements and updates more easily.

FPS is also conducting a comprehensive review of PSO Post Orders and looking to standardize and update them. NASCO commends this effort as many current post orders are fairly nebulous and vague. However, new post orders, in addition to being standardized, need to be facility specific and tailored to the specific post.[5]

[5] For instance, in some facilities there will be a "duress button" that sets off an alarm; however, there is nothing in the post orders about what to do upon setting off the alarm. Post orders should also have information on the closest fire alarm, and other location/post specific information.

In the area of security contractor oversight and the verification of PSO training and certifications (an often raised issue by GAO) in many instances the issue is not that a PSO did not receive one of the 24 required PSO trainings and certifications, but instead it is an issue of poor recordkeeping/file inspections and conflicting interpretations of contract requirements. To address this problem, FPS has revised its Contractor Officer Representative (COR) training and is bringing on board 39 dedicated Contracting Officer Representatives. This new COR cadre will not be spread thin doing other FPS duties as many current FPS inspectors doing COR duties are now. This should result in better FPS oversight of contract compliance, quicker resolution of contract issues, and more efficient data management.

I will return to these PSOP related issues later in my testimony after discussing some of the bigger picture threat and risk mitigation issues related to physical security at federal facilities.

Federal Employee and Contractor Personnel Screening and Access Control

As to the issue of federal employee and contractor security clearance screening that played a prominent role in the Navy Yard attack, this is an area where NASCO and it members are not involved. It is encouraging though that even before the attack, a major government-wide reform effort, initiated by DNI and OPM was underway to revise federal investigative standards so that they will incorporate the concept of "continuous evaluation" which will allow for information such as a recent arrest or conviction anywhere to become available on a timely basis for background screening officials. Also, the Administration's recent "Insider Threat" initiative seeks to complement the continuous evaluation concept by incorporating data from a broad set of data sources to identify problematic behavioral trends. [6] Without a doubt, improvements must be made to the security screening process so that someone like Navy Yard shooter, who after he received his security clearance was arrested several times and was also reported to the Navy as being mentally unstable, will have his access authority revoked.

As to access control at federal facilities, PSO's and other contract security officers at federal facilities are very involved in this process. (Both at the Navy Yard and the Holocaust Museum contract security officers at access control points were killed in those attacks). However, contract security companies, while they do have expertise in setting appropriate access control policies, do not generally have a say in the access control policies at federal facilities. One obvious access control policy solution related to the Navy Yard attack would be to require all federal employees and contractors to be subject to screening at federal facilities or at least implement random screening of employees and contractors.

Federal Facility Security Elements and the Interagency Security Committee

Federal facility security threats include terrorist attacks, active shooters, workplace violence, anti-government protests, unauthorized access, theft, and there is no doubt that protecting federal facilities and their occupants and visitors is an ongoing challenge for federal agencies. Federal facility threat

[6]Testimony of Mr. Greg Marshall, Chief Security Officer, U.S. Department of Homeland Security, before the House CHS Subcommittee on Oversight and Management Efficiency, Hearing: "Facility Protection: Implications of the Navy Yard Shooting on Homeland Security." October 30, 2013.
http://homeland.house.gov/sites/homeland.house.gov/files/documents/Testimony-Marshall.pdf

mitigation involves conducting facility security assessments (FSA's) and setting/re-setting facility security levels, devising and recommending countermeasures to mitigate risks, considering and adopting countermeasures, and then implementing countermeasures. The conduct of federal facility security assessments and the process for the consideration and adoption of security countermeasures are "governed" by Standards promulgated by the Federal Interagency Security Committee (ISC). Created by Executive Order after the Oklahoma City bombing, the ISC's mandate is "to enhance the quality and effectiveness of physical security in, and the protection of buildings and nonmilitary Federal facilities in the United States. The ISC standards apply to all nonmilitary Federal facilities in the United States - whether government-owned, leased or managed; to be constructed or modernized; or to be purchased."[7]

Earlier this year, the ISC came out with the "Risk Management Process: An Interagency Security Committee Standard." The Standard creates one formalized process for defining the criteria and process that should be used in determining the Facility Security Level of a Federal facility, determining risks in Federal facilities, identifying a desired level of protection, identifying when the desired level of protection is not achievable, developing alternatives, and risk acceptance, when necessary. The Standard provides an integrated, single source of physical security countermeasures for all non-military Federal facilities and guidance for countermeasure customization for Federal facilities.[8]

The Standard incorporates and supersedes numerous previous ISC Standards related to federal facility security and not only provides an introduction to the risk management process but also outlines the approach necessary to identify, assess, and prioritize the risks to Federal facilities.

As the Standard notes, consistent with Executive Order 12977, it is "intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities." [9] In fact, EO 12977 states that "Each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order" and the Order, as amended, gives DHS the responsibility to monitor federal agency compliance with ISC Standards. [10]

However, often throughout the risk management assessment process and in the process of considering and adopting suitable countermeasures, the requirements of the ISC Standards are not met.

Earlier this year, GAO released report titled Report "Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies."[11] In the Report, GAO noted that ISC Standards "are developed based on the collective knowledge and physical security expertise of ISC member agencies

[7] http://www.dhs.gov/interagency-security-committee

[8] "The Risk Management Process: An Interagency Security Committee Standard" August 2013, First Edition. http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf

[9] ISC RM Standard, page iii

[10] Executive Order 12977 of October 19, 1995. Federal Register Vol. 60, No. 205 Tuesday, October 24, 1995 http://www.gpo.gov/fdsys/pkg/FR-1995-10-24/pdf/95-26497.pdf

[11] GAO Facility Security Report January 2013. (See footnote 2).

and, therefore, reflect leading practices in physical security." More so, "the (u)se of ISC standards may be beneficial because they provide agencies with tools and approaches for consistently and cost-effectively establishing a baseline level of protection at all facilities commensurate with identified risks at those facilities. By using the standards to determine the level of protection needed to address the unique risks faced at each facility, agencies may be able to avoid expending resources on countermeasures that are not needed."

It seems very clear that ISC Standards provide effective guidance for all aspects of facility security.

However, in a survey of 32 federal agencies, GAO found that "the extent of agencies' use of ISC standards varied—with some agencies using them in a limited way." In this vein, at a House hearing last month on federal facility security, GAO testified that "our ongoing review of nine federal agencies' risk assessment methodologies indicate that several agencies, including FPS, do not use a methodology that aligns with ISC's risk assessment standards to assess federal facilities. (As a result) these agencies may not have a complete understanding of the risks facing…federal facilities. [12]

The GAO Report further found that "agencies' reasons for making limited use of ISC standards reflect a lack of understanding by some agencies regarding how the standards are intended to be used."

The Report acknowledges though that there are other sources for developing physical security programs for federal facilities in addition to ISC Standards, most notably, an agency's institutional knowledge or subject matter expertise in physical security. Agencies also turn to non-governmental experts, including private security companies, to establish their physical security plans. [13] Finally, agencies also are guided by federal statutes and regulations, state or local regulations and agency/facility specific information such as mission and the type, use, and location of their facilities.

Thus, while some agencies may not be putting facility security at risk by limiting their use of ISC Standards; nonetheless, the pervasive non-compliance with ISC Standards by federal agencies responsible for federal facility protection, whether intentional or as a result of a "lack of understanding" the standards, is not a good situation.

In one example of ISC standard non-compliance, an FPS security contractor encountered a situation where upon taking over a contract for the security/access control at a federal building was informed by the tenant agency that in order to maintain a "free and open culture" the agency had a "security" policy of

---

[12] Testimony of Mark Goldstein, Director of Physical Infrastructure Issues, before the House CHS Subcommittee on Oversight and Management Efficiency, Hearing: "Facility Protection: Implications of the Navy Yard Shooting on Homeland Security." October 30, 2013.
http://homeland.house.gov/sites/homeland.house.gov/files/documents/Testimony-Goldstein.pdf

[13] GAO Facility Security Report January 2013. One official told GAO that "his agency contracts with a security company that has extensive knowledge and experience in providing security and law enforcement to high profile institutions across the federal government, and that this knowledge is used in managing the agency's security program." Page 8.

not screening anyone coming into the building --- in clear non-compliance with ISC standards. The security contractor reported this situation to FPS and FPS then persuaded the tenant to implement some screening. Other security contractors too have seen instances of agencies ignoring ISC standards or not being aware of them. As will be discussed later, the central role of federal facility tenants in approving security policies for federal facilities has clearly been identified as a facility security concern.

Unfortunately, due to staff and resource limitations, the ISC does not formally monitor agencies' compliance with ISC standards. The ISC does hold regular meetings and has working groups where information is shared about agency compliance, but, as GAO reports, "this approach does not provide a thorough or systematic assessment of ISC member agencies' use of the standards, and provides no information on non-member agencies' physical security practices." [14]

The GAO recommended that the ISC "conduct outreach to all executive branch agencies to clarify how the standards can be used in concert with agencies' existing physical security programs." Also recommended, "To help agencies make the most effective use of resources available for physical security across their portfolios of facilities, develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standards." ISC has stated in its 2012 to 2017 action plan that it plans to establish protocols and processes for monitoring and testing compliance with its standards by fiscal year 2014.

Greater education on, use of, and compliance with ISC Standards by federal agencies/tenants should lead to more effective and efficient federal facility security. ISC should work to implement the recommendations of GAO and DHS should devote more resources to the ISC for educational and compliance efforts.

Federal Facility Security Assessments

As mentioned above, GAO has found that several agencies, including FPS, do not use a methodology to assess risk at their facilities that aligns with the Interagency Security Committee's (ISC) risk assessment standards, and as a result, "FPS and the other non-compliant agencies GAO reviewed may not have a complete understanding of the risks facing approximately 57,000 federal facilities located around the country (including the 9,600 protected by FPS)." Risk assessments (facility security assessments) are the foundation upon which an effective facility security policy is built and FPS needs to improve its FSA capabilities in both efficacy (and compliance with ISC Standards) as well as being able to do FSA's in a timely fashion. Several years ago FPS attempted to develop a comprehensive risk assessment tool (RAMP) that failed and set FPS back in the FSA arena. The current FPS risk assessment tool (MIST) in addition to not being aligned with ISC standards also has other limitations according to GAO.

In addition, in a recurring theme at FPS, the persons who are responsible for doing FSA's (FPS inspectors) are also doing law enforcement and investigative related work, acting as contracting officer representatives (COR's), providing screener and orientation training to PSO's, conducting PSO firearm qualification and doing other duties. They are spread thin, and this can further hamper the ability of FPS

[14] Ibid. page 12.

to conduct quality FSA's in a timely manner. As FPS is now doing with the creation of a much needed dedicated COR force, it might consider creating a dedicated FSA force, but such a force would need better training, tools and quality control management. As to better tools, FPS should look to the private sector and other agencies to find an effective risk assessment tool instead of trying to develop one. There are commercial off the shelf risk assessment tools available. In addition, FPS could free up Inspectors and increase the amount of FSA's completed by outsourcing FSA's to companies that have experts who specialize in such work and are currently doing FSA's for nuclear facilities, critical infrastructure, and high risk commercial buildings.

Federal Facility Security Committees

A critical player in prioritizing and mitigating threats to federal facilities is the "Facility Security Committee (FSC)." As explained in the ISC Risk Management Process Standard, the FSC consists of representatives of all Federal tenants in the facility, the security organization (Federal Protective Service for General Services Administration (GSA) owned and operated facilities), and the owning or leasing department or Agency. The FSC is responsible for determining the Facility Security Level for the facility, addressing the facility-specific security issues addressed in the facility security assessment and approving the implementation of security countermeasures and practices recommended by the security organization.[15] These are very serious facility security responsibilities.

In GSA owned/leased building, FPS is responsible for doing the FSA and then recommending (and explaining) the appropriate countermeasures to the FSC. However, it is clear that "the decision to implement those recommendations and mitigate the risk or to accept risk as part of a risk management strategy is that of the FSC."[16]

In past GAO Reports, and in contractor dealings with FSC's and tenant agencies, there have been serious issues as to whether FSC's are making "informed risk-based decision regarding the mitigation or the acceptance of risk" as required by the ISC Risk Management Process Standard. In a 2010 GAO Report, GAO noted something that FPS and security contractors have experienced first-hand at federal facilities; "tenant agency representatives to the FSC generally do not have any security knowledge or experience but are expected to make security decisions for their respective agencies." [17]

Security contractors working at federal facilities have observed that often at FSC meetings the lead agency will call the shots and ignore FPS recommendations. Tenant representatives do not want to be there, are disinterested and therefore FSC meetings are also not well attended. In addition, for some FSC's there is a greater interest in providing "customer service" than building security. [18]

While GAO also opined that tenant representatives on the FSC may not be getting adequate information from FPS (and some observers believe that FPS needs to do a "better sales job" with the FSC's);

[15] ISC RM Process Standard.
[16] ISC RM Process Standard. 6.0 "The Risk Informed Decision Making Process"
[17] GAO: HOMELAND SECURITY "Addressing Weaknesses with Facility Security Committees Would Enhance Protection of Federal Facilities" GAO 10-901 August 2010 http://www.gao.gov/new.items/d10901.pdf
[18] At some federal building PSO's are not allowed to "hand check" employee ID's when necessary.

nonetheless, the bottom line is that security decisions for federal facilities are often being made by persons with no education or training in risk mitigations and security. Also, with shrinking agency budgets combined with the fact that "many of the FSC tenant agency representatives do not have the authority to commit their respective organizations to fund security countermeasures"[19] it is becoming increasingly more likely that recommended and necessary security countermeasures are being voted down solely because of cost concerns.

Whether it be for a lack of understanding of the risks or a lack of a funding commitment, both of these scenarios are a prescription for increasing risks at federal facilities. There are though solutions to the above described FSC problems.

Last Congress, this Committee passed a bill (endorsed by NASCO), which introduced by former Chairman Lieberman and former Ranking Member Collins, that addressed both the FSC member lack of training/education issue as well as the refusal of an FSC (for whatever reason) to implement recommended countermeasures issue. In S.772, `Supporting Employee Competency and Updating Readiness Enhancements for Facilities Act of 2012' (SECURE Act) there was a provision that said that if the DHS Secretary in coordination with the ISC, "determines a Federal facility (protected by FPS) to be in noncompliance with Federal security standards established by the Interagency Security Committee or a final determination regarding countermeasures" and the facility loses an appeal and still does not implement the countermeasure, then "The Secretary may assess security charges to an agency that is the owner or the tenant of (the) Federal facility… for the costs of necessary security countermeasures."[20]

Also in the SECURE Act, there is a provision that requires that "before serving as a member of a Facility Security Committee, an employee shall successfully complete a training course that meets a minimum standard of training as established by the Interagency Security Committee" that is "commensurate with the security level of the facility." [21]

In the new ISC Risk Management Standard, there is too an FSC education requirement. "Federal employees selected to be members of a Federal FSC will be required to successfully complete a training course that meets the minimum standard of training established by the ISC." However, with no way to monitor/enforce compliance it is likely the percentage of current FSC members at federal facilities who have taken required training courses is small.

Congress should work with DHS, who chairs the ISC, FPS and all federal agencies to make sure that FSC members are taking the required training. The safety of the employees and visitors in federal facilities also needs to be funding priority. FPS will need to work harder with it federal clients to identify and

[19] Ibid.

[20] S. 772 ''Supporting Employee Competency and Updating Readiness Enhancements for 4 Facilities Act of 2012'' http://thomas.loc.gov/cgi-bin/query/z?c112:S.772.RS:/ SEC. 247. COMPLIANCE OF FEDERAL FACILITIES WITH FEDERAL SECURITY STANDARDS.

[21] S. 772 SECURE Act of 2012, SEC. 264. FACILITY SECURITY COMMITTEES (c) "Training for Members"

implement the most cost-effective countermeasure appropriate for mitigating vulnerability, but in the end, necessary security should never fall victim to budget cuts.

Effective Countermeasures: The Use of Protective Security Officers

In thousands of GSA facilities a primary security countermeasure is the deployment of contract PSO's through the FPS Protective Security Officer Program (formerly the "Contract Guard Program."). In other facilities, lesser security countermeasures, such as cameras and perimeter lighting, may be deployed to mitigate risk at these facilities.

PSO's are the most visible component of the FPS' operations, and they are the "eyes and ears" of the FPS mission. As part of their assigned duties, PSO's are expected to; control access to specific areas of a facility (access control includes checking visitor and employee identification; operating security equipment such as x-ray machines and Magnetometers to screen for prohibited materials;) enforce property rules and regulations; detect and report criminal acts; stop and if possible, detain persons engaging in criminal activities; provide security against loss from fire or mechanical equipment failure; respond to emergency situations involving the safety and security of the facility; and act occasionally as a crowd monitor to maintain order.[22] PSO's are specifically "authorized to detain people if it is necessary to ensure order and safety at (the) assigned facility."[23]

FPS PSOP Security Related Issues and Initiatives

As mentioned in the introduction, since 2007, NASCO and its members have worked with FPS on issues related to the FPS PSOP. Below are some of the current initiatives and issues which relate to the performance and capabilities of PSO's to provide security at federal facilities.

Active Shooter

On the subject of active shooter response, there are two issues. One is training and the other is authority to act. As to training, as mentioned, while other agencies are already providing active shooter training to its contract security officers, the current FPS "training" is light to non-existent.[24] Active shooter may come up in passing during a 2 hour segment of the 8 hour FPS provided orientation training, and some contractors provide their PSO's with active shooter resources, but FPS needs to do more for the PSO's on active shooter, and the agency is aware of this fact.

FPS recently provided PSO's with "Active Shooter Instructions" that are now part of their post orders and FPS has said that there will be additional PSO instruction on active shooter in the revised Security Guard Information Manual (now the SMART Book). FPS is also developing actual active shooter training for

[22] Federal Protective Service • "Security Guard Information Manual", 2008 Revision Chapter 2.1 "Your Roles and Responsibilities."

[23] FPS SGIM, Chapter 3.6 "Detainment Authority"

[24] DoE, State, Commerce, Holocaust Museum, NASA, Pentagon Force Protection Agency, IMF and World Bank all provide active shooter training for contract security officers. See Sept. 2013 GAO Report (footnote 2).

PSO's which could be incorporated into or added to the contractor provided portion of PSO training. Given the difficulties that FPS has with providing the mandated screener training to PSO's, and FPS' pilot program to have the screener training done by the security contractors, it is unimaginable that FPS would take on the active shooter training responsibility. FPS is reviewing the active shooter training other federal agencies are providing to contract security officers, and FPS is including its security contractors in that review process. NASCO hopes that FPS will also work with security contractors to develop an appropriate and effective active shooter training course for PSO's. This could involve contractor instructors getting trained and certified by FPS/FLETC to provide active shooter training to PSO's (as will happen in the screener training pilot program). Any active shooter training should be building specific, scenario specific, incorporate actual drills on a regular basis after the initial training, and consider if there are armed federal employees in the facility (i.e. DEA, FBI, DHS, ICE or other armed federal agents).

Authority to Act and Arrest Authority

An issue that is often raised in situations in federal facilities where violence, weapons, or the potential for violence is present is the ability/authority of PSO's to act, and the related legal issue of what constitutes "detaining" an individual, and what constitutes "arresting" an individual. PSO's are often put in situations where a person will enter a federal facility and starts acting strange or violent or potentially violent, or the person might have a weapon. In some instances, PSO's have detained individuals (including handcuffing them) and then later been sued for false arrest. Under FPS regulations, all PSO's must be licensed by the state where they are posted a federal facilities. As all PSO's are armed, this would require getting an armed officer license in that state. In some states, such as Virginia, licensed armed officers are given state statutory authority to arrest people that are committing crimes on the property where they work. With such arrest authority, a PSO can more confidently and assuredly detain a violent person at a federal facility and not worry about a false arrest charge. However, under FPS rules for PSO's (contained in the SGIM) it says that "even if you are deputized under current or past employment endeavors, you do not have arrest authority while performing on an FPS contract." [25] A violation of the SGIM is a violation of the contract.

Also as to what constitutes permissible detainment by a PSO is also very vague. The SGIM states that "as an FPS security guard you are authorized to detain people if it is necessary to ensure order and safety at your assigned facility. You should detain a person only when absolutely necessary and with the minimum level of force necessary to control the situation." It then goes on to say that "You should be aware that using an 'unreasonable level of force' to detain a person could result in a civil lawsuit filed against you. An 'unreasonable level of force' is defined as the level of force that is not appropriate to control a situation." [26] This is quite confusing and could condition a PSO to err on the side of not acting until things get out of control. Since all PSO's are required to carry handcuffs, be armed, have pepper spray and a baton, what are FPS' expectations as to how a PSO should and can act in a violent situation?

Even in an "active shooter" situation, FPS instructions as to what a PSO can do if there is an active shooter in the facility -- but not in the PSO's line of sight --are confusing. For other agencies such as DoE, the policy

[25] FPS SGIM, Chapter 3.2 Common Offenses.

[26] FPS SGIM Chapter 3.6 Detainment Authority

is essentially not to let the threat continue. In some remote FPS protected facilities, it could be a long time before law enforcement arrives. PSO's should not be restrained by confusing and conflicting FPS policies and fear of lawsuits and contract violations when faced with a dangerous or potentially dangerous situation. [27] In situations such as active shooter, FPS needs to instill in security contractors and PSO's a sense that if the PSO engages, the FPS will support their efforts. FPS has stated that the new SGIM (SMART Book) is a "version control document" that can be reviewed and revised more easily, it is likely the instructions for active shooter scenarios and detaining individuals are areas that security contractors and FPS will need to work on.

Another possible strategy for dealing with active shooter and violent/criminal situations is for DHS to authorize PSO's to make arrests. Other federal agencies, such as Department of Energy, under federal statutory authority, authorize their contract security officers to make arrests for certain crimes committed in their presence or if they reasonably believe such a crime was committed. [28] The Homeland Security Act provides for similar arrest authority to be given to employees of DHS "to make arrests without a warrant for any offense against the United States committed in the presence of the officer or agent or for any felony cognizable under the laws of the United States if the officer or agent has reasonable grounds to believe that the person to be arrested has committed or is committing a felony."[29] This section could be amended by Congress to provide such authority to PSO's. If PSO's were given arrest authority (and expected to use it) additional training would be required. However, providing PSO's with arrest authority --- or at the very least not restricting PSO's from exercising arrest authority they may have under some state statutes --- could lead to faster containment of dangerous situations at federal facilities.

Screener Training

The problems that FPS has had with providing PSO's with initial X-ray and Magnetometer training are well documented and FPS is still struggling to get all PSO's the required training. At the same time FPS is transitioning to a new 16 hour initial PSO training and adding an 8 hour annual refresher training. FPS has had to train its personnel to provide this new training and while some contractors are now receiving the new 8 hour refresher training, the 16 hour initial training is still lagging. As mentioned frequently, one solution to address the lack of FPS training resources is to turn over the training to the security

[27] For instance, PSO's are sometimes required to pat down individuals and if something is found the individual is asked to remove it. However, in cases where the individual refuses, there is no guidance. Also, FPS officials in the field are giving PSO's detention instructions that differ from what is in the SGIM.

[28] For DoE, arrest authority is provided to contract security officers under 10 CFR 1047 - LIMITED ARREST AUTHORITY AND USE OF FORCE BY PROTECTIVE FORCE OFFICERS. Arrest is defined as any act, including taking, seizing or detaining of a person, that indicates an intention to take a person into custody and that subjects the person to the control of the person making the arrest. http://www.gpo.gov/fdsys/pkg/CFR-2012-title10-vol4/pdf/CFR-2012-title10-vol4-part1047.pdf The U.S. Marshall Services, deputizes its Court Security Officers giving them full law enforcement authority. http://www.usmarshals.gov/duties/ However, CSO's are required to have a law enforcement background or law enforcement training (but this can be a double edged sword).

[29] 40 U.S.C. § 1315 : US Code - Section 1315: Law enforcement authority of Secretary of Homeland Security for protection of public property http://codes.lp.findlaw.com/uscode/40/I/13/1315#sthash.saToUhla.dpuf

contractors who are already supplying around 90% of all PSO training. Security contractors have dedicated trainers while FPS trainers are those same FPS inspectors doing FSA's, acting as COR's, doing patrols, etc.). Security contractor provided will be both more effective and efficient. Delaying PSO's from being able to assume a post because they are waiting on FPS training is not good for anyone, and permitting PSO's to assume posts without the training is a potential safety threat. FPS understands these arguments and has been working with NASCO to initiate a pilot program that will have security contractor instructors be given the training to teach PSO's the screener training. Currently four contracts are being modified to fund this security contractor instructor training and the subsequent 16 hour PSO screener training. In addition, training will be provided to PSO supervisors on the contracts for better quality control. This pilot should get underway early next year. While it has been a long time coming, it represents a sea change in FPS' attitudes toward training and is a milestone in FPS and contractor relations.

When the more expensive 16 hour training does become available, FPS should not unduly restrict the number of the PSO's that can receive the training (and thus be assigned to a screening post) in order to recoup the added costs of the training. FPS must realize that PSO's are often rotated (in some cases as a requirement of the FPS contract) and PSO's doing screening need to be regularly relieved to prevent "going blind" from looking at the x-ray machine too long. There are other situations and reasons why more PSO's will need screening. However, while FPS should not set a number or criterion that will lead to a lack of necessary trained PSO's, at the same time, it would be problematic for FPS to just leave it up to contract bidders to provide FPS with a number of PSO's in their bid that they think need to be given the training for the contract requirements. Based on experience, it is highly unlikely that FPS bid evaluators have the expertise and knowledge of the facilities/hours/rotational requirement/and other factors that are necessary to determine what is the necessary/sufficient amount of PSO's that need to be trained to effectively and safely satisfy the contract requirement. If FPS just leaves it to the bidders, this could lead to FPS selecting a bid that because of an insufficient amount of screening training costs included in the bid, the bid is given an elevated evaluation based on this screener trainer price differential.

Standardized Training and Certified Trainers

FPS is also working on an initiative with NASCO to review, revise and standardize the PSO Training (Lesson Plans) in a new and better format. FPS contractors through NASCO have provided FPS with various contractor PSO training lesson plans and FPS is pulling "best practices" from the plans and "cross walking" them against the new SMART Book at the ISC Armed Security Officer Standard. FPS will then work internally and with contractor to develop a draft national lesson plan for review. The lesson plan though needs to be able to incorporate training for new and developing threats and could have elements that are performance based instead of time based.

FPS also needs to consider ways to improve refresher training. At FPS a PSO's initial training (132 hours) never expires and the refresher training requirement is currently 40 hours every three years. Other agencies provide more initial training and provide substantially more refresher training. FPS needs more refresher training (perhaps 24 hours annually) and should consider at least one annual scenario drill run on site during off hours. These active drills, similar to force on force training currently executed at DoE sites nationally, keep the skills already provided to the contract security personnel fresh and allow for

better and safer weapons handling skills. These additional hours of refresher training and active drills will allow PSO's to learn from and immediately be adjusted for any minor corrections in tactics or technique that will then be perfected for use during a time of emergency such as an active shooter situation.

On a related issue, NASCO fully supports FPS certifying security contractor instructors to provide all the PSO training (not just the screener training as will be done via the pilot program and some of the current certifications). The 2013 ISC "Best Practices for Armed Security Officers in Federal Facilities" recommends that certified trainers provide most of the training for armed security officers (including PSO's). [30] Already numerous state governments "certify" private trainers to provide the required security officer training (firearms, handcuff, baton, "pepper spray") that they require for security officers to obtain state licenses and certifications. Also other federal agencies such as NASA and DoE require security officer instructors to be certified. This would provide for greater confidence in and consistency of PSO training. In its September Report, GAO recommended that FPS security contractor instructors "be certified to teach basic and refresher training courses to guards and evaluate whether a standardized instructor certification process should be implemented."[31] FPS concurred and it envisions using a standardized lesson plan being taught by certified instructors. NASCO stands ready to work with FPS to reach this vision in a timely manner.

PSO Drills and Testing

An important part of keeping a security workforce sharp to conduct regular drills and scenario testing. FPS, through its Operation Shield, conducts penetration tests at federal facilities that test PSO's ability to detect prohibited items. Often, FPS will provide remedial on the spot training during these exercises. However, a persistent problem related to these tests is that FPS is unwilling or does not in a timely fashion, share the results of the Operation Shield exercises with the security contractors. This makes it difficult to determine which PSO's were posted at the time, the conditions, and other information that can be helpful to the security contractor to take corrective and remedial action.

FPS security contractors too have the ability to perform their own penetration exercises of PSO's which are very productive. In these cases, with prior notice to the Government, a company can test a PSO's ability to identify weapons or contraband being introduced to the facility. While Operation Shield exercises by FPS are excellent testing tools, PSO's need to use their skills or they will degrade and FPS testing them in the field infrequently is less valuable than allowing the company to test them more frequently. FPS security contractors conduct such drills with their security officers at other federal agencies and such drills are encouraged by those agencies. However, FPS is inconsistent on allowing security contractor drills and the policies vary by region to region, COR to COR. There does seem to be valid arguments against allowing, under set FPS parameter, security contractors to conduct drills on their PSO's and NASCO supports FPS revisions on this policy to allow for more security contractor drills.

[30] Chapter 6.4 Providing Armed Security Officer Training. "All training, whether required or as a refresher, should be done with a certified trainer and/or training organization for: Defensive Tactics, Empty Hand Control Techniques, Firearms (Initial and Requalification Training), Handcuffing Techniques Intermediate Weapons/Compliance, and Use of Force."
ISC Best Practices for Armed Security Officers 2013

[31] See Footnote 3.

Information Sharing and Coordination with Local Law Enforcement

There can be better sharing of threat and risk information between FPS and security contractors. FPS does not share FSA's with contractors providing security for that facility. As to threat information, while FPS has considered utilizing the Homeland Security Information Network (HSIN) to provide alerts, bulletins and critical information to contractors on a timely basis, this has not produced much in terms of effective threat information sharing. Most information that is shared with contractors such as BOLO's and wanted notices, do not make it down to the PSO level. Additionally, FPS also does involve security contractors in the identification and prioritization of threats, thereby losing their potentially valuable input and preventing valuable information from being distributed to PSO's in the field.

Further, FPS Law Enforcement Personnel do not train with the PSOs and do not typically invite local LE to participate in training. Therefore, when a large scale incident or emergency event such as an active shooting does occur, it is unclear how anyone will react. Responsible parties have not discussed action plans in advance and drilled with all the appropriate security/law enforcement stakeholders who would necessarily respond. This leads to confusion during an incident, the worst possible time to have a breakdown in communications. The simple solution is to have more and better communications between the contract security providers and their federal/local law enforcement colleagues.

With less than 1000 FPS law enforcement personnel and thousands of buildings to protect, it is very important that FPS has good coordination with local law enforcement authorities who may be called by PSO to a respond to an incident at a federal facility, and FPS should also include the security contractor in this coordination.

Federalization of Security Officers is Not the Answer

Some have suggested that the solution to improving PSO performance and providing better security at federal facilities is to "federalize" the majority of FPS PSO's (who are stationed at Level III and Level IV facilities). This notion is not only cost-prohibitive but also completely lacking in performance based support for this notion. In response to a question at a hearing before this Committee on FPS in 2009, then FPS Director Gary Shenkel estimated that on an annualized cost basis (thus not including retirement benefits) federalizing FPS security officers would increase costs by about 35% or an extra $400M per year.[32] In terms of performance, a 2011 GAO Report that looked at federal agency use of federal security officers and contract security officers found no differences in performance (but found that using federal officers was more expensive and provided less personnel flexibility and more difficulty in disciplining non-performing officers). [33] Finally, one can look at the current performance problems of the federalized TSA screener force (and performance comparisons done with non-federalized airport screeners) and it abundantly clear that the "federalization" is not the prescription for better screening performance. What is clear though about "federalization" is that it would greatly increase the costs to FPS.

[32] Hearing before the Senate HSGAC "The Federal Protective Service: Time for Reform" April 19, 2009.
[33] GAO: FEDERAL FACILITY SECURITY: Staffing Approaches Used by Selected Agencies GAO-11-601 June 2011. http://www.gao.gov/assets/330/320625.pdf

Conclusion

Federal facility security is a multi-layered operation involving common standards as well as unique requirements. In order to increase the level of security provided at federal facilities in a cost-effective manner, Federal agencies and their security providers like FPS, need to work better and smarter together in assessing risks, discussing risks and countermeasures, and then implementing countermeasures. One important countermeasure is the use of contract security officers. Contract security officers are the front line forces in the protection of federal facilities and they often bear the initial brunt and/or provide the initial reaction to an active shooter incident. In the 2009 Holocaust shooting, upon entering the Museum the shooter shot and killed a contract security officer but then the shooter was shot and disabled by another contract security officer. There is no doubt that well trained contract security officers can be an important part of any facility security plan. FPS, as the largest supplier of contract security to the federal government, is definitely making progress in improving this element of the security service it provides to federal agencies. There continue to be issues with the Protective Security Officer Program, but under the direction of Director Patterson, working with his contract security partners, FPS is actively addressing these issues. Importantly, every element of the Program is subject to potential review and revision if necessary. New ways are being found to provide better training, including working with other agencies, and FPS' oversight and review processes are being reformed to provide for better quality management. All of these efforts will increase the performance and effectiveness of the FPS contract security force.

Some of the needed changes and improvements to the PSOP (such as more training) or the need to deploy more PSO's at a facility will likely require additional funding and FPS must explain to its federal clients why these increases are necessary but in the final federal facility security equation, federal tenants must not be allowed assume unreasonable risk because of budget concerns or because of a lack of understanding.

Background on NASCO and Private Security

NASCO is the nation's largest contract security trade association, whose member companies employ more than 300,000 security officers across the nation who are servicing commercial and governmental clients, including providing security officers to numerous federal agencies for the protection of federal facilities. NASCO also has a "Government Security Contractors Caucus" that includes non-NASCO members and focuses on federal security contracting programs, such as FPS. Formed in 1972, NASCO strives to increase awareness and understanding among policy-makers, consumers, the media and the general public of the important role of private security in safeguarding persons and property. At the same time, NASCO has been the leading advocate for raising standards for the licensing of private security firms and the registration, screening and training of security officers, and NASCO has worked with legislators and officials at every level of government to put in place higher standards for companies and officers.

At the federal level, NASCO was the driving force behind the 2004 passage of the Private Security Officers Employment Authorization Act (PSOEAA), which authorized all employers of private security officers to request FBI criminal background checks on their officers, and NASCO is continuing to work to establish an effective and comprehensive PSOEAA check process. Of more relevance to today's hearing, as mentioned in the introduction, since 2007 NASCO has worked closely with both the House and the Senate Homeland Security Committees (appearing at three House hearing), the Federal Protective Service (FPS) and the Government Accountability Office (GAO) on issues and legislation related to FPS.

Nearly 2 million people are employed in private security domestically compared to fewer than 700,000 public law enforcement personnel. Approximately 75 percent of private security personnel work for contract security companies, with the balance serving as proprietary or "in-house" security. The vast majority of contract security firms employ many former law enforcement and military personnel in management and as security officers. Private security officers are often the "first" responder on the scene of a security or terrorism-related incident providing crucial support to public law enforcement. In addition, with increasing fiscal pressure on governmental entities, private security is increasingly relied upon to fill the gaps resulting from law enforcement funding cutbacks.