Congressional Research Service
Informing the legislative debate since 1914

Protection of Classified Information by Congress: Current Practices

Updated May 29, 2026

Congressional Research Service
https://crsreports.congress.gov
RS20748

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The protection of classified national security and other controlled information is of concern to both the executive branch—which, for the most part, determines what information is classified and controlled—and Congress. The legislature uses such information to fulfill its constitutional responsibilities, particularly overseeing the executive, appropriating funds, and legislating public policy. Congress has established numerous mechanisms to safeguard controlled information in its custody, although these arrangements have varied over time, between the two chambers, and among offices in each. Both chambers, for instance, have created offices of security to consolidate relevant responsibilities. In addition, each chamber maintains its own security manual that establishes the policies for safeguarding information in the chamber's possession and the procedures for granting its staff access to classified materials. Other differences exist at the committee level, regarding the availability and use of information in committees' custody. Further, each chamber of Congress has cybersecurity and other protective policies to secure its communication and information systems from unauthorized access, use, or disruption.

Contents

Contacts

Current Practices and Procedures

Congress relies on a variety of mechanisms, instruments, and procedures to protect classified national security and other sensitive information in its custody.[1] Such information—most of which comes from the executive branch—can be hard for Congress to obtain. But accessibility to it is seen as necessary for the legislature to carry out its constitutional responsibilities, especially overseeing the executive and conducting the legislative process.

The safeguards surrounding this information deal with who is eligible for access, what information is made available and in what form, where and when it can be accessed, and how and in what circumstances or contexts it can be used afterward. The relevant requirements and mechanisms include

- House and Senate security offices responsible for setting and implementing standards for safeguarding classified information;
- committee rules determining access to committee-held classified information, including what is made available and to whom, as well as how and under what conditions;
- committee and certain chamber rules governing how classified information can be used afterward, in what contexts and forums, and under what conditions;
- establishment of special congressional groups to receive highly sensitive classified information;
- security clearances for congressional staff;
- a secrecy oath required for all Members and employees of the House; and
- formal procedures for investigating suspected security violations.

House and Senate rules and committee rules—as well as custom and practice, including informal agreements between legislators and executive officials—constitute the bases for these requirements and arrangements.[2] Some of these have evolved over time, in response to changing conditions and needs of both the legislative and executive branches.[3]

---

[1] Classification of national security information (and eligibility for access to it in the executive branch) is governed by executive orders, public laws, and administrative directives. For coverage of this issue, see CRS In Focus IF12318, *Rules and Statutes Relevant to Safeguarding Classified Materials*, by Jennifer K. Elsea and Andreas Kuersten; CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea; CRS In Focus IF12183, *Procedures for Declassifying Intelligence of Public Interest*, by Michael E. DeVine; CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by Michelle D. Christensen; and CRS In Focus IF12836, *Presidential Transitions: Security Clearance Background Investigations*, by Michelle D. Christensen.

[2] For a brief summary of congressional access to classified and controlled unclassified materials, see CRS Report RL30240, *Congressional Oversight Manual*, coordinated by Ben Wilhelm, Todd Garvey, and Christopher M. Davis, section titled "Classified Material."

[3] For further background on the protection and oversight of classified information by Congress, see Frederick M. Kaiser, "Congressional Rules and Conflict Resolution: Access to Information in the House Select Committee on Intelligence," *Congress and the Presidency*, vol. 15 (1988), pp. 49-73; House Select Committee on Intelligence, *Report on Intelligence Oversight Act of 1980*, 96th Cong., 2nd sess. H.Rept. 96-730 (1980); U.S. Commission on Protecting and Reducing Government Secrecy, *Secrecy: Report of the Commission* (1997); House Committee on Government Operations, Subcommittee on Legislation and National Security, *Congress and the Administration's Secrecy Pledges*, hearings, 100th Cong., 2nd sess. (1988); House Permanent Select Committee on Intelligence, *United States Counterintelligence and Security Concerns—1986*, 100th Cong., 1st sess., H. Rept. 100-5 (1987), pp. 3-4; Joint Committee on the Organization of Congress, *Committee Structure*, hearings, 103rd Cong., 1st sess. (1993), pp. 64-79, 312-316, 406-417, and 832-841; Senate Select Committee on Intelligence, *Meeting the Espionage Challenge*, S. Rept. (continued...)

House and Senate Offices of Security and Security Manuals

Senate

In 1987, the Senate established the Office of Senate Security (OSS) as the result of a bipartisan effort over two Congresses.[4] Located in the Office of the Secretary of the Senate, the Security Office sets and implements uniform standards for handling and safeguarding classified and other sensitive information in the Senate's possession. The Security Office's standards, procedures, and requirements—detailed in its *Senate Security Manual*, first issued in 1988 and revised in November 2020—"are binding upon all employees of the Senate."[5]

The *Senate Security Manual* "establishes requirements for safeguarding classified information in the possession of the Senate, its offices and its employees."[6] The requirements extend to a wide range of matters on safeguarding classified information: physical security requirements, procedures for storing materials, and mechanisms for protecting communications equipment.

OSS is also charged with personnel security, and the *Senate Security Manual* details the procedures and requirements for security clearances and nondisclosure agreements of all Senate staff needing access as well as the procedures for follow-up investigations of suspected security violations by employees. These procedures cover committee and Senate office staff and officers of the Senate as well as consultants and contract personnel.

House

In 2005, the House put its own security office in place—the Office of House Security (OHS)—under the jurisdiction of the House Sergeant at Arms, following approval of the Committee on House Administration.[7] The office is charged with developing an Operations Security Program for the House. Its responsibilities and jurisdiction encompass processing security clearances for staff, handling and storing classified information, managing a counterintelligence program for the House, and coordinating security breach investigations.[8] OHS's guidelines and procedures are outlined in the *House Security Policy Manual*.[9]

99-522, 99th Cong., 2nd sess. (1986), pp. 90-95; Office of the Director of National Intelligence (ODNI), *Reporting of Intelligence Activities to Congress*, Intelligence Community Policy Memorandum Number 2005-100-3 (January 10, 2006); and ODNI *Reforming Intelligence: The Passage of the Intelligence Reform and Terrorism Prevention Act* (2008).

[4] *Congressional Record*, vol. 133 (July 1, 1987), pp. 18506-18507. The resolution creating the new office (S.Res. 243, 100th Cong.) was introduced and approved on the same day.

[5] U.S. Senate, Office of Senate Security (OSS), *United States Senate Security Manual* (revised November 2020), p. 1 (hereinafter *Senate Security Manual*).

[6] *Senate Security Manual*, p. 1.

[7] The request and approval of the Office of House Security (OHS) occurred through two letters. These letters—one requesting an Operations Security Program under the direction of the House Sergeant at Arms and the other granting approval—are, respectively, to the chairman of the House Committee on House Administration, from the House Sergeant at Arms, February 25, 2003, and to the House Sergeant at Arms, from the chairman of the House Committee on House Administration, March 28, 2003.

[8] These are derived from its establishing authority (see footnote 7). For additional information on OHS operations, see House Office of the Sergeant at Arms, OHS, "House Security," http://saa.house.gov/ohs (accessible only to congressional clients), and House Office of the Sergeant at Arms, OHS, "Security Clearances," https://saa.house.gov/security-clearances.

[9] U.S. House, House Sergeant at Arms, *House Security Policy Manual* (revised October 2017) (hereinafter *House Security Policy Manual*).

Applicable to all House committees and Member offices, the *House Security Policy Manual* "establishes recommendations for safeguarding classified information in the possession of the House, its offices, and its employees."[10] The *House Security Policy Manual* provides uniform guidelines, security requirements, and other safeguards for the storage and overall protection of classified information.[11] In addition, the *House Security Policy Manual* outlines the instructions, forms, and requirements for security clearances, which are applicable to all committee and Member staff whose assigned duties require access to classified materials, including consultants, fellows, detailees, and contractors.[12]

Security Clearances for Staff

In general, the scope of House and Senate policies includes staff access to classified information that originated in the executive branch, as well as material generated internally that contains classified information.[13]

The level at which a specific piece of information is classified (i.e., Confidential, Secret, or Top Secret) is determined by the originating agency or agencies. Each category of information requires its own level of protection, which corresponds to the risk to national security for unauthorized disclosure. The three levels of classification, in ascending order, are

- *Confidential*, the unauthorized disclosure of which would "cause damage to the national security";
- *Secret*, the unauthorized disclosure of which would "cause serious damage to the national security"; and
- *Top Secret*, the unauthorized disclosure of which would "cause exceptionally grave damage to the national security."[14]

Although there is no across-the-board, comprehensive requirement for all legislative branch staff to hold a security clearance, staff are generally required to have a security clearance and sign a written nondisclosure agreement to gain access to classified information.[15] These exist through various mechanisms, which apply to different employee categories, as detailed below.

House and Senate Member Office Staff

Individual Member offices may on their own require both clearances and nondisclosure agreements for staff to be eligible for access to classified information. Even so, requirements and limitations are directed by each chamber's office of security.[16] For example, limits are typically imposed on the number of personal staff members with clearances in any individual Member or

[10] *House Security Policy Manual*, p. 4.

[11] *House Security Policy Manual*, p. 2. Individual Member offices and House committees may supplement these procedures and security requirements with additional security practices, such as those found in Intelligence Community Directives (ICDs), Policy Guidance, and Technical Specifications, at https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

[12] *House Security Policy Manual*, pp.15-23.

[13] *House Security Policy Manual*; *Senate Security Manual*.

[14] Executive Order 13526 of December 29, 2009, "Classified National Security Information," 75 *Federal Register* 707, January 5, 2010.

[15] The levels of security clearances correspond to the levels of sensitivity of the information that cleared individuals will be eligible to access. For additional information, see CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by Michelle D. Christensen.

[16] *House Security Policy Manual*; *Senate Security Manual*; and OHS, "Security Clearances."

Senate office. Along with this, congressional offices may on their own require a "need to know" for individual staff members seeking access to certain classified information.

Clearances for Representatives' Staff[17]

- House Members determine which positions require security clearances. Each Member of the House shall have no more than two cleared staff.[18] House policy is for staff clearances to be kept to "the absolute minimum required for the conduct of official House business."[19]
- Requests for individual staff clearances must originate from the employing House Member and should be submitted on official letterhead to the House Sergeant at Arms.
- Requests for staff clearances will not be processed during the last year of a retiring Member's term in office.
- Member office staff, including staff shared between a committee and a Member, may not obtain or hold a clearance with access to Sensitive Compartmented Information (SCI).
- House staff are not eligible for interim clearances.

Clearances for Senators' Personal Staff[20]

- Senators determine which positions require security clearances. Each Senator shall have no more than two cleared staff members. Additionally, each Senator shall have no more than one executive branch fellow or detailee who holds a clearance with their employing agency and one cleared system administrator. Senate policy is for staff clearances to be kept to "the absolute minimum required for the conduct of official Senate business."[21]
- Requests for individual staff clearances must originate from the employing Senator and be submitted, in writing, to the Director of Senate Security.
- Senators on the following committees and subcommittee are allowed one additional cleared personal staff member: (1) Armed Services, (2) Foreign Relations, (3) Homeland Security and Governmental Affairs, (4) Appropriations Subcommittee on Department of Defense, and (5) Appropriations Subcommittee on State, Foreign Operations, and Related Programs.
- Senators may request a waiver of these limitations from the Senate majority or minority leader.

[17] *House Security Policy Manual*, pp. 15-23; OHS, "Security Clearances."

[18] A recent proposal (H.Res. 46, 119th Cong.) would exclude from the allotment any employee who is a member of the Armed Forces who holds a security clearance issued by the Department of Defense (DOD) if they are an employee of one of the following House committees or appropriations subcommittees: (1) Armed Services; (2) Foreign Affairs; (3) Homeland Security; (3) Permanent Select Committee on Intelligence; (4) Appropriations Subcommittee on Defense; (5) Homeland Security; (6) State, Foreign Operations, and Related Programs.

[19] *House Security Policy Manual*, p. 15.

[20] *Senate Security Manual*, pp. 10-19.

[21] *Senate Security Manual*, p. 11.

House and Senate Committee Staff[22]

Each committee typically spells out requirements in its rules to cover access.[23] In general, both OSS and OHS require employees, including committee staff, who need access to classified information[24] to hold the appropriate-level security clearance.[25]

Clearances for House Committee Staff[26]

- The House committee chair is responsible for determining which positions require security clearances.
- To be eligible for a clearance, staff must be employed by the committee sponsoring the clearance, and requests must originate from the committee chair.
- Staff shared between a committee and a Member's personal office are considered personal staff for the purpose of security clearance limitations.

Clearances for Senate Committee Staff[27]

- The Senate committee chair is responsible for determining which positions require security clearances.
- Requests for Senate committee clearances must originate from the committee chair.
- Staff shared between a committee and a Senator's personal office are considered personal staff for the purpose of security clearance limitations.

Legislative Branch Support Agencies

Security clearance requirements are included in the personnel manuals and some job and position descriptions or vacancy announcements of Congress's support agencies: Congressional Budget Office (CBO), Congressional Research Service (CRS), Library of Congress (LOC), and Government Accountability Office (GAO).[28]

[22] *House Security Policy Manual*, pp. 15-23; OHS, "Security Clearances"; *Senate Security Manual*, pp. 10-19.

[23] For examples, see U.S. House Permanent Select Committee on Intelligence, *Rules of the Permanent Select Committee on Intelligence*, 119th Cong., Rules 12(b), 12(c), and 13(c); and U.S. Senate Select Committee on Intelligence, *Rules of Procedure*, 119th Cong., Rules 9.6, 10.1, 10.2, 10.8, and 10.10.

[24] The *House Security Policy Manual* applies to "information retained by the House that is classified in accordance with Executive Orders 13526 and 12333 as amended and the Atomic Energy Act of 1954." The manual notes that certain Controlled Unclassified Information (CUI) markings (e.g., "For Official Use Only" and "Law Enforcement Sensitive") are document designations rather than classifications. While unclassified, such information may not be appropriate for public release or passed over unencrypted communication lines. Similarly, the *Senate Security Manual* defines *classified information* as "official information, including foreign classified information, which has been determined, pursuant to statute or executive order, to require protection in the interests of national security." *House Security Manual*, p. 6; *Senate Security Manual*, p. 21.

[25] *Senate Security Manual*, pp. 10-11, 14; *House Security Policy Manual*, pp. 15-23; and OHS, "Security Clearances."

[26] *House Security Policy Manual*, pp. 15-23.

[27] *Senate Security Manual*, pp. 10-19.

[28] For example, see "LCR 10-200-Personnel Security" at Library of Congress, LC Regulations and Directives, https://staff.loc.gov/sites/rules-and-regulations.

Secrecy Oaths for Members and Staff

Senate

Neither the Senate nor its committees impose a secrecy oath or an affirmation on their Members.[29] However, a nondisclosure agreement must be executed by all Senate staff who are granted a security clearance.[30] Similarly, prior to obtaining access to classified materials, staff of the Senate Select Committee on Intelligence must agree in writing and under oath to be bound by Senate rules.[31]

House

Beginning with the 104th Congress, the House has required a secrecy oath (taken once per Congress) for each Member, Delegate, Resident Commissioner, officer, and employee of the chamber. Before any such person may have access to classified information, he or she must take the following oath:

> I do solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its Rules.[32]

Particular committees may require separate oaths. The House Committee on Homeland Security requires an oath or affirmation from each committee or staff member seeking access to classified information, modeled after one adopted by the House Permanent Select Committee on Intelligence.[33]

Sharing Committee-Held Information with Non-Committee Members

Procedures controlling access to classified information held by congressional offices exist throughout Congress. Although these differ, committee and chamber rules set conditions and requirements for sharing such information with other panels, Members, and staff.[34] This may include determining

- who may attend a panel's executive (or secret) session hearings;
- who is eligible for access to a committee's classified holdings;
- what information may be made available to all Members across the board;

[29] An earlier attempt to mandate such an oath for all Members and employees—of both chambers of Congress—seeking access to classified information arose in 1993, but it was unsuccessful. *Congressional Record*, daily edition, vol. 139 (August 4, 1993), pp. H5770-H5773; and *Congressional Record*, daily edition, vol. 139 (November 18, 1993), p. H10157.

[30] *Senate Security Manual*, p. 14.

[31] Senate Select Committee on Intelligence, 119th Cong., *Rules of Procedure, Appendix A—S. Res. 400, 94th Cong., 2nd Sess. (1976) as amended*.

[32] House Rule XXIII, cl. 13, 119th Cong. Copies of the oath or affirmation are retained by the Clerk of the House as part of the records of the House.

[33] House Committee on Homeland Security, *Committee Rules*, 119th Cong., Rule XIV(E).

[34] For further discussion, see the citations in footnote 2; *Senate Security Manual*, pp. 10-11, 14; *House Security Policy Manual*, p. 17; and OHS, "Security Clearances."

- what information covers (e.g., subject matter) and who has a need to know this information;
- how to deliver information (e.g., the actual documents, a portion of the documents, a summary, or a briefing), where to deliver it (in the committee offices or in a secure area elsewhere), and under what, if any, restrictions (e.g., with or without staff).

The current rules of the House Permanent Select Committee on Intelligence are based on the committee's 1977 establishing authority and reinforced by intelligence oversight provisions in public law, such as the 1991 Intelligence Authorization Act.[35] The committee's controls apply to select committee members sharing classified information outside the committee itself as well as to non-committee Representatives seeking permission to attend closed hearings and briefings.[36] In such cases, access is granted by the chair in consultation with the ranking member. In the case of admission to closed hearings or briefings, access may be conditional on reciprocal admission of intelligence committee Members and staff to classified hearings and briefings of the requesting committee (e.g., Appropriations, Armed Services). Additionally, it is possible for a non-committee member to be denied attendance at its executive sessions or access to its classified holdings, given only a briefing on it, granted partial access, or allowed full access. The select committee also sets rules on whether the Member may be accompanied by cleared staff or may take notes. When the House Permanent Select Committee on Intelligence releases classified information to another committee or non-member, moreover, the recipient must comply with the same rules and procedures that govern the intelligence committee's control and disclosure requirements.[37] Finally, access to non-committee and staff members may be limited at the request of the executive branch.[38]

By comparison, rules of the House Armed Services Committee are to

> ensure access to [classified] information by any member of the Committee or any other Member, Delegate, or Resident Commissioner of the House of Representatives, staff of the Committee, or staff designated under rule 9(c) who have the appropriate security clearances and the need to know, who has requested the opportunity to review such material.[39]

The rules of the Senate Select Committee on Intelligence provide that whenever classified materials are made available to another committee of the Senate or to any Senator who is not a member of the committee,

> such material shall be accompanied by a verbal or written notice to the recipients advising of their responsibility to protect such materials pursuant to section 8 of S. Res. 400 of the 94th Congress, as amended. The Security Director of the Committee shall ensure that such notice is provided and shall maintain a written record identifying the particular information transmitted and the committee or members of the Senate receiving such information.[40]

[35] H.Res. 658, 95th Cong.; and P.L. 102-88, 105 Stat. 441.

[36] House Permanent Select Committee on Intelligence, 119th Cong., Rule 14(A)-(C).

[37] House Permanent Select Committee on Intelligence, 119th Cong., Rule 14(A)-(C), Rule 14(F).

[38] House Permanent Select Committee on Intelligence, 119th Cong., Rule 14(J).

[39] House Committee on Armed Services, *Rules of the Committee*, 119th Cong., Rule 20(b). Under Rule 9(c), designated staff are defined as "one member of [each committee member's] personal staff, and an alternate, which may include fellows, with Top Secret security clearance."

[40] Senate Select Committee on Intelligence, *Rules of Procedure*, 119th Cong., Rule 9.5.

Notification to Special Groups: The "Gang of Eight" and "Four Corners"[41]

Executive branch notification about intelligence activities, including presidential findings regarding covert operations, is usually provided directly to the House and Senate select committees on intelligence.

These full panels may be bypassed—to address the urgency of a situation, to meet extraordinary circumstances affecting the vital interests of the United States, or to protect the extremely sensitive nature of the information—in favor of notification to the "Gang of Eight" or "Four Corners."[42] Notification about covert operations, in certain situations, is submitted to the statute-based Gang of Eight, composed of the Speaker and minority leader of the House, chair and ranking minority member of the House intelligence committee, majority and minority leaders of the Senate, and chair and vice chair of the Senate intelligence committee.[43] Alternatively, the executive branch may, as a matter of custom, notify the Four Corners of particularly sensitive intelligence activities (other than covert operations), which, if disclosed, might reveal intelligence sources and methods.[44] This non-statutory body is composed of the chairs and ranking minority members of the House and Senate intelligence committees.[45]

Investigation of Security Breaches

The Senate Office of Security and the House Office of the Sergeant at Arms are charged with investigating or coordinating investigations of suspected security violations by employees. The House and Senate security manuals spell out the potential investigative procedures and penalties for violations of congressional security requirements.[46] Administrative penalties in the House range in severity from a written reprimand to revocation of clearance and termination of employment.[47] Further, House Rule X authorizes the Ethics Committee to investigate certain unauthorized disclosures of intelligence-related information, including those by a Member or Delegate, and "report to the House concerning any allegation that it finds to be substantiated."[48]

In the Senate, "known, suspected or alleged security violations" are investigated by OSS.[49] If OSS determines that the violation was unintentional, it will either (1) recommend an administrative penalty to the staff's employing Senator or committee or (2) refer the matter to the Select Committee on Ethics.[50] The administrative penalties for unintentional violations might

[41] Also referred to as the "Gang of Four."

[42] For coverage of these select groups and related matters, see CRS Report R45191, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements*, by Michael E. DeVine.

[43] 50 U.S.C. §3093(c)(2).

[44] Additionally, the executive branch may notify the Four Corners of more routine, but nevertheless sensitive, intelligence.

[45] While the Four Corners is a non-statutory body, in certain cases, notification to it may satisfy reporting requirements under 50 U.S.C. §3092(a).

[46] *House Security Policy Manual*, pp. 19-23; *Senate Security Manual*, pp. 14-15.

[47] *House Security Policy Manual*, pp. 19-22. Violations are investigated by the House Sergeant at Arms; penalties are typically imposed by the individual's employing Member or committee chair.

[48] House Rule X, cl. 11(g)(4), 119th Cong.; House Committee on Ethics, *Rules of the Committee on Ethics*, 119th Cong., Rule 14(b).

[49] *Senate Security Manual*, p. 14.

[50] *Senate Security Manual*, p. 15.

range from written reprimands and security briefings to revocation of clearance and termination of employment.[51]

The Senate Committee on Ethics has the broad duty to "receive complaints and investigate allegations of improper conduct which may reflect upon the Senate, violations of law, violations of the Senate Code of Official Conduct, and violations of rules and regulations of the Senate."[52] The panel is also directed "to investigate any unauthorized disclosure of intelligence information [from the Senate Select Committee on Intelligence] by a Member, officer or employee of the Senate."[53]

Cybersecurity and Other Protective Measures

In addition to the foregoing, the House and Senate subscribe to measures designed to protect classified and controlled information. Some of these focus on the physical security of documents and facilities, while others affect individual conduct.

House and Senate cleared staff are required to undergo a security briefing prior to obtaining access to classified materials.[54] Additionally, staff are required to undergo annual "refresher" briefings, foreign travel briefings, and routine counterintelligence briefings.[55]

Cybersecurity

Each chamber has implemented policies to protect its communication and information systems from unauthorized access, use, or disruption. OHS is responsible for establishing guidance for the possession and transmission of classified information. For example, OHS and the U.S. Capitol Police Technical Security Counter Measures team can assist with communications security, including the establishment of secure spaces for classified briefings, and security sweeps prior to sensitive meetings.[56]

OSS is responsible for approving equipment used for the transmission of classified information. Senate policy prohibits discussion or transmission of classified information over open phone lines or personal computer systems.[57] Classified information should not be discussed in a personal office if a secure location is available, and information higher than Secret may never be discussed in personal offices. Secure spaces may be obtained through OSS.[58]

OSS also provides guidance for staff on email and password security, social media security, and telework best practices, as well as tips for recognizing malicious online activity (e.g., spear phishing, adware).[59]

[51] *Senate Security Manual*, p. 15. If the OSS determines that the violation was intentional, it may refer the matter to the Select Committee on Ethics and/or the Department of Justice.

[52] S.Res. 338, 88th Cong.

[53] S.Res. 400, 94th Cong.

[54] *Senate Security Manual*, pp. 15-16; *House Security Policy Manual*, p. 20.

[55] *Senate Security Manual*, pp. 16; *House Security Policy Manual*, pp. 20-21.

[56] *House Security Policy Manual*, pp. 9-14; OHS, "House Security," https://saa.house.gov/ohs.

[57] *Senate Security Manual*, pp. 9-10.

[58] *Senate Security Manual*, p. 9.

[59] *Senate Security Manual*, pp. 19-20.

Physical Security and Other Protective Measures

The House and Senate have each adopted protective measures to ensure the physical safety of classified materials stored by Congress. In the Senate, materials classified at the Secret and Confidential levels may be stored in a container or vault approved and certified by the General Services Administration (GSA).[60] Top Secret and Special Access materials are to be stored in either a container approved and certified by GSA or a class-A vault constructed in accordance with applicable Department of Defense requirements.[61] (The Department of Defense is now "using a secondary Department of War designation," under Executive Order 14347 of September 5, 2025.) These materials are also subject to supplementary controls, including greater restrictions on access to and supervision of containers.[62] Top Secret and Special Access material may not be stored in Senators' personal offices.[63]

In the House, classified materials are to be stored in GSA approved containers or under "direct surveillance of an authorized person" at all times.[64] Top Secret and Special Access materials are to be stored in a safe approved and certified by GSA or in a class-A vault constructed in accordance with applicable Department of Defense requirements.[65] Top Secret and Special Access materials are also subject to supplementary controls, including greater restrictions on access and protection by intrusion detection systems.[66] Under the *House Security Policy Manual*, Top Secret and Special Access material may be stored only in a room that has been certified as a sensitive compartmented information facility (SCIF) in accordance with Intelligence Community Directive 705.[67]

Other physical and protective measures include

- stationing U.S. Capitol Police officers throughout the Capitol complex, including at committee sites and areas where sensitive information is used;
- setting up procedures to acknowledge and document the receipt of specific classified information and its dissemination to particular individuals;
- conducting education and training programs; and
- reporting foreign travel and foreign national contacts.

[60] *Senate Security Manual*, p. 6.

[61] *Senate Security Manual*, p. 6; DOD Manual 5200.01, Vol. 3, *DoD Information Security Program: Protection of Classified Information*, "Enclosure 3 – Storage and Destruction," January 17, 2025, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001_p.PDF; and DOD Instruction 5220.31, *National Industrial Security Program*, May 9, 2023.

[62] *Senate Security Manual*, p. 6; DOD Manual 5200.01, Vol. 3, *DoD Information Security Program: Protection of Classified Information*, "Enclosure 3 – Storage and Destruction," January 17, 2025.

[63] *Senate Security Manual*, p. 6.

[64] *House Security Policy Manual*, p. 9.

[65] *House Security Policy Manual*, p. 9; DOD Manual 5200.01, Vol. 3, *DoD Information Security Program: Protection of Classified Information*, "Enclosure 3 – Storage and Destruction," January 17, 2025; and DOD Instruction 5220.31, *National Industrial Security Program*, May 9, 2023.

[66] *House Security Policy Manual*, p. 9; DOD Manual 5200.01, Vol. 3, *DoD Information Security Program: Protection of Classified Information*, "Enclosure 3 – Storage and Destruction," January 17, 2025.

[67] *House Security Policy Manual*, p. 10; ODNI, *Sensitive Compartmented Information Facilities*, ICD 705 (Technical Amendment), February 20, 2024, https://www.dni.gov/files/documents/ICD/ICD-705-SCIFs.pdf; and National Counterintelligence and Security Center, *Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities*, IC Tech Spec for ICD/ICS 705 (Version 1.5), March 13, 2020, https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.

Author Information

Michelle D. Christensen
Analyst in Government Organization and Management

Acknowledgments

An earlier version of this report was written by former CRS Specialist Frederick M. Kaiser.

Disclaimer