FPS Technical Countermeasures for Federal Facilities

December 21, 2020

Fiscal Year 2019 Report to Congress

Homeland Security

Federal Protective Service

Message from the Office of the Under Secretary for Management

December 21, 2020

I am pleased to submit the following report, "FPS Countermeasures for Federal Facilities," which has been prepared by the U.S. Department of Homeland Security's (DHS) Federal Protective Service (FPS).

This document has been compiled pursuant to language in the Fiscal Year 2019 DHS Appropriations Act (P.L. 116-6) and its accompanying Joint Explanatory Statement. The report provides several options for a revised method to assess and allocate costs for facility countermeasures under FPS's 40 U.S. Code 1315 authority.

Pursuant to congressional requirements, this report is being provided to the following members of Congress:

The Honorable Nita M. Lowey
Chairwoman, House Appropriations Committee

The Honorable Kay Granger
Ranking Member, House Appropriations Committee

The Honorable Richard Shelby
Chairman, Senate Appropriations Committee

The Honorable Patrick Leahy
Ranking Member, Senate Appropriations Committee

Inquiries relating to this report may be directed to me at (202) 447-3400.

Sincerely,

RANDOLPH D ALLES
Digitally signed by RANDOLPH D ALLES
Date: 2020.12.18 15:12:17 -05'00'

R.D. Alles
Deputy Under Secretary for Management

FPS Technical Countermeasures for Federal Facilities

Table of Contents

I. Legislative Requirement

This report was compiled in response to language set forth in the Fiscal Year (FY) 2019 Department of Homeland Security (DHS) Appropriations Act (P.L. 116-6) and its accompanying Joint Explanatory Statement.

P.L. 116-6 states:

> SEC. 301. Not later than 180 days after the date of enactment of this Act, the Federal Protective Service, in conjunction with the Office of Management and Budget, shall provide a report to the Committees on Appropriations of the Senate and the House of Representatives providing no fewer than three options for a revised method to assess and allocate costs for countermeasures.

The Joint Explanatory Statement states:

> A new revenue model study completed by the Administration and FPS, which proposed a method to more accurately assign security costs to users, is currently scheduled for implementation in fiscal year 2020. A provision is included requiring FPS to evaluate alternative approaches and methods to fund "Countermeasures" security costs and provide a report to the Committees on its conclusions not later than 180 days after the date of enactment of this Act. These approaches and methods should demonstrate efficiency, focusing on innovative countermeasures which are planned for in advance, and solutions that take into consideration a federal agency's own investments in security.
>
> Section 301. The conference agreement includes a provision requiring the Federal Protective Service, in conjunction with the Office of Management and Budget, to provide a report to the conferees providing no fewer than three options for a revised method to assess and allocate costs for countermeasures.

FPS developed this report in coordination with the Office of Management and Budget (OMB) to provide three alternative approaches for funding technical countermeasure projects across the portfolio of federal properties.

II. Background

Effective October 2019, DHS transferred the operation and administrative control of the Federal Protective Service (FPS) to the DHS Under Secretary for Management.

FPS is responsible for the protection of federal facilities through its statutory authority in 40 U.S. Code § 1315. FPS provides protective services to approximately 9,000 properties throughout the United States and its territories. The inventory constantly is changing as tenants move, leases expire, and the composition of the real property portfolio changes. The facilities that FPS protects either are owned or leased by the U.S. Government. The majority of the real property that FPS protects is owned, operated, or leased through/by the U.S. General Services Administration (GSA). The GSA Public Building Service (PBS) leases most of the portfolio from private commercial real estate companies. The remainder of the real property is owned and operated by the Federal Government through PBS or through individual federal agencies that have their own real property authority.

FPS is a full-cost recovery operation funded through security fees categorized as basic, building-specific, and customer agency-specific security. Title 41 of the Code of Federal Regulations (C.F.R.) § 102–85.35 provides the following guidance in relation to funding received from FPS customers:

> (a) A basic security fee is assessed in all PBS-controlled properties where the Federal Protective Service (FPS) provides security services. The rate is set annually on a per-square-foot basis.[1] The charge includes the following services:
>
> (1) General law enforcement on PBS-controlled property;
> (2) Physical security assessments;
> (3) Crime prevention and awareness training;
> (4) Advice and assistance to building security committees;
> (5) Intelligence sharing program;
> (6) Criminal investigation;
> (7) Assistance and coordination in Occupancy Emergency Plan development;
> (8) Coordination of mobilization and response to terrorist threat or civil disturbance;
> (9) Program administration for security guard contracts; and
> (10) Megacenter operations for monitoring building perimeter alarms and for dispatching appropriate law enforcement response.

[1] FPS, with approval from OMB, recently implemented a new method for assessing fees for basic security services, taking effect in FY 2020. The new method is service- and risk-based rather than the previous charge per square foot and a set percentage for oversight of countermeasures. FPS is working with GSA to amend 41 C.F.R. § 102–85.35 to reflect the new fee assessment method.

> (b) The building-specific security charge comprises two elements: Operating expenses and any legacy amortized capital costs on previous projects.[2] Building-specific charges, whether operating expenses or capital costs, are distributed to overall federal users by building or facility in direct proportion to each customer agency's percentage of federal occupancy. As with joint use charges, the distribution of building-specific charges among customer agencies is not re-adjusted for vacancy.

The GSA *Pricing Desk Guide, 5th Edition* (GSA Pricing Guide), which applies to all federal agencies occupying GSA-owned or -leased space, provides additional information into basic, building-specific, and agency-specific security fees. Section 2.9.1 of the GSA Pricing Guide addresses basic security services. It states that:

> The basic security charge is developed by FPS and approved by OMB. As outlined in the MOA [memorandum of agreement],[3] basic security includes the following:
>
> - Law enforcement – patrol and response, criminal investigations
> - Megacenter operations – security alarm monitoring and dispatch
> - Facility security assessments – identification of risks and countermeasures
> - Security consultation – new construction, major repair and alteration projects, leasing
> - FSC [Facility Security Committee] participation
> - Security assistance – occupant emergency plans and continuity of operations planning

Section 2.9.2 of the GSA Pricing Guide addresses the building-specific security services. It states that these services are building-specific countermeasures, including contract guards, security equipment, and security fixtures that mitigate security vulnerability.

Section 2.9.3 of the GSA Pricing Guide addresses customer agency-specific security fees. Agency-specific security fees are those collected for "security fixtures, equipment and features that are specific to one customer agency, requested by that customer agency and its internal security guidelines and not used in the entire building."

The term countermeasures can have multiple definitions within the space of security. For the purposes of countermeasures in this report, there are two distinct categories: security fixtures and security equipment. GSA and FPS divide responsibility for the implementation of countermeasures on the basis of the type of measure. Security fixtures are GSA's responsibility and are defined as:

---

[2] Although stated in the C.F.R. and the GSA *Pricing Desk Guide, 5th Edition* (www.gsa.gov/cdnstatic/Pricing%20Desk%20Guide%205th%20Edition%20November%2016,%202019_0.pdf), FPS does not amortize project/capital costs for the tenants and charge them back. FPS does charge a percentage of the total project costs for maintenance of the security equipment installed per square footage on a monthly basis. Some legacy amortized project costs still are being collected, which predated the decision to eliminate amortization from the FPS service offerings.

[3] The MOA referenced by the GSA Pricing Guide is the MOA between GSA and FPS concerning the protection of federally owned and leased buildings, grounds, and property under the jurisdiction, custody, or control of GSA. The most recent MOA became effective on September 27, 2018.

> Physical security measures that are either part of the building or attached and not easily removable from the building. Security fixtures include vehicular barriers, such as bollards, pop-up and arm gates, doors, locks, HVAC [heating, ventilation, and air conditioning] security items (including filtration systems), exterior lighting, PACS [Physical Access Control Systems], garage doors, security fencing and gates, guard booths (both attached to the building and free standing), and blast-resistant countermeasures. … Window glazing and progressive collapse are other examples of security fixtures.[4]

FPS is responsible for the design, installation, testing, maintenance, and repair of security equipment billed through the building-specific security charge or security work authorization. Security equipment is defined in the MOA as:

> Security countermeasures that are not part of a building and easily removable from the building, such as x-ray machines, magnetometers, closed circuit video systems, and intrusion detection and alarm systems.[5]

This is an important taxonomy distinction necessary for understanding investment and implementation of countermeasures in the federal space because it divides responsibility between two separate parties (GSA and FPS) with varying authorities, funding mechanisms, and processes. This distinction is most important upon the approval of a countermeasure by the FSC. FPS, GSA, and most other departments and agencies in the Federal Government utilize the Interagency Security Committee (ISC) standards and guidelines for conducting risk management.

On October 19, 1995, 6 months after the Oklahoma City bombing of the Alfred P. Murrah Federal Building, President Clinton issued Executive Order (EO) 12977,[6] creating the ISC to address continuing governmentwide security for federal facilities. Prior to 1995, minimum physical security standards did not exist for nonmilitary federally owned or leased facilities. The ISC's mandate is to enhance the quality and effectiveness of physical security and the protection of buildings and nonmilitary federal facilities in the United States.

The primary method for standardizing risk management and federal physical security by the ISC is the publication of standards. The source publication for accomplishing this is *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (RMP),[7] which applies to all facilities in the United States occupied by federal employees for nonmilitary activities, pursuant to EO 12977. These facilities include existing buildings, new construction, or major modernizations; facilities owned, to be purchased, or leased; standalone

---

[4] MOA by and between DHS and GSA, September 27, 2018, Section 11 Item H.1
[5] MOA by and between DHS and GSA, September 27, 2018, Section 10 Item B.2
[6] EO 12977, "Interagency Security Committee," October 19, 1995 (URL: www.govinfo.gov/content/pkg/FR-1995-10-24/pdf/95-26497.pdf accessed July 22, 2020), and as amended by EO 13286, March 5, 2003 (URL: https://www.govinfo.gov/content/pkg/FR-2003-03-05/pdf/03-5343.pdf accessed July 22, 2020).
[7] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 2nd Edition, November 2016. URL: https://www.cisa.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf accessed May 29, 2020.

facilities, federal campuses, and, where appropriate, individual facilities on campuses; and special-use facilities.

The RMP establishes roles and responsibilities for stakeholders involved in security of federal facilities. The most prominent and applicable roles involved in countermeasures are the FSC, security organization, and owning/leasing authority. Each of these roles, as defined by the RMP, is essential for planning, approving, and implementing countermeasures.

Security organizations are responsible for identifying and analyzing threats and vulnerabilities and for recommending appropriate countermeasures. The decision to implement those recommendations and to mitigate the risk or to accept risk as part of a risk management strategy is that of the FSC. FSCs are responsible for deciding and documenting the chosen strategy: risk mitigation (implementation of measures) or risk acceptance (implementation of lesser or no measures). Once a credible and documented risk assessment is presented to and accepted by the decision makers, the security provider is not liable for any future decision to accept risk.[8] With that, the ISC RMP is the sole mechanism for implementing security investments/countermeasures. Fundamentally, if the process is followed and the measure is not approved, FPS is still responsible for protection at the facility notwithstanding the lack of security mitigation resulting from adherance to the RMP.

The RMP mandates the approach necessary to identify, assess, and prioritize the risks to federal facilities.[9] The process provides a method for determining the facility security level (FSL) based on the characteristics of each facility and the federal occupants' mission space. The FSL is the starting point for implementing security countermeasures and is commensurate with approximately 100 measures that must be evaluated for applicability at the facilities being assessed. The FSL spans from level 1 (the lowest designation of security) to level 5 (the highest designation for security).[10]

Upon completion of an FSL determination, the security organization is responsible for assessing the facility.[11] This assessment evaluates threats, vulnerabilities, and consequences, which, when taken together, comprise risks applicable to the facility.[12] The assessment is documented in a written report that details countermeasure recommendations tailored to the risk profile for the facility. The report is presented to an FSC for approval or rejection of each countermeasure. A vote to approve the measure is considered a funding obligation/commitment, and the measure

[8] Id at 28, Section 5.1.10
[9] Id at 22, Section 5.1.2
[10] Id at 22, Section 5.1.2.
[11] Id at 22, Section 5.1.2.
[12] Note: The ISC does not mandate the use of a specific risk assessment methodology. The chosen methodology should adhere to the fundamental principles of a sound risk assessment methodology:

1. The methodology must be credible and must assess the threat, consequences, and vulnerability to specific acts.
2. The methodology must be reproducible and must produce similar or identical results when applied by various security professionals.
3. The methodology must be defensible and must provide sufficient justification for deviation from the baseline.

enters the project planning and implementation phase.[13] If the FSC rejects the measure, the risks associated with any unmitigated vulnerabilities are accepted.[14]

FPS, as a primary security organization for federal facilities, adheres to the RMP requirements to assess risks and to recommend countermeasures. FPS provides a report to the FSC and supports the conduct of FSC meetings through coordination, planning, and explanation of the RMP requirements as well as the proposed security countermeasures. Federal facilities (leased or owned) may choose, through FSC approval, to implement countermeasure recommendations as detailed in an assessment report or at the request of a tenant agency. FSCs may approve a countermeasure recommendation, but there is no mandatory provider for the measure unless a previous agreement or policy mandates one.

A vote to approve a measure by the FSC is considered a funding commitment/obligation. Each federal tenant has one vote. Each vote is weighted to the rentable square footage of assigned space (by percentage of total square footage for the building) for each federal tenant. A quorum of 50 percent of the FSC members is required for a vote on a decision item. A decision item passes or fails with a majority of the facility's weighted vote.[15] A measure receiving a majority vote for approval is considered "approved" no matter how each tenant voted; all tenants are obligated to provide a portion of the countermeasure cost, which is based upon their pro-rata share of rentable square footage. The voting procedures and FSC processes create numerous challenges when aligned with government budgeting procedures and cycles. For example, a measure approved by a majority of represented square footage in a facility is considered an unfunded requirement for tenants voting against the measure. This requires federal agencies to include new requirements in their budget requests and to prioritize the funding of the measure against all other priorities for that entity. As the new requirement enters the budget request cycle, depending upon the time of the approval, tenants may have to wait for the next fiscal year or two to request unobligated funds from other programs resulting in procurement delays for projects.

Upon approval of a countermeasure, if the measure is security equipment, FPS begins the process of establishing a statement of work (SOW), project plan, and collection of funding to request proposals or to solicit vendors to perform the work. FPS has a national contract vehicle that it utilizes for the purchase of walk-through metal detectors/magnetometers (WTMD). The WTMDs are standardized to ensure that consistent equipment is utilized by FPS Protective Security Officer (PSO) contract employees. FPS has a national contract for the leasing of X-ray machines. The X-ray machines also are standardized to ensure that consistent equipment is utilized by the FPS PSO contract employees.

Each new surveillance and intrusion detection system and substantial upgrades/replacements are accomplished through individual purchase contracts. The acquisition process requires a fully funded requisition, SOW, regulatory review and approval (information technology (IT) equipment approval), open solicitation and competition, selection, and installation/

[13] Id. at D-3, Section D.2.3.
[14] Id. at D-3, Section D.2.2.
[15] Id at D-2 Section D.3.1

acceptance.[16,17] Some repairs may fall below the threshold for micropurchases, and a government purchase card is utilized. Purchase card actions require significantly less work and only internal coordination and approvals.[18]

EO 12977 requires the ISC to "develop a strategy for ensuring compliance" with ISC policies and standards. In 2019, the ISC fully deployed the ISC Compliance System and completed its inaugural year of compliance reporting … .[19] According to the ISC 2019 Annual Report highlighting compliance reporting, 81 percent of ISC's primary members and 67 percent of associate members participated in the FY 2019 compliance reporting. Of the 45 organizations that reported compliance information, another 118 of their suborganizations or components entered compliance information.[20, 21] Compliance reporting is in the early stages of participation, and much work to understand the full U.S. Government's participation in the RMP still is needed.

FPS continues to document a lack of responses and participation by FSCs. Specifically, FPS has documented, in 3 fiscal years (FYs 2017, 2018, and 2019), that FPS produced and presented 5,619 facility security assessments (FSA) for a total of 19,933 countermeasure recommendations. Of those recommendations, 23.81 percent were approved, 9.80 percent were rejected, and 64.38 percent received no response from/by FSCs. The remaining 2.01 percent were not voted upon or required additional information/coordination. In summary, 75 percent of the measures recommended by FPS, as a security organization, have not been implemented in the last 3 years. FPS has invested significant resources into the conduct of FSAs. Nevertheless, FSCs have not responded to the majority of countermeasure recommendations, and ISC compliance reporting and assistance has not affected the statistics collected by FPS.

Successful implementation of many countermeasure recommendations is conditioned upon specific provisions of leases, lessor authorization, FSC, and contract officer approvals. To reiterate, ownership is important when identifying the restrictions for implementation. The ISC requires documentation and retention of all decision-making by the FSC, yet, there is nothing stating that upon approval of a countermeasure project (security equipment or not), the tenant must utilize FPS or any other source. In some instances, the owning-leasing authority, through occupancy agreements and leases, has established the requisite service provider and processes, but FPS typically is not included in those requirements. This lack of a required service provider, FSC participation, and fragmented funding mechanisms are affecting the rates of countermeasure projects. According to FPS records, there were 1,045 approved electronic security system projects in the last 3 fiscal years. This yielded 44 video surveillance system and 19 intrusion

[16] Federal Information Technology Acquisition Reform Act, P.L. 113-291, Title VIII, Subtitle D
[17] The procurement process for video surveillance systems is different for judiciary spaces. The U.S. Marshal Service has an established national contract vehicle to install systems.
[18] In FY 2018, 20 projects made it through the regulatory review (IT equipment and purchase approval) process. In FY 2019, 24 projects made it through the regulatory review process. It is important to identify that this merely means that the SOW contained enough information to receive an IT purchase approval from FPS and DHS. These projects may not have materialized in the fiscal year in which they were approved because the contracting process often crosses fiscal years.
[19] ISC 2019 Annual Report
[20] Id at 3.
[21] Primary members are the 21 federal departments and agencies designated by EO 12977 and modified by EO 13286.

detection system projects in the last 2 fiscal years, a significant disparity between security equipment approval and implementation. Given this lack of adoption and implementation, FPS records indicate that several systems are aging without a predictable replacement or modernization possibility in the near future.

III. Countermeasures: Alternative Methods for Assessing and Allocating Costs

The challenges in requesting, obligating, and applying funding, contracting, and risk management processes were evaluated with OMB. FPS has provided a summary of the potential options for improving countermeasures in federal facilities.

Option 1: Leveraging data collected during the last 5 fiscal years, FPS will identify the highest risk facilities, most antiquated systems, and requisite investments needed to coordinate with departments and agencies at the headquarters level.

Over the course of several months of coordination with OMB, FPS has identified many opportunities for improving internal Executive Branch coordination and prioritization of funding for federal facilities' countermeasures. FPS will begin compiling data to engage federal departments and agencies for security investments.

FPS will identify antiquated systems with unresolved (no response/no vote) countermeasure recommendations for security equipment. FPS also will correlate these projects with facility-specific configurations (single tenant, multitenant), FSC chairmanships held by departments and agencies, and risk factors (consequence scores, vulnerability scores, and threats). FPS will share this information with agency chief financial officers, as well as with OMB, to coordinate prioritization of appropriated funds and identification of efficient contract vehicles. Upon review and clearance by OMB, FPS will transmit a copy of these reported projects to congressional committees of jurisdiction when requested. This option enables FPS to coordinate with agencies and OMB to prioritize funding and to work with departments and agencies to increase participation in the process.

Additionally, OMB will support the identification and establishment of improved procurement processes to alleviate some of the current challenges associated with individual contract vehicles for each system procurement.

Option 2: FPS will coordinate with the ISC on process improvement and participation of federal departments and agencies. FPS will provide data and will coordinate outreach efforts with the ISC Compliance Subcommittee to improve FSC participation.

FPS is utilizing its data to inform disparities between ISC compliance reporting and FSC participation. A large section of federal facilities does not participate adequately in the assessment and risk management process. In addition to the ISC's efforts to educate and to assist in the adoption, utilization, and participation of the RMP, FPS will continue to collaborate and to share information about FSC participation in the assessment and countermeasure recommendation process. This information will enable the ISC to prioritize outreach and compliance efforts on departments and agencies not participating in the process. Alternatively, it will provide the ISC with an ability to compare and contrast compliance reporting data against FSC participation data.

FPS has coordinated a change to the RMP where FSCs will accept the risks associated with the countermeasure recommendations when they do not respond to the assessment. The revised language makes it clear to the FSCs that a lack of response to the security organization's assessment and recommendations is an acceptance of those risks. The RMP currently requires a documented decision to accept risk and does not address a lack of participation in the process. This leaves the security organization responsible for pursuing or attempting to compel participation. The revised language change to the standard will shift the burden of participation onto the FSCs responsible for the decision-making process in the RMP.

Option 3: FPS will include lifecycle replacement costs into building-specific security charges for security equipment projects.

FPS collects building-specific security fees for the operations and maintenance (O&M) of security equipment installed in federal facilities. These collections currently are limited by the language included in the FPS budget submissions, justifications, and approvals for the explanation and utilization of the fees. Specifically, O&M collections are required to be expended during the period of availability solely upon O&M-related expenditures. [22] This means that anticipated upgrades for the system cannot be factored into or allocated funding under the current financial construct. However, FPS will include the lifecycle costs into O&M and will work with agencies to ensure that adequate funding is available when the system exceeds its recommended lifecycle. FPS will provide a lifecycle date and estimated costs of replacement, and will include this information in the initial recommendation to the customer agencies for all new security equipment. Upon the occurrence of the anticipated lifecycle date, FPS will receive approval from the FSC to use the fees already collected for the contracting of a replacement system.

The Countermeasures program/project/activity uses the following two recovery charging categories in FPS' budget authority to collect for security services:

1. FPS provides building-specific security services in accordance with security requirements generated through an FSA or customer request. FPS distributes building costs to tenants based on their portion of square footage from the GSA occupancy agreements and recovers direct contract costs monthly.
2. FPS negotiates agency-specific security, also called tenant-specific security, via security work authorizations or reimbursable agreements between FPS and another federal agency. The security service charges are similar to building-specific charges, but FPS provides these to an individual customer rather than to the facility. Monthly, FPS collects the direct costs of the security services that customers request.

Lastly, the presence of antiquated technology and equipment that has reached and/or exceeded its intended useful life (much of the equipment is more than 10 years old) has created significant risks by degrading the ability to detect, deter, delay, and investigate credible threats to federal

[22] Unexecuted O&M funds normally are returned to the tenants unless the tenant declines acceptance. When this occurs, these funds result in "carryover." Carryover still is restricted to the same spending limitations as O&M. If the cost of requirements exceeds the amount available or does not fall within expenses related to maintenance of the system, the funding cannot be utilized.

facilities, personnel, information, and equipment. Older analog technology is not supported by manufacturers, integrators, or installers. Therefore, it is necessary for FPS to continue updating technical countermeasure projects with digital technology and equipment in order to address the evolving threat environment by enhancing its ability to secure federal facilities. This upgrade and refresh effort would assist in lowering security risks to facilities by addressing technology obsolescence and technical countermeasure requirement gaps, and by facilitating real-time intelligence and information sharing.

In sum, FPS has not included any options requiring legislative action to change the processes or methods utilized for technical countermeasures. FPS will continue to coordinate its efforts with OMB to implement the options included in this report and to monitor improvement of technical countermeasures in federal facilities.

Appendices

Appendix A: Equipment Descriptions

FPS Countermeasures	Equipment Description
VSS/CCTV	A video surveillance system (VSS), formally known as closed circuit television (CCTV), is an information technology system comprising camera units, digital storage media, monitors, and associated networking devices and equipment. VSS is deployed in a facility to deter threats, to record incidents, and to augment protective security officers' effectiveness through real-time monitoring. Historically, the Federal Protective Service (FPS) has procured Facility Security Committee (FSC)-approved security camera systems for deployment within given facilities through individual project procurements. See *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Standard*), 2nd Edition, Appendix B: Countermeasures*" for countermeasure recommendations by facility security level (FSL) and for operational deployment scenarios.[23]
IDS	An intrusion detection system (IDS) is a system that secures a facility's perimeter access points (e.g., doors, windows, etc.) through various equipment (e.g., door contacts, window-break sensors) and support hardware (e.g., low-voltage wiring, telecommunication media). IDS alarm activations alert FPS Megacenters of any unauthorized entry to a protected facility. Historically, FPS has procured FSC-approved IDSs for deployment within given facilities through individual project procurements. See *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Standard*), 2nd Edition, Appendix B: Countermeasures*" for countermeasure recommendations by FSL and for operational deployment scenarios.
WTMD/ Magnetometer	A walk-through metal detector (WTMD), also referred to as a magnetometer, is a passive device that monitors the earth's magnetic field and detects changes to that field caused by the presence of ferromagnetic materials.[24] WTMDs, in conjunction with X-ray machines, are the basis for security screening tools that are implemented in federal facilities to detect prohibited and threat items

[23] The Interagency Security Committee's *Countermeasures* is labeled For Official Use Only. Government users with a need to know may request access via email to ISCAccess@hq.DHS.gov with the user's full name and contact information, including email address, the name of the user's agency, and the reason that the user needs access.
[24] Fennelly, Lawrence J. *Effective Physical Security*, Third Edition. 2004

	from being introduced into the facility. FPS has procured 797 units through national purchase agreements with CEIA-USA. See *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Standard*), 2nd Edition, Appendix B: Countermeasures*" for countermeasure recommendations by FSL and for operational deployment scenarios.
X-ray Machines	X-ray machines are package-search tools that use single-energy transmission X-ray imagers to find metallic items.[25] X-ray machines, in conjunction with WTMDs, are the basis for security screening tools that are implemented in federal facilities to detect prohibited and threat items from being introduced into the facility. FPS has a national leasing agreement in place with Smiths Detection, with 1,491 leased units. See *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Standard*), 2nd Edition, Appendix B: Countermeasures*" for countermeasure recommendations by FSL and for operational deployment scenarios.

[25] Fennelly, Lawrence J. *Effective Physical Security*, Third Edition. 2004

Appendix B: Abbreviations

Abbreviation	Definition
CCTV	Closed Circuit Television
C.F.R.	Code of Federal Regulations
DHS	Department of Homeland Security
EO	Executive Order
FPS	Federal Protective Service
FSA	Facility Security Assessment
FSC	Facility Security Committee
FSL	Facility Security Level
FY	Fiscal Year
GSA	U.S. General Services Administration
HVAC	Heating, Ventilation, and Air Conditioning
IDS	Intrusion Detection System
ISC	Interagency Security Committee
IT	Information Technology
O&M	Operations and Maintenance
OMB	Office of Management and Budget
PACS	Physical Access Control System
PBS	Public Building Service
PSO	Protective Security Officer
RMP	*The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*
SOW	Statement of Work
VSS	Video Surveillance System
WTMD	Walk-Through Metal Detector