

Protection of Classified Information by Congress: Practices and Proposals

Frederick M. Kaiser
Specialist in American National Government

August 31, 2011

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Congressional Research Service
7-5700
www.crs.gov
RS20748

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

The protection of classified national security and other controlled information is of concern not only to the executive branch—which, for the most part, determines what information is classified and controlled—but also to 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; but these were established nearly two decades apart. Other differences exist at the committee level, regarding the availability and use of information in committees' custody. Proposals for change, some of which are controversial and could be costly, usually seek to set uniform standards or heighten requirements for access.

This report will be updated as conditions require.

GalleryWatch
http://www.crsdocuments.com
Penny Hill Press

Contents

Current Practices and Procedures 1
Chamber Offices of Security and Security Manuals 2
Senate 2
House 2
Security Clearances and Nondisclosure Agreements for Staff 3
House and Senate Committee Staff 3
House and Senate Member Office Staff 3
Legislative Branch Support Agencies 4
Secrecy Oaths for Members and Staff 4
Sharing Committee-Held Information with Non-Committee Members 5
Limiting Access to Special Groups: The "Gang of Eight" and "Gang of Four" 6
Investigation of Security Breaches 7
Other Protective Measures 7
Proposals for Change 8
Mandate That Members of Congress Hold Security Clearances to Be Eligible for Access to Classified Information 8
Pros 9
Cons 9
Direct Senators or Senate Employees to Take or Sign a Secrecy Oath to Be Eligible for Access 9
Direct All Cleared Staff—or Just Those Cleared for the Highest Levels—to File Financial Disclosure Statements Annually 10
Require Polygraph Examinations and/or Drug Tests for Staff to Be Eligible for Access to Classified Information 10

Contacts

Author Contact Information 10

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 to obtain. But accessibility to it is seen as necessary for the legislature to carry out its constitutional responsibilities, especially overseeing the executive and legislating public policy.

The safeguards surrounding 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 afterwards. 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 afterwards, in what contexts and forums, and under what conditions;
- establishment of special congressional groups to receive highly sensitive classified information;
- a secrecy oath required for all Members and employees of the House and several of its committees;
- security clearances and nondisclosure agreements for staff; and
- formal procedures for investigating suspected security violations.

Public laws, 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 Report RL33494, *Security Classified and Controlled Information: History, Status, and Emerging Management Issues*, by Kevin R. Kosar; and CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea.

[2] A number of CRS reports deal with various aspects of this area: CRS Report R40136, *Congress as a Consumer of Intelligence Information*, by Alfred Cumming and Richard A. Best Jr.; CRS Report R40691, *Sensitive Covert Action Notifications: Oversight Options for Congress*, by Alfred Cumming and Richard A. Best Jr.; CRS Report R40698, *"Gang of Four" Congressional Intelligence Notifications*, by Alfred Cumming and Richard A. Best Jr.; CRS Report RL32525, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, by Frederick M. Kaiser; CRS Report R40602; *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, by Jerome P. Bjelopera; CRS Report RL33616, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Mark A. Randol; and CRS Report RL30240, *Congressional Oversight Manual*, by Frederick M. Kaiser, Walter J. Oleszek, and Todd B. Tatelman, especially pp. 61-69.

[3] For further background on the protection of classified information by Congress, see Frederick M. Kaiser, (continued...)

Chamber Offices of Security and Security Manuals

The two chambers have approached their security program differently, although each now has an office of security and a set of requirements, instructions, and guidelines regarding the protection of classified and other controlled information.

Senate

The Senate established an Office of Senate Security in 1987, the result of a bipartisan effort over two Congresses. It is charged with consolidating information and personnel security.[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—"are binding upon all employees of the Senate."[5] These cover committee and Member office staff and officers of the Senate as well as consultants and contract personnel—but not Members themselves. 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.

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 chamber's Committee on House Administration.[6] The 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

(...continued)

"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; 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. 99-522, 99th Cong., 2nd sess. (1986), pp. 90-95; and Office of the Director of National Intelligence, *Reporting of Intelligence Activities to Congress*, Intelligence Community Policy Memorandum Number 2005-100-3 (10 Jan. 06), and *Reforming Intelligence: The Passage of the Intelligence Reform and Terrorism Prevention Act* (Washington: ODNI, 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), *Security Manual* (revised, 2007), preface.

[6] The two relevant 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.

breach investigations.[7] Unlike its Senate counterpart, however, the House Office of Security has not issued an official security manual. Nonetheless, OHS provides relevant services, instructions, and forms for security clearances and other safeguards to protect classified information.[8] Prior to the establishment of OHS, the chamber had relied on individual committee and Member offices to set requirements following chamber and committee rules, guidelines in internal office procedural manuals, and custom.

Security Clearances and Nondisclosure Agreements for Staff

Although there is no across-the-board, comprehensive requirement for all legislative branch staff, they are required to have security clearances and written nondisclosure agreements to gain access to classified information. These exist through various mechanisms,[9] which apply to different employee categories:

House and Senate Committee Staff

Each panel spells out its requirements in its rules to cover access.[10] In addition, the Office of Senate Security and Office of House Security both require employees needing access to classified information to have security clearances and nondisclosure agreements in order to be eligible for access to classified national security information.[11] A provision in the *Senate Security Manual* along these lines stipulates that "Senators and Committee Chairmen must determine which positions on their staffs require a security clearance. Clearances will only be granted to employees whose assignments require access to classified information."[12]

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. Even so, requirements and limitations are directed by each chamber's office of security.[13] A limit may also be imposed on the number of staff with clearances in any individual Member office.[14] Along with this, congressional offices may on their own require a need-to-know for individual staffers seeking access to certain classified information.

[7] These are derived from its establishing authority (ibid.) and spelled out in House Office of the Sergeant at Arms, Office of House Security, *OHS Website*, available at http://saa.house.gov/ohs, and *Security Clearances*, available at http://saa.house.gov/ohs/security-clearances.

[8] Ibid.

[9] Herrick S. Fox, "Staffers Find Getting Security Clearances Is Long and Often a Revealing Process," *Roll Call*, October 30, 2000, pp. 24-25.

[10] For examples, see U.S. House Permanent Select Committee on Intelligence, *Rules of Procedure*, 112th Congress, Rules 12(b) and 14(c); and House Committee on Homeland Security, *Committee Rules*, 112th Congress, Rule XV(C).

[11] OSS, *Security Manual*, pp. 8 and 10; and OHS, *Security Clearances*.

[12] OSS, *Security Manual*, p. 8.

[13] Ibid. and OHS, *Security Clearances.*

[14] Only two cleared staff, for instance, are allotted to an individual House Member's office at any one time. OHS, *Security Clearances*.

Legislative Branch Support Agencies

Security clearance requirements are included in the personnel manuals, job and position descriptions, or vacancy announcements of Congress's support agencies: Congressional Budget Office (CBO), Congressional Research Service (CRS) as well as the Library of Congress (LOC), and Government Accountability Office (GAO).[15]

Secrecy Oaths for Members and Staff

The House and Senate differ with regard to secrecy oaths for Members and staff. Neither the full Senate nor any Senate panel apparently imposes a secrecy oath or affirmation on its Members or employees.

The House, by comparison, has adopted such special procedures. 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

> 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.[16]

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.[17] The oath is still in effect for the panel's Members and staff:

> I do solemnly swear (or affirm) that I will not disclose or cause to be disclosed any classified information received in the course of my service on the House Permanent Select Committee on Intelligence, except when authorized to do so by the Committee or the House of Representatives.[18]

At least one other panel has adopted a similar measure. The House Committee on Homeland Security requires an oath or affirmation from each committee Member or staff seeking access to classified information, modeled after the one adopted by the House Intelligence Committee.[19]

---

[15] For illustration, see CBO, *Employment Opportunities*, "Employment Requirements," available at https://careers.cbo.gov/ext/search.asp; CRS and LOC, Office of the Inspector General, LOC*, Office of Security and Emergency Preparedness: Survey of the Personnel Security Office's Policies and Procedures*, Audit Survey Report No. 2011-PA-102 (Washington, DC, 2011), p.5; and GAO, position description for Controller, Administrative Service Officer (SES Career Appointment), available at http://jobview.usajobs.gov/GetJob.aspx?JobIG=101883709&JobTitle=Controller%2Ad.

[16] House Rule XXIII, cl. 13, 112th Congress. Copies of the oath or affirmation are retained by the Clerk as part of the records of the House. Ibid.

[17] 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.

[18] House Intelligence Committee, *Rules of Procedure*, Rule 14(d).

[19] U.S. House Committee on Homeland Security, *Committee Rules*, 112th Congress, Rule XV(E).

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.[20] This includes 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; and if so, how, to what extent, and in what form;[21]
- what specific committee-held information is to be made available to non-committee Members seeking access; a panel's requirements and conditions for access may depend on what the information covers (the specific subject matter and a need-to-know), to what extent it may be made available (all or only a part of it), in what form (e.g., the actual documents, a summary account, or a briefing from a committee Member or staff), under what restrictions (with or without staff in attendance or taking notes), or where (in the committee offices, most likely, or in a secure area elsewhere); and
- how and in what other forums (e.g., with another congressional panel or on the floor of the chamber) may the information be used and under what restrictions.

The most exacting requirements along these lines have been developed by the House Permanent Select Committee on Intelligence; its rules 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.[22] The panel's controls apply to select committee Members sharing classified information outside the committee itself as well as to non-committee Representatives seeking access to the panel's holdings.[23] In the latter case, an individual requester must go through a multi-stage process to obtain access.[24] Consequently, 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 a cleared staffer or may take notes. When the House Select Committee on Intelligence releases classified information to

[20] For further discussion, see the citations in footnote 2, above.

[21] For example, the classified annex to the annual intelligence authorization act is available to Members in the secure offices of the select committees on intelligence. Committees may also selectively release classified information to Members of their own chamber. As an illustration, see Hon. Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence, Dear Colleague letter regarding access to two classified Central Intelligence Agency reports, March 13, 2009. Based on a request from a select committee member and approved by the panel, these reports were made "available to all members of the House who have executed the [standard] secrecy oath .... and who will be asked to sign a specific non-disclosure agreement." Ibid.

[22] H.Res. 658, 95th Congress; and P.L. 102-88, 105 Stat. 441. For background, see Kaiser, "Congressional Rules and Conflict Resolution."

[23] House Intelligence Committee, *Rules*, Rules 13(b) and 14(f).

[24] Ibid., Rule 14(f).

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.[25]

By comparison, rules of the House Armed Services Committee are to "ensure access to information [classified at Secret or higher] by any member of the Committee or any other Member, Delegate, or Resident Commissioner of the House of Representatives … who has requested the opportunity to review such material."[26]

Limiting Access to Special Groups: The "Gang of Eight" and "Gang of Four"

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, however, may be bypassed—based on 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 so-called "Gang of Eight" or "Gang of Four."[27] 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 and chairman and ranking minority Member of its intelligence committee and the majority and minority leaders of the Senate and chairman and vice chairman of its intelligence committee. A separate so-called "Gang of Four" has also come into existence to receive briefings on particularly sensitive intelligence activities (other than covert operations), which, if disclosed, might reveal intelligence sources and methods. This non-statutory body is composed of the chairs and ranking minority Members of the House and Senate select committees on intelligence. On occasion, its meetings are attended by their staff directors.

A controversy had erupted recently, however, over the existing arrangements, when the intelligence committees are not the direct and immediate recipients of these presidential findings or executive briefings. The dispute arose, in part, because the members of either "Gang" had not been permitted to share the information with the full intelligence committee in their respective chamber; and they may have been delayed or prevented from even informing their panel that a notification or briefing had occurred.

The primary response by Congress was to modify the notification procedures—via the Intelligence Authorization Act of FY2010—allowing for more communication between the members of the "Gangs" and their respective select committees on intelligence.[28] Such new congressional notification procedures, along with several other proposed changes in the law, however, were of "serious concern to the Intelligence Community," prompting a threatened

[25] Ibid., Rule 14(f)(4)(B).

[26] U.S. House Committee on Armed Services, *Rules of the Committee, 112th Congress*, Rule 20(b). The same provision applies to committee staff, along with one individual of each committee Member's personal staff (designated by the Member in a letter to the committee chair and approved by the chair) "who have the appropriate security clearances and the need to know." Ibid., Rules 20(b) and 9(c).

[27] For coverage of these select groups and related matters, see CRS reports by Cumming and Best cited in footnote 2.

[28] P.L. 111-259, sec. 331.

presidential veto.[29] (A veto did not materialize.) The executive's opposition had been based on the changes' perceived adverse impact on "the long tradition of comity between the branches regarding intelligence matters."[30]

Investigation 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.[31] 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, importantly, 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."[32] 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."[33] The House, in creating its Permanent Select Committee on Intelligence, issued similar instructions. H.Res. 658 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."[34]

Other Protective Measures

In addition to the foregoing, each chamber and its committees subscribe to other measures designed to protect classified and controlled information. Some of these—derived from the House and Senate Offices of Security or such committees as the House and Senate select committees on intelligence—focus on the physical security of documents and facilities, while others affect individual conduct. These include

- stationing U.S. Capitol Police officers at committee sites;
- conducting Technical Security Countermeasures sweeps of offices and facilities to detect surveillance devices (e.g., bugs) and technical security weaknesses;
- safeguarding the storage and use of controlled information;
- setting up procedures to acknowledge the receipt of specific classified information and its dissemination to particular individuals;

[29] Peter R. Orszag, Director, Office of Management and Budget, letter to Hon. Dianne Feinstein and Hon. Silvestre Reyes, regarding the Intelligence Authorization Act for Fiscal Year 2010, and *Conference Letter regarding S. 1494 and H.R. 2701, the Intelligence Authorization Act for Fiscal Year 2010*, p. 1.

[30] Orszag, *Conference Letter*, p. 1. The *Conference Letter* continues: these changes would "undermine this fundamental compact between the Congress and the President regarding the reporting of sensitive intelligence matters as embodied in Title V of the National Security Act—an arrangement that for decades has balanced congressional oversight responsibilities with the President's responsibility to protect sensitive national security information." Ibid.

[31] For Senate staff, see OSS, *Security Manual*, pp. 10-11, which spells out the investigative procedures and penalties for violations.

[32] S.Res. 388, 88th Congress.

[33] S.Res. 400, 94th Congress.

[34] H.Res. 658, 95th Congress.

- conducting education and training programs; and
- reporting foreign travel and foreign national contact.

Proposals for Change

A variety of proposals—coming from congressional bodies, government commissions, and other groups—have called for changes in the procedures for handling and safeguarding classified information in the custody of Congress.[35] These plans, some of which might be controversial or costly, focus on setting uniform standards for congressional offices and employees and heightening access eligibility requirements.

Mandate That Members of Congress Hold Security Clearances to Be Eligible for Access to Classified Information

This would mark a significant and unprecedented departure from the past. Members of Congress (as with the President and Vice President, 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, following charges and countercharges between the executive and legislative branches over unauthorized disclosure of classified information. A more recent bill, introduced in 2006, would have required 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.[36] The resolution, however, did not specify which entity (in the legislative or executive branch) would conduct the background investigation or which officer (in Congress or in the executive) would adjudicate the clearances of Members.

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 the 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 would be "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.

[35] See citations in footnote 2, above.

[36] H.Res. 747, 109th Congress.

Pros

The main goals behind this proposed 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.

Cons

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 were fully under legislative control, concerns might arise over a number of matters: its fairness, impartiality, objectivity, and correctness (if determined by an inexperienced person); the effects of a negative judgment 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 also contend that adding this new criterion could have an adverse impact on individual Members, the full legislature, and the legislative process in other ways. It might impose an unnecessary, unprecedented, and unique (among elected federal officials and members of the federal judiciary) 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 secret sessions); and inordinately slow down the legislative process, while background investigations, adjudications, and appeals connected with security clearances of Members are conducted.

Direct Senators or Senate Employees to Take or Sign a Secrecy Oath to Be Eligible for Access

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 arose in 1993, but it was unsuccessful.[37] 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. Each would have to pledge that he or she "will not willfully directly or indirectly

[37] *Congressional Record*, daily ed., vol. 139, Aug. 4, 1993, pp. H5770-H5773; and Nov. 18, 1993, p. H10157.

disclose to any unauthorized person any classified information"—and the oath had been published in the *Congressional Record*.[38]

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 high-level 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, drug tests or polygraph examinations could be imposed in several different circumstances: as a condition of employment for all personnel in offices holding classified information, only on staff seeking access to such information, or for both employment and access. Objections have been expressed to such tests, especially as a pre-condition of employment, however, because of their costs and questioned reliability and validity.[39]

Author Contact Information

Frederick M. Kaiser
Specialist in American National Government
fkaiser@crs.loc.gov, 7-8682

[38] Ibid.

[39] For background on polygraph testing, see CRS Congressional Distribution Memorandum, *Polygraph Examinations of Federal Employees and Applicants*, by Frederick M. Kaiser; and CRS Report RL31988, *Polygraph Use by the Department of Energy: Issues for Congress*, by Alfred Cumming.