Order Code RS20748
Updated April 5, 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 the information to fulfill its constitutional responsibilities. It has established mechanisms to safeguard controlled information in its custody, although these arrangements vary over time between the two chambers and among panels in each. Both chambers, for instance, have created offices of security to consolidate relevant responsibilities, but these were established two decades apart. Other differences exist at the committee level. Proposals for change, some of which are controversial, usually seek to set uniform standards or heighten 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 House and Senate offices responsible for setting and implementing standards for handling classified information; detailed committee rules 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

[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, amending it, issued by President George W. Bush in 2003. 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 National Intelligence. Other controlled information — such as "sensitive security" and "sensitive but unclassified" information — is determined largely by executive directives. CRS Report RL31845, *"Sensitive But Unclassified" and Other Federal Controls on Scientific and Technological Information*, by Genevieve J. Knezo; CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Nathan Brooks; and CRS Report 97-771, *Security Classification Policy and Procedure: E.O. 12958, as Amended*, by Harold C. Relyea.

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]

Chamber Offices of Security and Security Manuals

The chambers have approached their security program differently, although each now has a security office. The Senate established an Office of Senate Security nearly two decades ago, in 1987, as the result of a bipartisan effort over two Congresses. It is charged with consolidating information and personnel security.[3] 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*, issued initially in 1988 — "are binding upon all employees of the Senate."[4] They cover committee and Member office staff and officers of the Senate as well as consultants and contract personnel. The regulations extend to 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; and follow-up investigations of suspected security violations by employees.

The House put its own security office in place, under the jurisdiction of the Sergeant at Arms, in 2005, following approval of the chamber's Committee on House Administration. The new office, similar to the Senate predecessor, 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. In the past, the House had relied on individual committee and Member offices to set requirements following chamber and committee rules, guidelines in internal office procedural manuals, and custom.

---

[2] 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); 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); 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; 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 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 and approved on 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 have been handled differently by each chamber.[5] The Senate Office of Security mandates such requirements for all Senate employees needing access to classified information.[6] No comparable across-the-board requirements for security clearances or secrecy agreements yet exist for all House employees. But these could be applied by the new office of security, when it becomes fully operational.

Secrecy Oath for Members and Staff

The House and Senate differ with regard to secrecy oaths for Members and staff. 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, cl. 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 adoptions have occurred under committee rules. The House Select Committee on Homeland Security (Rules of Procedure, Rule 7(f), 108th Congress), for instance, required an oath from each Member, officer, and employee of the committee, or a non-Member seeking access; each 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." 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 and the House counterpart are charged with investigating or coordinating investigations of suspected security violations by employees.

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

---

[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; but each requires security clearances for its staff to gain access.

[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.

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 creating 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 along these lines have been developed 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). Representatives who are not members of the Intelligence Committee go through a multi-stage process (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

A variety of proposals, coming from congressional bodies, government commissions, and other groups, have called for changes in the current procedures for handling and safeguarding classified information in the custody of Congress. These plans, some of which might be controversial or costly, focus on setting uniform standards for congressional offices and employees and heightening the access eligibility requirements.[8]

Mandate That Members of Congress Hold Security Clearances to Be Eligible for Access to Classified Information. This would mark a significant departure from the past. Members of Congress (as with the President and Vice President,

---

[8] See citations to the House and Senate Select Committees on Intelligence, House Subcommittee on Legislation and National Security, and Joint Committee on the Organization of Congress.

Justices of the Supreme Court, or other federal court judges) have never been required to hold security clearances. Most of the proposals along this line appeared in the late 1980s. A recent one, however, was introduced in 2006 by Representative Steve Buyer; H.Res. 747 (109th Cong.) would require a security clearance for Members serving on the House Permanent Select Committee on Intelligence and on the Subcommittee on Defense of the House Appropriations Committee. The resolution does not specify which entity (legislative or executive branch) would conduct the background investigation or which officer (in Congress or in the executive) would adjudicate the clearances.

The broad mandate for such clearances could be applied to four different groups: (1) all Senators and Representatives, thus, in effect, becoming a condition for serving in Congress; (2) only Members seeking access to classified information, including those on panels receiving it; (3) only Members on committees which receive classified information; or (4) only those seeking access to classified information held by panels where they are not members.

Under a security clearance requirement, background investigations might be conducted by an executive branch agency, such as the Office of Personnel Management or Federal Bureau of Investigation; by a legislative branch entity, such as the House or Senate Office of Security, or the Government Accountability Office; or possibly by a private investigative firm under contract. Possible adjudicators — that is, the officials who would judge, based on the background investigation, whether applicants are "trustworthy" and, therefore, eligible for access to classified information — could extend to the majority or minority leaders, a special panel in each chamber, a chamber officer, or even an executive branch officer, if Congress so directed.

The main goals behind this change are to tighten and make uniform standards governing eligibility for access for Members. Proponents maintain that it would help safeguard classified information by ensuring access only by Members deemed "trustworthy" and, thereby, limit the possibility of leaks and inadvertent disclosures. In addition, the clearance process itself might make recipients more conscious of and conscientious about the need to safeguard this information as well as the significance attached to it. As a corollary, supporters might argue that mandating a clearance to serve on a panel possessing classified information could increase its members' appreciation of the information's importance and its protection's priority. This, in turn, might help the committee members gain the access to information that the executive is otherwise reluctant to share and improve comity between the branches.

Opponents, by contrast, contend that security clearance requirements would compromise the independence of the legislature if an executive branch agency conducted the background investigation; had access to the information it generated; or adjudicated the clearance. Even if the process was fully under legislative control, concerns might arise over: its fairness, impartiality, objectivity, and correctness (if determined by an inexperienced person); the effects of a negative judgement on a Member, both inside and outside Congress; and the availability of information gathered in the investigation, which may not be accurate or substantiated, to other Members or to another body (such as the chamber's ethics committee or Justice Department), if it is seen as incriminating in matters of ethics or criminality. Opponents might contend, moreover, that adding this new criterion could have an adverse impact on individual Members and the full legislature in other ways. It might impose an unnecessary, unprecedented, and unique (among

elected federal officials and court judges) demand on legislators; create two classes of legislators, those with or without a clearance; affect current requirements for non-Member access to holdings of committees whose own members might need clearances; possibly jeopardize participation by Members without clearances in floor or committee proceedings (even if held in executive or secret session); and retard the legislative process, while the investigations, adjudications, and appeals are conducted.

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 and staffers, similar to the current requirement for their House counterparts. An earlier attempt to mandate such an oath for all Members and employees of both chambers of Congress seeking access to classified information occurred in 1993, but was unsuccessful.[9] If approved, 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 the recipients had signed a nondisclosure agreement — 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 Just Those Cleared for the Highest Levels — to File Financial Disclosure Statements Annually. This demand might make it easier to detect and investigate possible misconduct instigated for financial reasons. And many staff with clearances may already file financial disclosure statements because of their employment rank or salary level; consequently, few new costs would be added. Nonetheless, objections might arise because the proposal would impose yet another burden on staff and result in additional record-keeping and costs. This requirement's effectiveness in preventing leaks or espionage might also be questioned by opponents.

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

---

[9] The initial version, part of the FY1994 Intelligence Authorization Act, applied only to Representatives but was later extended 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 all employees with security clearances. The provision was dropped in conference. *Congressional Record*, daily ed., 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), directing "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).