Order Code RS20748
Updated January 11, 2006

Protection of Classified Information by Congress: Practices and Proposals

Frederick M. Kaiser
Specialist in American National Government
Government and Finance Division

Summary

The protection of classified national security and other controlled information is of concern not only to the executive branch, which determines what information is to be safeguarded for the most part,[1] but also to Congress, which uses such information to fulfill its constitutional responsibilities. As a result, Congress has established procedures and mechanisms to protect controlled information in its custody. These arrangements, however, differ between the House and the Senate and among panels in each chamber. The Senate, for instance, has established an Office of Senate Security to centralize responsibility for personnel and information security, whereas the House has not created a counterpart. Proposals to change the system, some of which could prove controversial or costly, usually seek to set uniform standards or increase requirements for access. This report will be updated as conditions require.

Current Practices and Procedures

Congress relies on a variety of mechanisms and instruments to protect classified information in its custody. These include a specific Senate office responsible for setting

[1] Classification of national security information is governed for the most part by executive orders: E.O. 12958, issued by President William Clinton in 1995, and E.O. 13292, which amends it, issued by President George W. Bush in 2003. Other national security-related information — such as atomic energy "Restricted Data" (42 U.S.C. 2162-2168) and "intelligence sources and methods" (50 U.S.C. 403(d)(3)) — is specified in statute and subsequent rules issued, respectively, by the Department of Energy and Director of Central Intelligence (to be replaced by the Director of National Intelligence). Other controlled information — such as "sensitive security" and "sensitive but unclassified" information — is governed for the most part by executive directives. See CRS Report RL32597, *Information Sharing for Homeland Security*, by Harold C. Relyea and Jeffrey W. Seifert; CRS Report RL31845, *"Sensitive But Unclassified" and Other Federal Controls on Scientific and Technological Information*, by Genevieve J. Knezo; and CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Nathan Brooks.

and implementing uniform standards for handling classified information; detailed rules for committees in both chambers for controlling access to such information; a secrecy oath for all Members and employees of the House and of some committees; security clearances and nondisclosure agreements for staff; and formal procedures for investigations of suspected security violations. Public law, House and Senate rules, and committee rules, as well as custom and practice, constitute the bases for these requirements.[2]

Senate Office of Security and Security Manual

Each chamber has approached its security responsibilities differently. The Senate established an Office of Senate Security in 1987 — the result of a bipartisan effort over two Congresses — to centralize responsibility for information and personnel security.[3] Located in the Office of the Secretary of the Senate, the Security Office is charged with setting and implementing 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*, issued initially in 1988 — "are binding upon all employees of the Senate."[4] They include committee and Member office staff and officers of the Senate as well as consultants and contract personnel. The regulations cover a wide range of matters on safeguarding classified information: physical security requirements; procedures for storing materials; mechanisms for protecting communications equipment; security clearances and nondisclosure agreements for all Senate staff needing access to classified information; and follow-up investigations of suspected security breaches by employees.

The House does not have a separate security office or a comprehensive security manual covering the entire chamber and all offices and employees. Instead, individual committee and Member offices set requirements, following chamber and committee rules, guidelines in internal office procedural manuals, and custom. As part of this process, the U.S. Capitol Police are responsible for staff security clearances and making rooms secure for handling classified information.

---

[2] For background, see Herrick S. Fox, "Staffers Find Getting Security Clearances Is Long and Often a Revealing Process," *Roll Call*, Oct. 30, 2000, pp. 24-25; Frederick M. Kaiser, "Congressional Rules and Conflict Resolution: Access to Information in the House Select Committee on Intelligence," *Congress and the Presidency*, vol. 15 (Spring 1988), pp. 49-73; U.S. Commission on Protecting and Reducing Government Secrecy, *Secrecy: Report of the Commission* (Washington: GPO, 1997); U.S. House, Committee on Government Operations, Subcommittee on Legislation and National Security, *Congress and the Administration's Secrecy Pledges*, Hearings, 100th Cong., 2nd sess. (Washington: GPO, 1988); U.S. House, Permanent Select Committee on Intelligence, *United States Counterintelligence and Security Concerns — 1986*, 100th Cong., 1st sess., H.Rept. 100-5 (Washington: GPO, 1987), pp. 3-4; U.S. Congress, Joint Committee on the Organization of Congress, *Committee Structure*, Hearings, 103rd Cong., 1st sess. (Washington: GPO, 1993), pp. 64-79, 312-316, 406-417, and 832-841; and U.S. Senate, Select Committee on Intelligence, *Meeting the Espionage Challenge*, S.Rept. 99-522, 99th Cong., 2nd sess. (Washington: GPO, 1986), pp. 90-95.

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

[4] U.S. Senate, Office of Senate Security, *Security Manual* (Washington: OSS, 1998), preface.

Security Clearances and Nondisclosure Agreements for Staff

Security clearances and written nondisclosure agreements can be required for congressional staff but are handled differently by the Senate and House.[5] The Senate Office of Security mandates such requirements for all Senate employees needing access to classified information. No comparable across-the-board requirement for security clearances or secrecy agreements exists for House employees. Security clearances for staff and nondisclosure agreements are required, however, for House offices that follow the provisions of Executive Order 12968, governing access in the executive branch.[6]

Secrecy Oath for Members and Staff

House and Senate requirements differ with regard to secrecy oaths. At the beginning of the 104th Congress, the House adopted a secrecy oath for all Members, officers, and employees of the chamber. Before any such person may have access to classified information, he or she must "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" (House Rule XXIII, clause 13, 108th Congress). Previously, a similar oath was required only for members and staff of the House Permanent Select Committee on Intelligence; this requirement had been added in the 102nd Congress as part of the Select Committee's internal rules, following abortive attempts to establish it in public law.[7]

Other examples exist in committee rules. The House Select Committee on Homeland Security, for instance, required a separate oath from each Member, officer, and employee of the committee (or another Member seeking access); he or she affirmed that "I will not disclose any classified information received in the course of my service on the Select Committee on Homeland Security, except as authorized by the Committee or the House of Representatives or in accordance with the Rules of such Committee or the Rules of the House" (House Select Committee on Homeland Security, Rules of Procedure, Rule 7(f)), 108th Congress). Neither the full Senate nor any panel, including the Select Committee on Intelligence, apparently imposes a similar obligation on its members or employees.

Investigations of Security Breaches

The Senate Office of Security is charged with investigating suspected security violations by Senate employees.

---

[5] The three congressional support agencies (i.e., Congressional Budget Office, Congressional Research Service, and Government Accountability Office) have separate personnel security systems and policies. Each entity, however, requires security clearances for its staff to gain access to classified information.

[6] Executive Order 12968, "Access to Classified Information," issued by President William Clinton, on Aug. 2, 1995, *Federal Register*, Aug. 7, 1995, vol. 60, pp. 240, 245-250, and 254.

[7] U.S. Congress, Committee of Conference, *Intelligence Authorization Act, Fiscal Year 1992*, 102nd Cong., 1st sess., H.Rept. 102-327 (Washington: GPO, 1991), pp. 35-36.

In addition, investigations by the House and Senate Ethics Committees of suspected breaches of security are authorized by each chamber's rules, directly and indirectly. The Senate Ethics Committee, for instance, 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" (S.Res. 338, 88th Congress). The panel is also directed "to investigate any unauthorized disclosure of intelligence information [from the Senate Intelligence Committee] by a Member, officer or employee of the Senate" (S.Res. 400, 94th Congress). The House, in establishing its Permanent Select Committee on Intelligence, issued similar instructions. H.Res. 658 (95th Congress) ordered the Committee on Standards of Official Conduct to "investigate any unauthorized disclosure of intelligence or intelligence-related information [from the House Intelligence Committee] by a Member, officer, or employee of the House ...."

Access for Non-Committee Members

Procedures controlling access to classified information held by committees exist throughout Congress. These set conditions for viewing classified information and determine whether legislators who are not on a panel are eligible for access to its classified holdings and attend closed hearings or executive sessions. Other rules govern staff access and the sharing of classified information with other panels in the chamber.

The most exacting requirements and procedures along these lines have been adopted by the House Permanent Select Committee on Intelligence; these rules are based on its 1977 establishing authority (H.Res. 658, 95th Congress) and reinforced by intelligence oversight provisions in public law, such as the 1991 Intelligence Authorization Act (P.L. 102-88; 105 Stat. 441). To gain access to the panel's classified holdings or attend a closed hearing or other executive session, for instance, Representatives who are not members of the Intelligence Committee must go through a six-stage process, including a written request and recorded votes by a quorum of committee membership (Committee Rule 10, 108th Congress). Thus, it is possible for a non-member to be denied attendance at its executive sessions or access to its classified holdings. By comparison, the rules of the House Armed Services Committee (Rule 21, 108th Congress) "ensure access to [its classified] information by any member of the committee or any other Member of the House of Representatives who has requested an opportunity to review such material."

When the House Intelligence Committee releases classified information to another panel or non-member, moreover, the recipient must comply with the same rules and procedures that govern the Intelligence Committee's control and disclosure requirements.

Proposals for Change

There have been a number of proposals from congressional bodies, government commissions, and other groups, suggesting changes in the current procedures for handling and protecting classified information in the custody of Congress. These proposals have focused, for the most part, on establishing uniform standards for relevant congressional offices and employees and increasing the access eligibility requirements for both

Members and staff.[8] These suggestions, some of which might be controversial or costly, include the following:

Establish an Office of Security for the House of Representatives, along with a Comprehensive *Security Manual*, Similar to the Senate's Devices. The new House Security Office could be responsible for developing and implementing uniform standards and regulations for all phases of the handling and safeguarding of classified and other sensitive information. This responsibility would cover physical and communications security practices in all offices; proper storage and tracking of relevant information, documents, and materials; security clearances and nondisclosure agreements for employees; and investigative practices, appeals procedures, and penalties for security violations by staff. Such uniformity and standardization, according to proponents, would enhance security across the board and clarify responsibility for all aspects of it. Opposition to such a proposal would likely be based on the cost of a new office; the additional layer of bureaucracy it could entail, replacing, for instance, duties now performed by the Capitol Police; and the transfer of some responsibility for employee standards and conduct from committee chairs and individual legislators to a central office.

Mandate That Members of Congress Have Security Clearances to Be Eligible for Access to Classified Information. The goal of those pursuing this change is to tighten and make uniform standards governing access for all Members who request or need it. This would mark a significant departure from past precedent. Members of Congress (as with the President and Vice President or Justices of the Supreme Court) have never been required to hold security clearances. Critics have argued that the proposal raises an issue of independence of the national legislature if an executive branch agency conducted the background investigation and had access to the information it generated or an executive official adjudicated the clearance for elected legislators. Even if the adjudication were performed by other legislators, concerns might arise over their fairness, impartiality, and objectivity, as well as over the publicity of a negative decision.

Such a requirement could be applied in different ways: (1) to all Senators and Representatives and thus, in effect, becoming a condition for serving in Congress; (2) only to Members needing access to classified information, including those on relevant panels or seeking access to their holdings; (3) only to Members who are on panels that receive classified national security information; or (4) only to those seeking access to such information held by panels where they are not members.

Under the security clearance proposal, background investigations might be conducted by an executive branch agency, such as the Office of Personnel Management, Defense Investigative Service, or the Federal Bureau of Investigation; by a legislative branch entity, such as the U.S. Capitol Police or General Accounting Office; by a special security office in each chamber; or possibly by a private investigative firm under contract. This approach would presumably specify the adjudicator(s), that is, the positions or officials who would judge, based on the background investigation, whether an individual Member is eligible for access to classified information. Proponents have suggested that the

---

[8] See the various proposals from the House and Senate Select Committees on Intelligence, House Subcommittee on Legislation and National Security, and Joint Committee on the Organization of Congress, all of which are cited in footnote 2.

adjudicators could include, among others, the majority or minority leader, a special panel of in each chamber, or even an executive branch official, if Congress so directed.

Direct Senators or Senate Employees to Take or Sign a Secrecy Oath to Be Eligible for Access to Classified Information. This proposal would require a secrecy oath for Senators or Senate staffers, similar to the current requirement for Members, officers, and employees of the House of Representatives. An earlier attempt — to mandate such an oath for all Members and employees of both chambers of Congress seeking access to classified information — was initiated in 103rd Congress, as part of the FY1994 Intelligence Authorization Act, but failed.[9] If enacted, it would have prohibited intelligence entities from providing classified information to Members of Congress and their staff, as well as officers and employees of the executive branch, unless these persons had signed an oath of secrecy — pledging that he or she "will not willfully directly or indirectly disclose to any unauthorized person any classified information" — and the oath had been published in the *Congressional Record*.

Direct All Cleared Staff — or Possibly Just Those Cleared for the Highest Levels — to File Financial Disclosure Statements Annually. Many congressional staff with such clearances may already file financial disclosure statements because of their employment rank or salary level. Nonetheless, objections might arise because the proposal would impose yet another burden on some staff and necessitate additional record-keeping. This requirement's effectiveness might also be questioned.

Require Polygraph Examinations and/or Drug Tests for Staff to Be Eligible for Access to Classified Information. Under such a proposal, tests could be imposed as a condition of employment for personnel in offices holding classified information, applied only to staff seeking access to such information, or required for both employment and access.[10] Objections have been expressed to such tests, however, because of their cost and possible unreliability.

---

[9] The initial version, applicable to only Representatives, had been introduced as a floor amendment in the House; it was further amended to extend the requirement to Senators along with officers or employees of the executive branch, including the President, Vice President, cabinet secretaries, and the heads of all intelligence agencies, as well as the approximately three million federal employees with security clearances. The provision was not included by the conferees on the bill. For coverage of these developments, see *Congressional Record*, daily edition, vol. 139, (Aug. 4, 1993), pp. H5770-H5773, and Nov. 18, 1993, p. H10157.

[10] In the 105th Congress, the House approved a rule change to allow for drug testing for Members and staff (as a condition of employment). House Rule I, cl. 13 directed that "the Speaker, in consultation with the Minority Leader, shall develop through an appropriate entity of the House a system for drug testing in the House. The system may provide for the testing of a Member, Delegate, Resident Commissioner, officer, or employee of the House...." CRS Report RS20689, *Drug Testing in the House of Representatives: Background, Legislation and Policy*, by Lorraine Tong (archived, available from author).