
# Federal Building and Facility Security: Frequently Asked Questions

**Shawn Reese**
Analyst in Emergency Management and Homeland Security Policy

March 6, 2017

**Congressional Research Service**
7-5700
www.crs.gov
R43570

**CRS REPORT**
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. Federal building and facility security is decentralized and disparate in approach, as numerous federal entities are involved and some buildings or facilities are occupied by multiple federal agencies. The federal government is tasked with securing over 446,000 buildings or facilities daily.

The September 2001 terrorist attacks, the September 2013 Washington Navy Yard shootings, and the April 2014 Fort Hood shootings focused the federal government's attention on building security activities. This resulted in an increase in the security operations at federal facilities and more intense scrutiny of how the federal government secures and protects federal facilities, employees, and the visiting public.

This renewed attention has generated a number of frequently asked questions. This report answers several common questions regarding federal building and facility security, including

- What is federal facility security?
- Who is responsible for federal facility security?
- Is there a national standard for federal facility security?
- What are the types of threats to federal facilities, employees, and the visiting public?
- How is threat information communicated among federal facility security stakeholders?
- What are the potential congressional issues associated with federal facility security?

There has been congressional interest concerning federal facility security in past Congresses. On May 21, 2014, the House Transportation and Infrastructure Committee held a hearing on "Examining the Federal Protective Service: Are Federal Facilities Secure?" and on December 17, 2013, the Senate Homeland Security and Governmental Affairs Committee held a hearing on "The Navy Yard Tragedy: Examining Physical Security for Federal Facilities." Even though the majority of ongoing congressional interest in federal facility security has focused on the Federal Protective Service (FPS), FPS is only responsible for the security of 9,000 of the approximately 446,000 federal facilities. In addition to FPS, there are approximately 20 other federal law enforcement entities with federal facility security missions. Federal facility security is the responsibility of all branches of the government and all federal departments and agencies.

# Contents



## Tables



## Contacts

# Introduction

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. Federal building and facility security is decentralized and disparate in approach, as numerous federal entities are involved and some buildings or facilities are occupied by multiple federal agencies. The federal government is tasked with securing over 446,000 buildings or facilities daily.

Prior to the April 19, 1995, bombing of the Alfred P. Murrah Building in Oklahoma City, the federal government had no established approach to security for federally owned or leased facilities. 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. 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 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 *Vulnerability Assessment of Federal Facilities* report.[1] 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 GSA-managed facilities.[2]

The September 2001 terrorist attacks, the September 2013 Washington Navy Yard shootings, and the April 2014 Fort Hood shootings focused the federal government's attention on building security activities. This resulted in an increase in the security operations at federal facilities and more intense scrutiny of how the federal government secures and protects federal facilities, employees, and the visiting public.

There has been congressional interest concerning federal facility security in past Congresses. On May 21, 2014, the House Transportation and Infrastructure Committee held a hearing on "Examining the Federal Protective Service: Are Federal Facilities Secure?" and on December 17, 2013, the Senate Homeland Security and Governmental Affairs Committee held a hearing on "The Navy Yard Tragedy: Examining Physical Security for Federal Facilities." Even though congressional interest and oversight primarily focuses on the Federal Protective Service (FPS), it should be noted that the most recent incidents at federal facilities are not facilities that are the responsibility of FPS. FPS federal facility security responsibility is limited to only 9,000 of the approximate 446,000 federal facilities. In addition to FPS, there are approximately 20 other federal law enforcement entities with federal facility security missions. Federal facility security is an issue for all branches of the government and every federal department and agency.

This attention resulted in a number of frequently asked questions. This report answers several common questions regarding federal building and facility security. These questions include

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

[2] 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.

- What is federal facility security?
- Who is responsible for federal facility security?
- Is there a national standard for federal facility security?
- What are the types of threats to federal facilities, employees, and the visiting public?
- How is threat information communicated among federal facility security stakeholders?
- What are the potential congressional issues associated with federal facility security?

# What is federal facility security?

In general, federal facility security includes operations and policies that focus on reducing the exposure of the facility, employees, and the visiting public to criminal and terrorist threats. Each federal facility has unique attributes that reflect its individual security needs and the missions of the federal tenants. In 1995, USMS categorized federal facilities by security level:

- 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
- Level V—buildings that are similar to Level IV but are considered critical to national security (e.g., the Pentagon).[3]

Security operations may include

- all-hazards risk assessments;
- emplacement of criminal and terrorist countermeasures, such as vehicle barriers, closed-circuit cameras, security checkpoints at entrances, and the patrolling of the grounds and perimeter of federal facilities;
- federal, state, and local law enforcement response;
- emergency and safety training programs; and
- proactive gathering and analysis of terrorist and criminal threat intelligence.

# Who is responsible for federal facility security?

In addition to the FPS, and according to the Department of Justice's Office of Justice Programs (OJP), there are approximately 20 federal law enforcement entities that provide facility security. The federal law enforcement entities responsible for facility security are

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

- U.S. Department of Commerce's National Institute and Standards and Technology Police—Officers provide law enforcement and security services for NIST facilities;
- U.S. Department of Defense's Pentagon Force Protection Agency—Officers provide law enforcement and security services for the occupants, visitors, and infrastructure of the Pentagon, Navy Annex, and other assigned Pentagon facilities;
- U.S. Department of Health and Human Services' National Institutes of Health, Division of Police—Officers provide law enforcement and security services for NIH facilities;
- U.S. Department of Homeland Security's Federal Emergency Management Agency, Security Branch—Officers are responsible for the protection of FEMA facilities, personnel, resources, and information;
- U.S. Department of Homeland Security's U.S. Secret Service—Uniformed Division officers protect the White House complex and other presidential offices, the main Treasury building and annex, the President and Vice President and their families, and foreign diplomatic missions;
- The Federal Reserve Board Police—Officers provide law enforcement and security services for Federal Reserve facilities in Washington, DC;
- National Aeronautics and Space Administration, Protective Services—Officers provide law enforcement and security services for NASA's 14 centers located throughout the United States;
- Smithsonian National Zoological Park Police—Officers provide security and law enforcement services for the Smithsonian Institution's 163-acre National Zoological Park in Washington, DC;
- Tennessee Valley Authority Police—Officers provide law enforcement and security services for TVA employees and properties, and users of TVA recreational facilities;
- U.S. Postal Inspection Services—Postal police officers provide security for postal facilities, employees, and assets, as well as escort high-value mail shipments;
- U.S. Department of the Interior's U.S Bureau of Reclamation, Hoover Dam Police—Officers provide security and law enforcement services for the Hoover Dam and the surrounding 22-square-mile security zone;
- Judiciary's U.S. Supreme Court Police—Officers provide law enforcement and security services for the Supreme Court facilities;
- U.S. Department of Justice's Federal Bureau of Investigation Police—FBI police officers provide law enforcement and security for FBI facilities;
- U.S. Department of Justice's U.S. Marshals Service—Deputy marshals provide security for federal judicial facilities and personnel;
- Legislative Branch's U.S. Capitol Police—Officers provide law enforcement and security services for the U.S. Capitol grounds and buildings, and in the zone immediately surrounding the Capitol complex;[4]

[4] The U.S. Capitol Police assumed the security of the Library of Congress and its facilities in October 2009.

- Legislative Branch's U.S. Government Publishing Office, Uniformed Police Branch—Officers provide law enforcement and security services for facilities where information, products, and services for the federal government are produced and distributed;
- U.S Department of the Treasury's Bureau of Engraving and Printing Police—Officers provide law enforcement and security services for facilities in Washington, DC, and Fort Worth, TX, where currency, securities, and other official U.S. documents are made;
- U.S. Department of the Treasury's United States Mint Police—Officers provide law enforcement and security services for employees, visitors, and government assets stored at U.S. Mint facilities in Philadelphia, PA; San Francisco, CA; West Point, NY; Denver, CO; Fort Knox, KY; and Washington, DC; and
- U.S. Department of Veterans Affairs' Veterans Health Administration, Office of Security and Law Enforcement—Officers provide law enforcement and security services for VA medical centers.[5]

Some federal law enforcement agencies, such as the Federal Protective Service, do not stand post at federal facilities, but instead train, inspect, and monitor private security guard companies that provide personnel that occupy security check points and patrol federal facilities. Additionally, FPS responds to criminal and emergency incidents. FPS is responsible for over 9,000 federal facilities and monitors over 15,000 private security guards.[6] These 9,000 facilities are a small portion of the approximately 446,000 federal facilities, and the other 437,000 facilities may be secured by the law enforcement entities listed above; however, one may assume some of these facilities have no law enforcement presence.

# Is there a national standard for federal facility security?

Due to the large number and different types of federal facilities, there is no single security standard that applies to every facility. There is, however, an interagency committee responsible for providing a number of standards that address federal facility security. The Interagency Security Committee (ISC) has the mission to "safeguard U.S. nonmilitary facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners."[7] GSA originally chaired the ISC until the establishment of the Department of Homeland Security (DHS). Presently, DHS chairs[8] the ISC. Congressional enactment of the Homeland Security Act in 2002 and the creation of DHS centralized the federal government's efforts to respond to terrorism, including enhancing physical security of federal facilities. Accordingly, the chairmanship of the ISC was transferred from the GSA Administrator

[5] See http://www.bjs.gov/content/pub/pdf/fleo08.pdf.

[6] See https://www.dhs.gov/federal-protective-service-0.

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

[8] Specifically, DHS's Assistant Secretary for Infrastructure Protection is the DHS representative that chairs the ISC.

to DHS in March 2003.[9] ISC membership consists of over 100 senior level executives from 53 federal agencies and departments.[10] ISC centralizes some efforts to secure federal facilities.

These federal agency and department executives, through working groups, have developed and issued the following federal facility policy and standards:

- *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide* (November 2015);
- *The Risk Management Process: An Interagency Security Committee Standard* (November 2016);
- *The Risk Management Process for Federal Facilities, Appendix A: Design-Basis Threat Report* (January 2016);
- *The Risk Management Process for Federal Facilities, Appendix B: Countermeasures* (January 2016);
- *The Risk Management Process for Federal Facilities, Appendix C: Child-Care Centers Level of Protection Template* (January 2016); and
- *Items Prohibited from Federal Facilities: An Interagency Security Committee Standard* (February 2013).[11]

In addition to these standards, the ISC has issued numerous "best practices" including the following:

- *Security Specialist Competencies: An Interagency Security Committee Guide* (January 2017);
- *Federal Mobile Workplace Security: An Interagency Security Committee White Paper* (January 2017);
- *Best Practices for Security Office Staffing in Federal Facilities: An Interagency Security Committee Guide* (September 2016);
- *Best Practices and Key Considerations for Enhancing Federal Facility Security and Resilience to Climate-Related Hazards* (December 2015);
- *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (December 2015);
- *REAL ID Act of 2005 Implementation: An Interagency Security Committee Guide* (August 2015);
- *Facility Security Plan: An Interagency Security Committee Guide* (February 2015);
- *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper* (February 2015);
- *Securing Government Assets through Combined Traditional Security and Information Technology: An Interagency Security Committee White Paper* (February 2015);

[9] 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.

[10] Ibid.

[11] U.S. Department of Homeland Security, Interagency Security Committee, https://www.dhs.gov/isc-policies-standards-best-practices.

- *Best Practices for Working with Lessors: An Interagency Security Committee Guide* (November 2014);
- *Best Practices for Armed Security Officers in Federal Facilities* (April 2013);
- *Violence in the Federal Workplace: A Guide for Prevention and Response* (April 2013);
- *Occupant Emergency Programs: An Interagency Security Committee Guide* (March 2013);
- *Combating Terrorism Technical Support Office, Technical Support Working Group—Best Practices for Managing Mail Screening and Handling Processes: A Guide for the Public and Private Sectors* (September 2012); and
- *Combating Terrorism Technical Support Office, Technical Support Working Group—Best Practices for Managing Mail Screening and Handling Processes* (September 2012).[12]

Again, there is no single standard, but rather a combination of the USMS security-level designations and the ISC-developed standards and best practices.

# What are the types of threats to federal facilities, employees, and the visiting public?

Federal facilities, employees, and the visiting public are threatened with assault, weapon and explosive possession, sexual assault, robbery, demonstrations, homicide, and arson. Physical assault by criminals and weapon (including explosives) possession appear to be the most frequent crimes committed at federal facilities. On September 16, 2013, a federal contractor shot fellow employees at the Washington Navy Yard facility. This resulted in a Department of Defense (DOD) investigation on the Navy Yard's security operations.[13]

Federal facility security is as diffuse as the number of law enforcement agencies securing them. Individual facilities secured by the same law enforcement agency may be secured in different manners based on specific security needs and threats. This makes it challenging to collect official and comprehensive data on threats to or incidents occurring at federal facilities. A brief search of media sources between 2005 and 2017 reveals approximately 67 media-reported threats or incidents. It should be noted that the following examples are not representative of the full number of threats or incidents. These threats and incidents range from bomb threats to the shooting of federal facility employees and the visiting public. Of these 67 threats or incidents, 24 were an evacuation of a federal facility due to either a "suspicious package" or a "bomb threat." Fifteen of the incidents were shooting incidents, including the Navy Yard shooting in September 2013.

[12] Ibid.

[13] U.S. Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting*, November 2013, at http://www.defense.gov/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf; U.S. Department of Defense, *Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense*, November 20, 2013, at http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf; U.S. Department of the Navy, Office of the Chief of Naval Operations, *Report of the Investigation into the Fatal Shooting Incident at the Washington Navy Yard on September 16, 2013 and Associated Security, Personnel, and Contracting Policies and Practices*, November 8, 2013, at http://www.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf; U.S. Office of Management and Budget, *Suitability and Security Processes Review Report to the President*, February 2014, at http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf.

Other threats or incidents included a plane flying into a building with the IRS as a tenant in Austin, TX, in February 2010, and a Molotov cocktail thrown at a St. Louis, MO, federal building in April 2012. The April 2014 shooting at Fort Hood, TX, is not included in these 67 incidents.

In contrast to CRS's brief survey of media-reported incidents, FPS has provided crime data[14] to CRS[15] that reflect threats or incidents at facilities that FPS is responsible for securing (see **Table 1**). FPS criminal data on violent crime at federal facilities reflect information that is categorized as assault, weapons and explosive possession, sexual assault, robbery, demonstrations, homicide, and arson.

**Table 1. Crime Incidents at FPS-Secured Federal Facilities, 2010-2013**

| Crime | Number |
|---|---|
| Assault[a] | 497 |
| Weapons and Explosives[b] | 350 |
| Sexual Assault[c] | 42 |
| Robbery | 16 |
| Demonstrations or Disturbances | 14 |
| Homicide | 4 |
| Arson | 3 |
| **Total** | **926** |

**Source:** CRS analysis of FPS data (available by contacting the author of this report) and does not include incidents categorized as "multiple offenses."

a. Includes simple (verbal or physical) and aggravated.

b. Includes bombings or bomb possession, firearms possession, and related material.

c. Includes forcible rape.

The numbers in this table reflect incidents categorized by FPS, and such incidents as "assault" include both verbal and physical assaults, and "sexual assaults" include both aggravated and rape. FPS only secures approximately 9,000 federal facilities of the approximately 446,000 federal facilities, and as a result, the total number of threats against and incidents at all federal facilities is likely to be much higher.

# How is threat information communicated among federal facility security stakeholders?

One established method the federal government used to communicate threats was the Homeland Security Advisory System (HSAS), which was managed by DHS. In 2009, however, DHS's Homeland Security Advisory Council established a task force to review the HSAS and recommended changes to the administration and use of the system.[16] Upon completion of the

[14] CRS specifically asked the FPS to provide all violent crime information related to the 9,000 federal facilities it is responsible for, and these data only cover 2010-2013. FPS has not provided more recent data.

[15] It should be noted that these FPS data are only comprised of violent crimes reported, investigated, and prosecuted in relation to facilities that are secured by FPS.

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

review, DHS replaced the HSAS with the National Terrorism Advisory System (NTAS). NTAS communicates terrorism threat information by providing "timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector."[17]

Within DHS, the Office of Operations Coordination and Planning 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 System (HSIN) and state and local intelligence fusion centers.[18]

In addition to established information sharing processes, there are also ad hoc coordination and threat-specific information sharing processes. In 2005, the 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. The Deputy Assistant Director stated that the FBI has developed liaison relationships with DHS, the Department of Energy (DOE), and DOD, and detailed how the FBI and these departments would coordinate their response efforts if there was a nuclear threat or incident.[19] 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 DOE.

Threat information relevant to federal facility security is communicated between federal facility security managers, federal law enforcement entities securing the facilities, and local law enforcement entities that assist the federal government. Some federal facilities, especially those located in areas without a large federal government presence, rely on state and local law enforcement entities.

Congress reviews the communication of threat information because of the continued criminal and terrorist threats faced by federal facilities. How this threat information is shared among federal, state, and local government entities is an important aspect to federal facility security and is a proactive step in the risk management process.

# What are the potential congressional issues associated with federal facility security?

Congress may continue its oversight of federal facility security generally, and the FPS specifically. One issue the Government Accountability Office identified in a report published on May 21, 2014, was FPS's continued shortcomings in training and monitoring its contract security guards. GAO stated that FPS continued to face challenges ensuring that its contract security guards have been properly trained and certified before being deployed to federal facilities.[20] In its

[17] http://www.dhs.gov/files/programs/ntas.shtm.

[18] http://www.dhs.gov/about-office-operations-coordination-and-planning.

[19] 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).

[20] U.S. Government Accountability Office, *Federal Protective Service: Protecting Federal Facilities Remains A* (continued...)

December 2013 report, GAO found that FPS was challenged in providing active shooter response and screener training. As a result, GAO found that FPS had limited assurance that contract security guards at federal facilities are prepared to respond to active shooter incidents, and that contract security guards may have been using screening equipment without proper training.[21]

Additionally, GAO found that FPS and other federal agencies continued to face issues in assessing risk at federal facilities. GAO stated that its continuing study of federal facility risk assessment activities indicates that several federal agencies, including FPS, face challenges in completing and implementing the results of in-depth risk assessments. Specifically, GAO found that the Departments of the Interior and Veterans Affairs, FPS, the Federal Emergency Management Agency, and the Nuclear Regulatory Commission did not assess the threat, consequences, or vulnerability to specific events as required by ISC federal facility security standards.[22] Also, GAO found that FPS's Modified Infrastructure Survey Tool, which it currently uses to assess risk at federal facilities, does not assess potential consequences.[23]

Another issue Congress may address is federal facility emergency plans and planning. Even though GAO found that selected federal facilities' emergency plans generally reflect federal guidance, there are still challenges that federal agencies face. These challenges include employee participation apathy, accounting of employees, and updating of employee emergency contact information during testing of emergency plans.[24]

These issues, and other potential issues, were initially prompted by the 1995 bombing of the Alfred P. Murrah building. Since then, efforts have been made to improve standards. However, incidents such as the September 2001 attacks on the Pentagon and the shootings at the U.S. Navy Yard and Fort Hood, TX, indicate that some issues remain.

## Author Contact Information

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

(...continued)

*Challenge*, GAO-14-623T, May 21, 2014, p. 1.

[21] U.S. Government Accountability Office, Homeland Security: Federal Protective Service Continues to Face Challenges with Contract Guards and Risk Assessments at Federal Facilities., GAO-14-235T, December 17, 2013, p. 2, at http://www.gao.gov/assets/660/659744.pdf.

[22] U.S. Government Accountability Office, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, GAO-14-86, March 2014, p. 1, at http://www.gao.gov/assets/670/661348.pdf.

[23] Ibid.

[24] U.S. Government Accountability Office, *Federal Facilities: Selected Facilities' Emergency Plans Generally Reflect Federal Guidance*, GAO-14-101, October 2013, pp. 19-20, at http://www.gao.gov/assets/660/658554.pdf.