Federal Building and Facility Security

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy

Lorraine H. Tong
Analyst in American National Government

March 24, 2010

Congressional Research Service
7-5700
www.crs.gov
R41138

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The security of federal government buildings and facilities affects not only the daily operations of the federal government but also the health, well-being, and safety of federal employees and the public. Recent congressional action concerning the security of federal buildings includes P.L. 111-83 (FY2010 appropriations for the Department of Homeland Security), which addressed the issue of the transfer of the Federal Protective Service from Immigration and Customs Enforcement to the National Protection and Programs Directorate.

For the purposes of this report, federal facilities include any building leased or owned by the General Services Administration. In FY2007, the federal government's real property portfolio comprised 446,000 buildings with an area of 3.3 billion square feet and a replacement value of $772.8 billion.

Security of federal facilities includes physical security assets such as closed-circuit television cameras, barrier material, and security guards (both federally employed and contracted). Federal facility security practices have been subject to criticism by government auditors and security experts. Elements that have received criticism include the use of private security guards, the management and security practices of the Federal Protective Service, and the coordination of federal facility security.

Contents

Contacts

Prior to the April 19, 1995, bombing of the Alfred P. Murrah Building in Oklahoma City, the federal government had no formally established security standards for federally owned or leased facilities.[1] Immediately following the bombing, President William J. Clinton directed the Department of Justice (DOJ) to assess the vulnerability of federal facilities to terrorist attacks or violence and to develop recommendations for minimum security standards.[2] The U.S. Marshals Service (USMS), within DOJ, coordinated two working groups to accomplish these presidential directives. The working groups identified and evaluated various security measures and activities that could address potential vulnerabilities, and minimum security standards were also proposed for federal facilities. Additionally, USMS deputies and General Services Administration (GSA) security specialists conducted inspections at more than 1,200 federal facilities to obtain security data on buildings for use in upgrading existing conditions to comply with the proposed minimum standards. The result of the working groups' efforts was the report *Vulnerability Assessment of Federal Facilities*.[3] This report was significant because it represented the first time that broad security standards were applied to federal facilities.

After the report was issued, President Clinton directed all executive branch agencies to begin upgrading their facilities to meet the recommended minimum security standards. Following the DOJ recommendations, President Clinton also required GSA to establish building security committees for all GSA facilities.[4]

Federal Facility Security Levels

Because of the differences among federal buildings and their security needs, USMS categorized federal facilities into five classes based on building size, agency mission and function, tenant population, and the degree of public access to the facility, and developed security standards corresponding to the security level needed for each class:

- Level I—buildings with no more than 2,500 square feet, 10 or fewer federal employees, and limited or no public access;
- Level II—buildings with 2,500 to 80,000 square feet, 11 to 150 federal employees, and moderate public access;
- Level III—buildings with 80,000 to 150,000 square feet, 151 to 450 federal employees, and moderate to high public access;
- Level IV—buildings with 150,000 square feet or more, more than 450 federal employees, and a high level of public access; and

[1] U.S. Department of Justice, U.S. Marshals Service, *Vulnerability Assessment of Federal Facilities*, Washington, DC, June 28, 1995, p. 1-1.

[2] U.S. Government Accountability Office, *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities*, GAO-02-1004, September 2002, p. 5.

[3] U.S. Department of Justice, U.S. Marshals Service, *Vulnerability Assessment of Federal Facilities*, Washington, DC, June 28, 1995.

[4] U.S. President (Clinton), "Memorandum on Upgrading Security at Federal Facilities," *Public Papers of the Presidents of the United States*, vol. I, June 28, 1995, pp. 964-965.

- Level V—buildings that are similar to Level IV but are considered critical to national security (for example, the Pentagon).[5]

Interagency Security Committee (ISC)

The Interagency Security Committee was established in 1995, originally as part of GSA, and was transferred to the Department of Homeland Security (DHS) in 2003. The following two sections describe the ISC's work under GSA and DHS chairmanships.

1995-2003: GSA Chairmanship

On October 19, 1995, President Clinton issued an executive order that established the ISC to address "continuing government-wide security" for federal facilities.[6] Chaired at the time by the GSA Administrator, the ISC was composed of representatives from each of the executive branch agencies. The ISC was authorized to consult with other entities, including the Administrative Office of the U.S. Courts, in order to perform its duties. The executive order directed the ISC to

> (1) establish policies for security in and protection of Federal facilities;
>
> (2) develop and evaluate security standards for Federal facilities, develop a strategy for ensuring compliance with such standards, and oversee the implementation of appropriate security measures in Federal facilities; and
>
> (3) take such actions as may be necessary to enhance the quality and effectiveness of security and protection of Federal facilities, including but not limited to:
>
> (A) encouraging agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner;
>
> (B) assessing technology and information systems as a means of providing cost-effective improvements to security in Federal facilities;
>
> (C) developing long-term construction standards for those locations with threat levels or missions that require blast resistant structures or other specialized security requirements;
>
> (D) evaluating standards for the location of, and special security related to, day care centers in Federal facilities; and
>
> (E) assisting the Administrator in developing and maintaining a centralized security data base of all Federal facilities.[7]

Following its establishment, the ISC began to address new security technology developments, cost considerations, and the need to balance security standards with public access to federal buildings. In May 2001, the ISC issued its *Security Design Criteria for New Federal Office*

[5] U.S. Department of Justice, U.S. Marshals Service, *Vulnerability Assessment of Federal Facilities*, Washington, DC, June 28, 1995.

[6] Executive Order 12977, "Interagency Security Committee," 60 *Federal Register* 54411-54412, October 24, 1995.

[7] Ibid., p. 54412.

Buildings and Major Modernization Projects (updated in 2004), based on the five security levels for federal facilities.[8] This document required new construction projects to include the use of window glazing protection, establish minimum acceptable distances between federal buildings and streets, control vehicular access to buildings, and evaluate the location and securing of air intake vents.

The September 2001 terrorist attacks on the Pentagon and the World Trade Center heightened concerns about the vulnerability of federal buildings to violence or bombings. In response to these events, the ISC issued revised procedures to respond to potential vehicle bomb attacks by recommending that new federal buildings be constructed at a minimum distance of between 20 to 50 feet from the nearest perimeter barrier, depending upon the security level.[9]

Even though the ISC successfully completed its security design criteria and related documents, a 2002 GAO report found that the committee had made "little progress" in other mandated responsibilities. While GAO reported that the ISC was successfully disseminating security information to member agencies, it also found that the committee's effectiveness was hindered by GSA's "lack of aggressive leadership and support," in that the agency failed to issue operating procedures and did not provide sufficient staff support and funding. GSA was also unable to provide any documentation indicating that the agency or the ISC had actually monitored agency compliance with the security recommendations.[10]

2003-Present: DHS Chairmanship

Congressional enactment of the Homeland Security Act[11] in 2002 and the creation of DHS centralized the federal government's efforts to respond to terrorism, including enhancing physical security for federal facilities. Accordingly, the chairmanship of the ISC was transferred from the GSA Administrator to the DHS Secretary on February 28, 2003.[12] Within DHS, the chairmanship of the ISC was delegated to the Director of the Federal Protective Service (FPS) in January 2004.[13]

A 2004 report issued by GAO recommended that DHS direct the ISC to develop a plan that "identifies resource needs, implementation goals, and time frames for meeting the ISC's ongoing and yet-unfulfilled responsibilities."[14] GAO reported that standard operating procedures had been approved by agency members, and included new requirements for attendance and participation at ISC meetings. To address these issues, DHS (through the ISC) is creating and maintaining a

[8] This document is available only from the ISC. Contact information for the ISC is at http://www.dhs.gov/files/committees/gc_1194977813020.shtm.

[9] U.S. General Services Administration, Public Building Service, Memorandum for Assistant Regional Administrators, *Implementation of the Interagency Security Committee (ISC) Design Criteria Regarding Site Selection*, Washington, DC, April 26, 2002, pp. 1-2.

[10] U.S. Government Accountability Office, *Building Security*, GAO-02-1004, 2002, pp. 7-11.

[11] 116 Stat. 2135.

[12] Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security," 68 *Federal Register* 10624, March 5, 2003.

[13] U.S. Government Accountability Office, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices*, GAO-05-49, September 6, 2004, p. 9.

[14] Ibid., pp. 47-48.

centralized security database of all existing federal facilities. Since its transfer to DHS, the ISC has either updated or established the following standards or best practices:

- *Use of Physical Security Performance Measures*, gives policy guidance on metrics and testing for physical security programs;
- *Facility Security Level Determinations*, defines the criteria and process used in determining the security level of a federal facility;
- *Security Standards for Leased Spaces*, provides background information on why standards expressly for leased facilities are needed and identifies the framework of considerations upon which the standards were developed;
- *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, establishes design security criteria for new federal facilities; and
- *ISC Best Practices for Safe Mail Handling*, identifies best practices for mail room operations in federal agencies and assists security managers in implementing safe mail-handling practices.[15]

In addition to its duties to coordinate federal security efforts and develop security standards for the construction of new federal facilities, the ISC has been assigned responsibility for reviewing federal agencies' physical security plans. Homeland Security Presidential Directive 7, issued December 17, 2003, required federal agencies "to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks," and it assigned implementation responsibilities to DHS.[16] In July 2004, the ISC was designated to oversee and review each agency's physical security plan pertaining to protection of the nation's infrastructure and key resources. According to GAO, the ISC's successful completion of these new responsibilities would represent "a major step" toward carrying out its existing duties pertaining to compliance and oversight.[17] The ISC, however, does not have the authority to enforce standards on other federal departments and agencies. It relies on other federal entities' willingness and abilities to implement security standards and best practices.

Executive Branch Facility Security

Numerous agencies have responsibility for federal building security entities. Among them are such law enforcement agencies as the Central Intelligence Agency's (CIA) Security Protective Service, the Department of Defense's (DOD) Pentagon Police Directorate, and the State Department's Diplomatic Security Service's uniformed law enforcement officers. These agencies and facilities are usually limited in scope and size, involving a single location or a limited number of buildings. However, the primary agency for protecting federal facilities is the Federal

[15] These documents are "For Official Use Only" and can be obtained from the ISC.

[16] HSPD-7, "Directive on Critical Infrastructure Identification, Prioritization, and Protection," *Weekly Compilation of Presidential Documents*, vol. 39, December 17, 2003, p. 1816.

[17] U.S. Government Accountability Office, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices*, GAO-05-49, September 6, 2004, p. 11.

Protective Service (FPS), which is responsible for protecting almost half (48%) of all GSA owned or leased property.[18]

Federal Protective Service

FPS, now within FEMA's National Protection and Programs Directorate (NPPD),[19] is responsible for the protection and security of federally owned and leased buildings and property and of federal personnel.[20] In general, FPS operations focus on security and law enforcement activities that reduce vulnerability to criminal and terrorist threats. FPS protection and security operations include all-hazards based risk assessments; emplacement of criminal and terrorist countermeasures, such as vehicle barriers and closed-circuit cameras; law enforcement response; assistance to federal agencies through Facility Security Committees; and emergency and safety education programs. FPS also assists other federal agencies with additional security, such as assisting the U.S. Secret Service at National Special Security Events (NSSE).[21] FPS is the lead Government Facilities Sector Agency for the National Infrastructure Protection Plan.[22] Currently, FPS employs approximately 1,225 law enforcement officers, investigators, and administrative personnel, and administers the services of approximately 15,000 contract security guards.[23] P.L. 111-83 (FY2010 DHS appropriations) included provisions that required the FPS to maintain no fewer than 1,200 full-time equivalent staff and 900 full-time police officers, investigators, inspectors, area commanders, and special agents.

Historical Overview and Current FPS Authority

The responsibility to protect federal buildings was given to the Federal Works Agency in June 1948.[24] Specifically, Congress authorized the Federal Works Administrator to appoint uniformed guards as special policemen with responsibility for "the policing of public buildings and other areas under the jurisdiction of the Federal Works Agency."[25] The special policemen were given the same responsibility as sheriffs and constables on federal property to enforce the laws enacted for the protection of persons and property, and to prevent "breaches of peace, and suppress affrays or unlawful assemblies."[26]

[18] U.S. Government Accountability Office, *Homeland Security: Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants*, GAO-09-749, July 2009, p. 22. Other GSA-controlled facilities use an internal office within the tenants' agency (29%). The remainder rely on specific entities, such as GSA's Building Security and Policy Division, the U.S. Marshals Service, U.S. Postal Service Inspection Services, and private contractors (23%).

[19] FPS was transferred to NPPD from Immigration and Customs Enforcement following the enactment of FY2010 DHS appropriations (P.L. 111-83). 123 Stat. 2157.

[20] 40 U.S.C. 1315.

[21] For information on NSSEs, see CRS Report RS22754, *National Special Security Events*, by Shawn Reese.

[22] Information on the NIPP is at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

[23] U.S. Department of Homeland Security, National Protection and Programs Directorate, *Federal Protective Service: Fiscal Year 2011 Congressional Justification*, Washington, DC, February 2010, pp. FPS-1.

[24] 62 Stat. 281.

[25] Ibid.

[26] Ibid.

On June 30, 1949, the Federal Works Agency was abolished, and all of its functions, including the protection of federal buildings, were transferred to GSA.[27] In September 1961, Congress authorized the GSA Administrator to appoint non-uniformed special policemen to conduct investigations in order to protect property under the control of GSA; enforce federal law to protect persons and property; and make an arrest without a warrant for any offense committed upon federal property if a policeman had reason to believe the offense was a felony and the person to be arrested was guilty of the felony.[28]

The GSA Administrator formally established the Federal Protective Service (FPS) in January 1971 through GSA Administrative Order 5440.46. FPS, as an official GSA agency, continued to protect federal property and buildings with both uniformed and non-uniformed policemen.

FPS was transferred to the Department of Homeland Security, and placed within U.S. Immigration and Customs Enforcement (ICE), with enactment of the Homeland Security Act of 2002 (P.L. 107-296). The act required the DHS Secretary to "protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed ownership corporation thereof) and persons on the property."[29] With the passage of FY2010 DHS appropriations, Congress authorized the transfer of FPS from ICE to the National Protection and Programs Directorate.[30] On October 29, 2009, DHS Secretary Janet Napolitano announced this transfer.[31]

Under current statutory provisions, FPS officers are authorized to

- enforce federal laws and regulations to protect persons and federal property;
- carry firearms;
- make arrests without a warrant for any offense against the United States committed in the presence of an officer or for any federal felony;
- serve warrants and subpoenas issued under the authority of the United States;
- conduct investigations, on and off federal property, of offenses that may have been committed against federal property or persons on the property; and
- carry out other activities for the promotion of homeland security as the DHS Secretary may prescribe.[32]

[27] 63 Stat. 380.

[28] P.L. 87-275, Sec. 5, 40 U.S.C. §318.

[29] 40 U.S.C. § 1315(a). The DHS Secretary was authorized to designate DHS employees, including those transferred from FPS, as officers with responsibility for protecting federal property. Some federal buildings, however, are protected by guards who are not part of FPS, such as the buildings of the U.S. State Department, which has its own uniformed law enforcement officers.

[30] P.L. 111-83, Title III. 123 Stat. 2157.

[31] U.S. Department of Homeland Security, "Secretary Napolitano Announces Transfer of Federal Protective Service to National Protection and Programs Directorate," press release, October 29, 2009, http://www.dhs.gov/ynews/releases/pr_1256829032272.shtm.

[32] 40 U.S.C. § 1315(b)(2).

FPS's Use of Contract Security Guards

FPS's contract security guard responsibilities include federal building access control, employee and visitor identification checks, security equipment monitoring, and roving patrols of the interior and exterior of federal property.[33] Within the National Capital Region (NCR), FPS contracts with 54 private security guard companies to provide approximately 5,700 guards to protect 125 federal facilities. FPS issues task orders to contract security guard services that detail the terms and conditions under which the contract security guard services are to be provided. Some of these task orders include the identification of buildings requiring protection, specific guard post locations, and the hours and days of the week each post is to be staffed; whether security guards are to be armed; and the number of guards at each post. FPS currently employs approximately 15,000 contract security guards across the nation, and, according to the DHS Inspector General (DHS IG), contract guard services "represent the single largest item in the FPS operating budget, with an estimated FY2006 budget of $487 million."[34]

Federal Court Facility Security

The safe conduct of court proceedings and the security of judges, court personnel, and visitors in courtrooms, as well as the safety of judges off-site, continue to be a concern. The 2005 murders of family members of a federal judge in Chicago; the killings of a state judge, a court reporter, and a sheriff's deputy at an Atlanta courthouse; and the 2006 sniper shooting of a state judge in his Reno office all spurred efforts to improve judicial security.[35] Other threats against judges and court facilities have not stopped. For example, in September 2009, a plan to bomb the Paul Findley Federal Building and Courthouse in Springfield, IL, was uncovered and an arrest was made. On January 4, 2010, a gunman wounded a deputy U.S. marshal and killed a court security officer at the Lloyd D. George U.S. Courthouse and Federal Building in Las Vegas. Possible threats in the first week of 2010 included suspicious substances in letters sent to courthouses in Alabama. These recent incidents may result in review and increased oversight of judicial security at court facilities to ensure that adequate protective policies, procedures, and practices are in place. Additionally, increased security enhancements may be necessary for federal courthouses where trials of individuals charged with acts of terrorism are to be held.

Each of the three branches of the federal government plays a unique role in helping to ensure the safety of judges and the security of the federal courts. The role of Congress is to authorize programs that enhance security, appropriate funds, and provide oversight of judicial security. The Judicial Conference's Committee on Judicial Security monitors the security of the judiciary (including the protection of court facilities and proceedings, judicial officers, and court staff at federal court facilities and other locations) and makes policy recommendations to the conference. The Administrative Office of the U.S. Courts implements Judicial Conference policies, including security matters.

[33] U.S. Department of Homeland Security, Office of Inspector General, *Federal Protective Service Needs to Improve Its Oversight of the Contract Guard Program*, OIG-07-05, October 2006, p. 2.

[34] Ibid.

[35] In the 110th Congress, the President signed into law the Court Security Improvement Act of 2007 (P.L. 110-177), which was designed to enhance security for judges and court personnel as well as courtroom safety for the public.

By statute,[36] the United States Marshals Service within the Department of Justice has primary responsibility for the security of the federal judiciary, including the safe conduct of court proceedings, as well as the security of federal judges and court personnel at court facilities and off-site. USMS is charged with the protection and security of more than 2,000 federal judges and approximately 5,250 other court officials[37] at over 400 court facilities nationwide. [38] Within USMS, the Judicial Security Division (JSD) is specifically responsible for providing security services and staff support for the federal judiciary, including personal protection for judges and physical security for federal courthouses. Other space in the court facilities under the control of USMS includes holding cells adjacent to courtrooms, interview rooms used by attorneys and prisoners, cellblocks, prisoner elevators, and office space for USMS use. An appointed U.S. marshal, confirmed by the Senate, has security responsibility in each of the 94 federal judicial districts and the District of Columbia Superior Court. District U.S. marshals provide and oversee security of the judiciary using USMS resources and court security officers (CSO), who are employees of private security companies under contract with USMS. Over 4,500 CSOs provide various types of security (e.g., fixed posts, roving patrols, entry screening, and mail and package screening) in courthouses and at multi-tenant facilities. Also under USMS jurisdiction are the design, installation, and maintenance of security systems, and the oversight of communications equipment.

USMS conducts investigations of threats made against federal judges, U.S. attorneys, court staff, and their family members to determine the level of security that is necessary for developing security plans. In accordance with these findings, USMS assigns the required resources to ensure the safety of these people. A deputy marshal is required to attend any session of court at the request of the presiding judge.[39] A judicial security inspector (a senior-level deputy marshal) is assigned to each judicial district to evaluate courthouse security and procedures and to coordinate scheduling, posting, and other matters related to CSOs. The inspectors also conduct security surveys at judges' homes and recommend improvements. On June 1, 2004, USMS established the Office of Protective Intelligence (OPI) to review and analyze intelligence information about the security of those under USMS protection. OPI issues daily security advisories, intelligence bulletins, and law enforcement alerts to USMS district offices and senior staff at headquarters so that protective measures can be taken. When threats are made, USMS works with the Federal Bureau of Investigation (FBI) to evaluate the threats.

Within the Department of Homeland Security, FPS has overall responsibility for security in GSA-managed, multi-tenant federal buildings. When the buildings include court facilities, USMS and FPS share security responsibilities; this is authorized by a series of memoranda of agreement and understanding (MOA and MOU) between GSA and DOJ.[40] When the court is the sole tenant in a

[36] 28 U.S.C. § 566(a).

[37] USMS also provides protective details for judges and others who are targets of threats and attacks, and provides other law enforcement services for DOJ. For example, USMS is responsible for (1) providing protection for witnesses who testify for the government in cases involving organized crime and other significant criminal activity, (2) transporting criminal defendants to and from court appearances, (3) arranging for space in detention facilities to house pre-sentenced criminals, and (4) managing and disposing of forfeited properties acquired by criminals through illegal activities. For more information, see http://www.usmarshals.gov/duties.

[38]U.S. Department of Justice, United States Marshals Service, "Fact Sheet: Facts and Figures," USMS Pub. No. 21-H, revised February 9, 2009, Washington, DC, p. 1.

[39] As federal law enforcement officers, deputy marshals have other responsibilities, including criminal investigations, fugitive apprehension, witness protection, prisoner transportation, and execution of court orders.

[40] The December 1997 "Memorandum of Agreement for Court Security Between the GSA, USMS and AOUSC" (continued...)

GSA-managed building, USMS has primary responsibility for security, although FPS may provide some support for the perimeter security, or it may delegate this responsibility to USMS. The manner in which the responsibilities are shared varies case by case, depending on the differing requirements of tenants, functions, and locations of occupied space. These shared responsibilities and jurisdictions at individual court-occupied buildings are further determined by agreements (sometimes in writing), and coordinated to avoid duplication. Generally, USMS is responsible for and controls access to judicial space, while FPS is primarily responsible for perimeter security and for other interior space that is not court-related space. FPS conducts risk assessments of multi-tenant buildings to deter threats and take countermeasures. Uniformed FPS officers and hired contract guards (similar to court security officers) protect the buildings and their assets, and investigate crime at the facilities. Other than perimeter responsibilities, FPS duties may include visitor entry processing, roving patrols, garage access control, and mail and package screening.[41]

These principal entities communicate and coordinate at the national and district levels to ensure the security of the courts. At the national level, the Judicial Conference's Committee on Judicial Security coordinates security issues involving the federal courts with USMS, DOJ, and DHS. According to USMS, the Marshals Service works daily with the AOUSC Office of Court Security and the Office of Facilities and Security, and the Committee on Judicial Security also consults and coordinates over national and district-level security matters. At semi-annual meetings, the Committee on Judicial Security and USMS senior management discuss security, legal, and budget issues. In addition, USMS and AOUSC hold working sessions to discuss issues that include the purchase and installation of security systems, CSO staffing, and budget matters. At the local level, U.S. marshals routinely meet with the district chief judge at court security committee meetings including representatives from the magistrate, district, and bankruptcy courts (and sometimes circuit judges and U.S. attorneys) to review and implement security plans. AOUSC and USMS also consult on security considerations (e.g., design and installation of security systems) in the construction of new or renovated courthouses.

On January 5, 2009, USMS implemented a pilot program to assume primary responsibility for perimeter security at selected courthouses that were previously the responsibility of the FPS. This pilot was undertaken in accordance with FY2009 enacted legislation[42] as a result of the

(...continued)

defined each agency's area of responsibility for judicial security. According to the MOA, the three parties recognized that a cooperative effort was needed to provide the federal courts with the necessary security. This MOA stated, "The requirements of this joint effort are delineated in the March 1982, 'Report of the Attorney General's Task Force on Security'; the March 1982, 'Joint Statement of the Chief Justice and the Attorney General before the Judicial Conference of the United States'; the December 1982, Delegation of Procurement Authority from GSA to the Department of Justice (DOJ); the June 1995 DOJ report entitled 'Vulnerability Assessment of Federal Facilities'; and the 1997 Delegation of Authority from GSA to DOJ delegating USMS authority to determine and provide the appropriate level of perimeter access control at all GSA-controlled facilities that house a judicial officer." When FPS was transferred from GSA to DHS in 2003, the MOA was reaffirmed by a Memorandum of Understanding (MOU), which stated that the terms of the 1997 MOA would continue without interruption with DHS assuming the responsibilities transferred from GSA. Parties to the MOU were DOJ, DHS, and AOUSC (signed by then-Attorney General John Ashcroft on November 20, 2003; then-director of AOUSC Leonidas R. Mecham on November 21, 2003; and then-Secretary of DHS Tom Ridge on January 21, 2004).

[41] Among FPS protective and security capabilities are (1) specialized response capabilities (e.g., canine, hazardous materials, and weapons of mass destruction response teams); (2) intelligence-sharing and investigative collaboration with law enforcement agencies at local, state, and federal levels; (3) key participation in federal anti-terrorism task forces; and (4) continuous monitoring of facility alarms and emergencies through FPS remote dispatch control centers.

[42] Omnibus Appropriations Act, 2009 (P.L. 111-8), Sec. 306, Title III, 123 Stat. 648.

judiciary's concerns that FPS was providing inadequate perimeter security. The pilot program, expected to cover an 18–month period, includes five courthouses located in Chicago, Detroit, Phoenix, New York, and Tucson, and two in Baton Rouge. The judiciary submitted a report to the House and Senate Appropriations Subcommittees on Financial Services and General Government on the implementation progress of the pilot program and is currently working with USMS on assessment tools for the program.

Supreme Court

As the Supreme Court's general manager, paymaster, and chief security officer, the Marshal of the Supreme Court oversees the administration and operations of the Court building.[43] The Marshal manages over 200 Court employees and supervises the federal property used by the Court. The Marshal also directs the Supreme Court Police Force, which comprises a chief of police and approximately 80 officers. The police force jurisdiction covers the Court building, its grounds, and adjacent streets.

Coordination of Federal Building Security

Federal building security includes such activities as the daily interaction of FPS and its federal customers, the coordination between USMS and the FPS in federal multi-use buildings, and the federal agency interaction with contract security guard companies. Federal agencies communicate with one another and state, local, and private sector entities to coordinate federal building security. It is important to note that the federal government's communication of potential and imminent terrorist and criminal threats to states, localities, and private sector entities is an important aspect of federal building security because the majority of federal agencies and departments lease, build, and occupy facilities located in local jurisdictions and are not segregated from the general populace, private industries and businesses, and state and local government facilities. Not only would local jurisdictions be susceptible to collateral damage in a terrorist attack on a federal building, but some federal agencies and departments also rely on state and local law enforcement entities in the event of criminal or terrorism activities at federal facilities.[44]

One established way the federal government communicates threats is through use of the Homeland Security Advisory System (HSAS), which is managed by DHS. HSAS, established on March 12, 2002, is a color-coded terrorist threat warning system. The system, which federal departments and agencies are required to implement and use, provides recommended protective measures for federal departments and agencies to prevent, prepare for, mitigate against, and respond to terrorist attacks. DHS disseminates HSAS terrorist threat warnings to federal departments, state and local agencies, the public, and private-sector entities. DHS, however, only provides protective measures for federal departments. This dissemination of warnings is conducted through multiple communication systems and public announcements. HSAS has five threat levels: low, guarded, elevated, high, and severe.[45] In 2009, DHS's Homeland Security

[43] The Court building is U.S. government property, which was completed in 1935 as a permanent home to the Supreme Court.

[44] U.S. Government Accountability Office, *Homeland Security: Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants*, GAO-09-749, July 2009, pp. 5-6.

[45] Information on HSAS is available at http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm.

Advisory Council established a task force to review the HSAS and recommend changes to the administration and use of the system.[46]

Some federal entities, in response to targeted and specific threats, have developed mechanisms for notifying other federal departments and agencies, such as the U.S. Nuclear Regulatory Commission's Office of Nuclear Security and Incident Response, which coordinates with DHS, the federal intelligence and law enforcement communities, and the Department of Energy (DOE). In 2005, John E. Lewis, Deputy Assistant Director of the FBI's Counterterrorism Division, testified before the House Committee on Homeland Security about the FBI's coordination with other federal agencies concerning potential nuclear threats or incidents. Mr. Lewis stated that the FBI has developed liaison relationships with DHS, DOE, and DOD, and he detailed how the FBI and these departments would coordinate their response efforts if there was a nuclear threat or incident.[47]

Within DHS, the Office of Operations Coordination is responsible for monitoring the nation's security situation daily, through the National Operations Center (NOC), and coordinating activities among DHS, governors, homeland security advisors, law enforcement entities, and critical infrastructure operators. Information on domestic incident management is shared with Emergency Operations Centers at federal, state, and local levels through the Homeland Security Information Network (HSIN), and state and local intelligence fusion centers.[48]

Federal Building Security Issues

Due to recent attacks on federal buildings and continued terrorism threats, Congress may wish to address issues associated with federal building security. Some of these issues include FPS's operations and use of contract security guards, coordination and sharing of federal building security information, Facility Security Committees, and appropriations and resources. These issues are discussed below.

FPS's Operations and Use of Contract Security Guards

The threat of terrorism since the September 11, 2001, attacks has increased emphasis on the physical security of federal property and congressional interest in FPS.[49] Since 2009, GAO has issued three reports about FPS, one on FPS's use of contract security guards[50] and two on FPS's operations to address federal facility vulnerabilities.[51]

---

[46] The task force's report and recommendations are available at http://www.dhs.gov/xlibrary/assets/hsac_task_force_report_09.pdf.

[47] Testimony of John E. Lewis, FBI Deputy Assistant Director, Counterterrorism Division, in U.S. Congress, House Committee on Homeland Security, Subcommittee on Prevention of Nuclear and Biological Attack, *Nuclear Incident Response Teams*, 109th Cong., 1st sess., October 27, 2005, Serial No. 109-50 (Washington: GPO, 2007).

[48] U.S. Department of Homeland Security, "Office of Operations Coordination," at http://www.dhs.gov/xabout/structure/editorial_0797.shtm. For further information on homeland security information sharing, see CRS Report RL34070, *Fusion Centers: Issues and Options for Congress*, by John Rollins.

[49] U.S. Government Accountability Office, *Federal Real Property: An Update on High Risk Issues*, GAO-09-801T, July 15, 2009, p. 14.

[50] U.S. Government Accountability Office, *Homeland Security: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered by Weaknesses in Its Contract Security Guard Program*, (continued...)

FPS's Operations

In November 2009, GAO identified the following concerns about FPS's operations:

- FPS does not have a risk management framework that couples threats and vulnerabilities with resource requirements;
- FPS lacks a strategic human capital plan to guide its current and future workforce planning efforts;[52]
- FPS lacks a systematic approach for using technology to reduce risk to federal facilities;
- FPS is inconsistent in sharing information and coordinating security with GSA and tenant agencies; and
- FPS lacks a reliable data management system for accurately tracking performance measurement and testing.[53]

One GAO recommendation is for FPS to improve its use of a fee-based system by developing an accurate method of accounting for the cost of providing security services to tenant agencies and ensuring that its fee structure takes into consideration the varying levels of risk and service provided at GSA facilities. [54] Congress may wish to address the implementation of this recommendation by requiring FPS specifically, and DHS generally, to develop an accurate method for assessing security service costs through statutory or conference language.

Additionally, GAO recommended an evaluation of whether continued use of the current fee-based system or another funding mechanism would be the most appropriate method for funding FPS operations.[55] Congress might want to require the DHS IG to review the use of the fee-based system versus the method of directly providing appropriations to FPS. Alternatively, Congress could determine without further review to begin a direct appropriation for FPS operations through statutory language in annual DHS appropriations. This approach would possibly reduce the amount of appropriations GSA and tenant agencies currently receive to pay FPS for security operations.

Considering all of these issues, Congress may want to review FPS operations further through oversight hearings or require FPS and DHS to report on what actions, if any, the agency is taking to address GAO and DHS IG findings. Further review and hearings may not, however, immediately ameliorate continuing FPS shortcomings.

(...continued)

GAO-09-859T, July 8, 2008.

[51] U.S. Government Accountability Office, *Homeland Security: Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist*, GAO-09-1047T, September 23, 2009; and *Homeland Security: Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings*, GAO-10-236T, November 18, 2009.

[52] U.S. Government Accountability Office, *Homeland Security: Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist*, GAO-09-1047T, September 23, 2009, p. 1.

[53] U.S. Government Accountability Office, *Homeland Security: Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings*, GAO-10-236T, November 19, 2009, p. 1.

[54] Ibid., p. 6.

[55] Ibid.

Concerns About FPS's Use of Contract Security Guards

GAO identified concerns with FPS's use of contract security guards, including that

- FPS does not fully ensure that its contract security guards have the training and certifications required to secure federal facilities;
- FPS does not have a completely reliable system for monitoring and verifying contract guard training and certification requirements;
- FPS does not have specific national guidance on when and how contract guard inspections should be performed; and
- FPS inspections of contract security guard posts at federal facilities are inconsistent, and the quality of the inspections varies across FPS regions.[56]

FPS has implemented some actions in response to GAO's findings. According to FPS officials, these actions include authorizing overtime to monitor contract security guards during non-routine business hours and requiring penetration tests to identify weaknesses at access control contract security guard posts. Additionally, FPS has implemented a new directive developed to clarify FPS responsibilities for conducting and reporting the results of inspections and evaluations.[57]

In FY2010, Congress attempted to address FPS's use of contract security guards by requiring FPS to maintain no fewer than 1,200 full-time equivalent staff and 900 full-time police officers, investigators, inspectors, area commanders, and special agents.[58] This requirement could increase FPS's oversight of contract security guards; however, increasing the number of FPS law enforcement officers may not solve problems immediately because of the time required to inspect contract security guard operations, to identify continuing shortcomings, and to train FPS and contract security guard personnel. Additionally, increasing the number of FPS law enforcement personnel could further strain FPS resources by increasing the amount of personnel benefits afforded to federal employees.

Coordination and Sharing of Federal Building Security Information

Terrorism threat information sharing and coordination of federal, state, and local government security operations are multi-faceted endeavors that require constant attention and are immediately reviewed, and possibly revised, following an attempted or successful terrorist attack, such as the recent attempted bombing of an airplane on December 25, 2009.[59] Federal facilities and agencies sharing terrorism threat information and coordinating facility security are specific

[56] U.S. Government Accountability Office, *Homeland Security: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered by Weaknesses in Its Contract Security Guard Program*, GAO-09-859T, July 8, 2008, p. 1.

[57] Ibid., pp. 16-17.

[58] P.L. 111-83, Title III, 123 Stat. 2157.

[59] For more information on terrorism information sharing, see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Mark A. Randol; and CRS Report RL33873, *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, by Richard A. Best Jr.

and integral parts of this government endeavor to ensure the nation's security. Congressional action on terrorism information sharing includes passage of the Intelligence Reform and Terrorism Prevention Act of 2004, which mandated the creation of an Information Sharing Environment (ISE).[60] The ISE is to facilitate the sharing of terrorism information among federal, state, local, and private sector entities through the use of policy guidelines and technologies.[61] However, problems have arisen related to the coordination and sharing of federal building security information.

GAO, in November 2009 testimony before the House Committee on Homeland Security, stated that even though FPS and GSA management officials have established communication processes, information sharing at the regional and facility levels is inconsistent, and FPS and GSA disagree overall about what information should be shared. As an example, GAO cited a memorandum of agreement between DHS and GSA that specified that FPS will provide quarterly briefings at the regional level; however, this has not been done consistently across all FPS regions. GSA security officials stated that the briefings that did occur primarily focused on crime statistics and did not constitute comprehensive threat analyses.[62]

Additionally, on September 30, 2009, DHS Secretary Janet Napolitano stated, before the Senate Homeland Security and Governmental Affairs Committee, that there is no single process or system for federal, state, and local entities to receive or share terrorism intelligence and threat information. The Secretary stated that the present system of sharing information is not streamlined, that it is a "work in progress," and that this may be the result of the security classification of the information. Also, the Secretary said that state and local officials may be confused about where to obtain terrorism threat information.

To address the issue of coordination and sharing of terrorism threat information among federal facilities, Congress could choose to require, through statutory language, that federal agencies report periodically on this matter to the committees of jurisdiction. Additionally, Congress could request that GAO revisit the ISE and its implementation since 2004. In 2008, GAO reported limited success with the implementation and noted that the ISE lacked guidance on ensuring accountability and assessing progress.[63] Additionally, Congress could request information on how federal agencies train personnel (specifically, building security managers and officials) on the sharing of terrorism threat information.

Congress could also require a review of the coordination and integration of information sharing systems used by federal agencies, such as Law Enforcement Online and the Homeland Security Information Network. This review might identify what systems are utilized most and what systems appear effective. The review might disclose which federal agencies are involved, and at what level, in each system. On this point, GAO noted in 2007 that when "identical or similar

[60] P.L. 108-458, Sec. 1016(b), 118 Stat. 3665.

[61] Ibid. For more information on ISE, see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Mark A. Randol.

[62] U.S. Government Accountability Office, *Homeland Security: Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings*, GAO-10-236T, November 18, 2009, pp. 13-14.

[63] U.S. Government Accountability Office, *Information Sharing: Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-637T, July 23, 2008, p. 1.

types of information are collected by or submitted to multiple agencies, integrating or sharing this information can lead to redundancies."[64]

None of these options, however, address the issue of how specific federal facilities interact with federal security entities such as FPS, or what type of informal coordination is conducted daily to ensure the safety and well-being of federal employees, and members of the general public who visit federal facilities.

Facility Security Committees

When a federal court is in a multi-tenant building, the court's representative is a member of the Facility Security Committee (FSC) (previously known as the Building Security Committee). Each FSC, made up of tenants in the building, considers and makes decisions on building security matters.

FSCs were mentioned at the November 18, 2009, House Committee on Homeland Security hearing on Federal Protective Service Transition.[65] The committee chair raised the issue of the potentially dangerous items that are allowed to be brought into federal buildings. In July 2009, GAO staff reported that they were able to smuggle bomb-making components into 10 high-security federal facilities in four different cities and successfully assemble the items inside the building. The components were not on the prohibited list for those facilities. Reportedly, FSCs in each federal building determine what items are prohibited, and there is no standard list of prohibited items. FPS makes security assessments and presents them to FSCs, but, according to the FPS director, FPS does not determine the prohibited items list.[66]

Congress might consider whether the current process for determining which items should be prohibited is sufficient, and whether the input provided by various tenants, including the judiciary—as well as recommendations by USMS, FPS, GSA, and others—is effective. Further, consideration might be given to mandating a standard list of prohibited items to enhance security at federal facilities and to establishing regular evaluations of the list.

Research[67] also indicated that few across-the-board standards have been established for the FSCs. The Interagency Security Committee formed a working group to examine and issue a document to address FSC operations.

While each federal facility may have different or unique security administrative challenges, the lack of standards in FSC administrative operations could imperil security. Among the areas that could be examined are the following:

---

[64] U.S. Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35, October 30, 2007, p. 1.

[65] U.S. Congress, House Committee on Homeland Security, *Federal Protective Service Transition*, hearing, 111th Congress, 1st sess., November 18, 2009. Based on the *Congressional Quarterly* transcript of the hearing, accessible by subscription only at http://www.cq.com/display.do?dockey=/cqonline/prod/data/docs/html/transcripts/congressional/111/congressionaltranscripts111-00003252978.html@committees&metapub=CQ-CONGTRANSCRIPTS&searchIndex=1&seqNum=6.

[66] Ibid.

[67] Research included various government documents, and discussions with the Administrative Office of the U.S. Courts (January 26 and 28, 2010), GSA (February 17, 2010), and other organizations.

- FSC membership composition, and the designation and authority of the committee chair;
- voting issues, including how a quorum and majority vote are determined;
- whether one vote for each tenant is fair or whether votes should be proportional to tenant space;
- whether the formula for allocating how much each tenant pays for security enhancements, now generally based on square footage, is equitable or appropriate;
- whether a minimum number of mandatory regularly scheduled meetings of the FSC (and others on an as-needed basis) should be required;
- whether there is a need for possible standards for written records of FSC meetings and other recordkeeping requirements;
- whether there is a system for tenants to appeal decisions and resolve possible disagreements;
- whether each tenant has efficient processes for securing the approval of its headquarters office with regard to security enhancement requests so that FSC can act to implement improvements without delay from one or more tenants;
- whether FSCs have adequate and timely communication with federal, state, and local law enforcement organizations; and
- whether there should be regular congressional or ISC review of FCS operations and reporting requirements.

Appropriations and Resources

If the Administration decided to hold trials of individuals[68] charged with terrorist acts in federal civilian court rather than in military tribunals, enhancing communication and coordination of all law enforcement agencies (federal, state, and local) and the judiciary would be critical. The planning and implementation of additional security enhancements, including staff, training, technology, and equipment, would be necessary for the security and safety of all parties involved. A systematic method for identifying and addressing concerns of the local community and officials might include assessing the disruptive impact security measures might have on the businesses and residences in the area, and on traffic around and leading to the courthouses. Depending on the location of such trials, airspace surveillance and extension of the perimeter for security might be considered.

Congress might take into account the unique jurisdictional responsibilities of each entity, including national intelligence agencies. Establishing a system for entities to coordinate expenditures in a timely manner might be necessary because such trials could continue for several years. Planning for multiple years of appropriations might be needed to enable the entities to continue to fulfill their functions.

[68] Such individuals may include the September 11, 2001, mastermind suspect Khalid Sheikh Mohammed and Umar Farouk Abdulmutallab, the man accused of attempting to blow up an airplane on Christmas Day 2009.

Congressional oversight could be critical to ensure that funds and resources are maximized under fiscal constraints. If sufficient funding is not provided in a timely manner to the federal entities involved, Congress might consider whether authorities are in place for entities to transfer resources currently devoted to other programs, and whether such transfers might adversely affect the performance of other missions.

Congress might also consider whether funding FPS directly could provide it with more stable and predictable funding than its current reliance on fees from other agencies and the judiciary. In addition, direct appropriations to FPS might reduce administrative costs for both FPS and the federal courts.

Conclusion

The federal government faces, daily, the task of securing a portfolio comprising 446,000 buildings. Accordingly, Congress could address concerns, some of which are addressed in this report, to ensure effective federal agency operations and the health, well-being, and safety of federal employees and the public.

Author Contact Information

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy
sreese@crs.loc.gov, 7-0635

Lorraine H. Tong
Analyst in American National Government
ltong@crs.loc.gov, 7-5846