Congressional Research Service
Informing the legislative debate since 1914

Federal Building and Facility Security: Frequently Asked Questions

Updated January 27, 2021

Congressional Research Service
https://crsreports.congress.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. The approach to federal building and facility security is decentralized and numerous federal entities are involved. The federal government is tasked with securing over 113,000 buildings or facilities daily.

The recent breach of U.S. Capitol security on January 6, 2021, has refocused the federal government's attention on building security activities. This renewed attention has raised a number of frequently asked questions. This report answers the six most common questions regarding federal building and facility security:

- 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?

Currently, Congress and federal law enforcement entities are conducting investigations into the breach of the U.S. Capitol security on January 6, 2021. Congress has previously taken an interest in federal facility security following the September 2001 terrorist attacks, the September 2013 Washington Navy Yard shootings, and the April 2014 Fort Hood shootings.

Contents

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 as well as the public. The approach to federal building and facility security is decentralized and involves numerous federal entities across all three branches of government. Further, some buildings or facilities are occupied by and fall under the jurisdiction of multiple federal agencies. In total, the federal government secures over approximately 113,000 executive branch, nonmilitary federal buildings.[1]

Prior to the April 19, 1995, bombing of the Alfred P. Murrah Building in Oklahoma City, the federal government had no consistent 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 and 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 and proposed minimum security standards for federal facilities. Additionally, USMS deputies and General Services Administration (GSA) security specialists conducted inspections of more than 1,200 federal facilities to determine the cost and feasibility of the potential security upgrades that would be required to comply with the proposed minimum standards. The results were published in the *Vulnerability Assessment of Federal Facilities* report.[2] 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.[3]

The recent breach of U.S. Capitol security on January 6, 2021, has again renewed the federal government's interest in building security activities. Federal law enforcement agencies are currently conducting an investigation of the breach, and some Members of Congress are calling for a congressional investigation.[4] Congressional interest in the events of January 6, 2021, have parallels to congressional interest in past federal security incidents, including the September 2001 terrorist attacks, the September 2013 Washington Navy Yard shootings, and the April 2014 Fort Hood shootings. In the wake of these incidents, Congress held hearings to review and evaluate the protection of federal facilities. 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

[1] Federal Real Property Council, *FY2015 Federal Real Property Report* (the most recent report available.) The figure provided excludes military assets. In recent work, the U.S. Government Accountability Office (GAO) assessed the reliability of the *Federal Real Property Report's* data and found problems with data collection practices. However, it found the data to be reliable for the purposes of providing a broad overview of the makeup of the government's federal real property portfolio. See GAO, *Federal Real Property: Improving Data Transparency and Expanding the National Strategy Could Help Address Long-standing Challenges*, GAO-16-275 (Washington, DC: March 31, 2016); and GAO, *Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*, GAO-13-222 (Washington, DC: January 24, 2013). For more information on federal real property, see CRS Report R46594, *Federal Real Property Data: Limitations and Implications for Oversight*, by Garrett Hatch and Carol Wilson.

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

[3] 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.

[4] Rep. Ayanna Pressley, "Pressley Calls for Congressional Investigation into Domestic Terrorist Attack on U.S. Capitol," press release, January 7, 2021, https://pressley.house.gov/media/press-releases/pressley-calls-congressional-investigations-domestic-terrorist-attack-us.

Committee held a hearing on "The Navy Yard Tragedy: Examining Physical Security for Federal Facilities."

Renewed attention to federal security raises a number of frequently asked questions. This report answers the six most common questions regarding federal building and facility security:

- 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 a facility, employees, and the visiting public to criminal and terrorist threats. Each federal facility has unique attributes that affect its individual security needs and the missions of the federal tenants. In 1995, following the Oklahoma City Bombing, USMS created five categories to classify federal facilities by security level, which are still used today. They are

- 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).[5]

A building's security level determines which security activities and operations need to be established and maintained to secure the facilities.

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

Security operations at these federal facilities may include the following:

- all-hazards risk assessments;
- 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 plans;
- emergency and safety training programs; and
- proactive gathering and analysis of terrorist and criminal threat intelligence.

Who is responsible for federal facility security?

Approximately 30 federal law enforcement agencies provide security for 45% of federal facilities and their occupants. The remaining 55% of federal facilities are owned and occupied by military, intelligence, and national security entities with their own facility security force such as the Pentagon's uniformed police.[6]

Examples of the federal law enforcement entities responsible for facility security include the following:

- U.S. Department of Health and Human Services' National Institutes of Health (NIH), Division of Police—Officers provide law enforcement and security services for NIH facilities;
- U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA), Security Branch—Officers are responsible for the protection of FEMA facilities, personnel, resources, and information; and
- National Aeronautics and Space Administration (NASA), Protective Services—Officers provide law enforcement and security services for NASA's 14 centers located throughout the United States.[7]

According to the Department of Justice's Office of Justice Programs (OJP), 2% of full-time federal law enforcement officers' primary function is security/protection. OJP states that there were 132,110 federal law enforcement officers in 2016 and, of those, 2,645 officers had security/protection as their primary function.[8] The security/protection function includes duties primarily related to providing security for federal buildings, courts, records, assets, or other property, or to providing personal protection for federal government officials, judges, prosecutors, jurors, foreign dignitaries, or any other designated persons.[9] Some federal law enforcement agencies do not stand post at federal facilities, but instead train, inspect, and monitor private

[6] U.S. Government Accountability Office (GAO), *Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk*, GAO-18-72, October 2017, p. 1, https://www.gao.gov/products/GAO-18-72.

[7] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, "Federal Law Enforcement Officers, 2008," NCJ 238250, June 2012, at http://www.bjs.gov/content/pub/pdf/fleo08.pdf. For more information on law enforcement data, see https://www.bjs.gov/index.cfm?ty=pbdetail&iid=6708, including a 2019 update with data through 2016, available at https://www.bjs.gov/content/pub/pdf/fleo16st.pdf.

[8] Department of Justice, Office of Justice Programs, *Federal Law Enforcement Officers, 2016 - Statistical Tables*, 2016, p. 6, https://www.bjs.gov/content/pub/pdf/fleo16st.pdf. This is the most recent OJP statistical data on federal law enforcement officers.

[9] Ibid., p. 11.

security guard companies. These companies provide personnel that occupy security checkpoints and patrol federal facilities.

Is there a national standard for federal facility security?

No single security standard applies to every federal facility, primarily because of the large number and different types of federal facilities. An interagency committee, however, is responsible for setting a number of standards to address the breadth of federal facility security needs. The Interagency Security Committee's (ISC's) 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" helps centralize efforts to secure federal facilities.[10] GSA chaired the ISC until the enactment of the Homeland Security Act in 2002 and the establishment of the Department of Homeland Security (DHS), at which time DHS assumed the chair.[11] ISC membership consists of over 100 senior-level executives from 53 federal agencies and departments.[12]

The federal agency and department executive members of the ISC, through working groups, have developed and issued federal facility policies and standards, including the following:

- *The Risk Management Process for Federal Facilities* (2019);
- *The Risk Management Process: An Interagency Security Committee Standard* (November 2016);
- *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide* (November 2015); and
- *Items Prohibited from Federal Facilities: An Interagency Committee Standard* (February 2013).[13]

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

- *Protecting Against the Threat of Unmanned Aircraft Systems: An Interagency Security Committee Best Practice* (2020);
- *Facility Access Control: An Interagency Security Committee Best Practice* (2020);
- *Armed Contract Security Officers in Federal Facilities: An Interagency Security Committee Best Practice* (2019);
- *Violence in the Federal Workplace: A Guide for Prevention and Response* (2019);
- *REAL ID Act of 2005 Implementation: An Interagency Security Guide* (2019);

[10] Department of Justice, Office of Justice Programs, *Federal Law Enforcement Officers, 2016 - Statistical Tables*, 2016, p. 6, https://www.bjs.gov/content/pub/pdf/fleo16st.pdf. This is the most recent OJP statistical data on federal law enforcement officers.

[11] Ibid., p. 11.

[12] Ibid.

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

- *Security Specialist Competencies: An Interagency Security Committee Guide* (January 2017);
- *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (December 2015);
- *Best Practices and Key Considerations for Enhancing Federal Facility Security and Resilience to Climate-Related Hazards* (December 2015);
- *Facility Security Plan: An Interagency Security Committee Guide* (February 2015);
- *Best Practices for Working with Lessors: An Interagency Security Committee Guide* (November 2014); and
- *Occupant Emergency Programs: An Interagency Security Committee Guide* (March 2013).[14]

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

Federal facilities, employees, and the visiting public face a variety of threats, including assault, illegal weapon and explosive possession, robbery, riots, civil disturbances, homicide, and arson. An example of a threat to a federal building is the shooting at the Washington Navy Yard facility on September 16, 2013. As a result, the Department of Defense (DOD) investigated and adjusted the Navy Yard's security operations.[15] The occupation of a federal wildlife refuge in Oregon for 40 days by armed private citizens in 2016 constituted a similar threat.

Security of federal facilities is as diverse as the number of law enforcement agencies securing them due a facility's security level rating, location, and known threats. One law enforcement agency may secure individual facilities under their purview differently based on specific security needs and threats. The diversity of security concerns and conditions makes the collection of official and comprehensive data on threats to or incidents occurring at federal facilities challenging.

How is threat information communicated among federal facility security stakeholders?

Prior to 2009, the Department of Homeland Security Advisory System (HSAS) was used to communicate homeland security threats, including domestic and international terrorism. In 2009,

[14] Ibid.

[15] 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.

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 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 homeland security and federal facility security activities among DHS, governors, homeland security advisors, law enforcement entities, and critical infrastructure operators. Information on domestic incidents is shared with federal, state, and local Emergency Operations Centers 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. For example, 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 were 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 periodically 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.

[16] The task force's report and recommendations are available at U.S. Department of Homeland Security, Homeland Security Advisory Council, *Homeland Security Advisory System Task Force Report and Recommendations*, September 2009, at http://www.dhs.gov/xlibrary/assets/hsac_task_force_report_09.pdf.

[17] U.S. Department of Homeland Security, "National Terrorism Advisory System (NTAS)," at http://www.dhs.gov/files/programs/ntas.shtm.

[18] U.S. Department of Homeland Security, "Office of Operations Coordination," at 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, DC: GPO, 2007).

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

Federal facility security is an issue for all three branches of the government and every federal department and agency. Congress is generally interested in federal facility security issues and conducts oversight through the House Homeland Security and Senate Homeland Security & Government Affairs Committees. In a 2017 report, the Government Accountability Office (GAO) stated that government facilities and their employees continue to be targets of potential harm.[20] Additionally, GAO stated that it is important for federal agencies to use risk-based methodologies to assess the physical security of the approximately 113,000 executive branch, nonmilitary federal buildings.[21]

In the wake of the January 6, 2021, breach of the U.S. Capitol's security, another issue Congress may choose to address is the development and implementation of federal facility emergency plans. In the above-mentioned report, GAO found that although selected federal facilities' emergency plans generally reflect federal guidance, these agencies still have issues with assessing and monitoring such threats, for example, as domestic terrorism. Finally, Congress may wish to address how federal law enforcement agencies coordinate their response to attacks at and on federal facilities.

These issues, and others, were initially caused by the 1995 bombing of the Alfred P. Murrah building. Since then, efforts have been made to improve the protection of federal facilities by establishing security standards, improving information sharing, and assessing and monitoring threats. However, incidents such as the January 6, 2021, breach of the U.S. Capitol's security; the September 2001 attacks on the Pentagon; and the shootings at the U.S. Navy Yard and Fort Hood, TX, indicate that issues remain.

Author Information

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy

[20] U.S. Government Accountability Office (GAO), *Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk*, GAO-18-72, 2017, p. 1, https://www.gao.gov/products/GAO-18-72.

[21] Federal Real Property Council, *FY2015 Federal Real Property Report* (the most recent report available.) The figure provided excludes military assets. In recent work, GAO assessed the reliability of the *Federal Real Property Report's* data and found problems with data collection practices. However, it found the data to be reliable for the purposes of providing a broad overview of the makeup of the government's federal real property portfolio. See GAO, *Federal Real Property: Improving Data Transparency and Expanding the National Strategy Could Help Address Long-standing Challenges*, GAO-16-275 (Washington, DC: March 31, 2016); and GAO, *Facility Security: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies*, GAO-13-222 (Washington, DC: January 24, 2013).

Disclaimer