8 JAN 1979

MEMORANDUM FOR: Deputy Director for National Foreign Assessment
Deputy Director for Operations
Deputy Director for Science and Technology
Inspector General
General Counsel
Legislative Counsel
Comptroller

25X1 FROM : [redacted]
Chief, Regulations Control Branch
Information Systems Analysis Staff

25X1 SUBJECT : [redacted] Accountability and Handling of Classified Material (Job #8766)

FOR YOUR CONCURRENCE OR COMMENTS:

1. The attached proposal initiated by the Office of Security implements changes dictated by Executive Order 12065, and will replace the existing [redacted] and that portion of [redacted] pertaining to the safeguarding of classified material. (U) [illegible] 25X1

2. Please forward your concurrence or comments no later than 29 January 1979. Since Executive Order 12065 became effective 1 December 1978, please consider this as a priority action to be given immediate attention. Questions may be directed to [redacted] 25X1

25X1 [redacted]

[redacted] 25X1

25X1 Attachments:
1. Proposed [redacted]
2. Concurrence Sheet

*New Series

WARNING NOTICE--INTELLIGENCE SOURCES AND METHODS INVOLVED

cc: AO/DCI
SSA/DDA
C/ISAS
RAB
OS
OL
OC

DERIVATIVE CL BY [redacted] 25X1
☐ DECL ☒ REVW ON 8 January 99
DERIVED FROM A9c5.2

Next 16 Page(s) In Document Exempt

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300120010-3

Report No. 79-105 GOV

CONGRESS AND PROCEDURES FOR PROTECTING SECURITY OR INTELLIGENCE INFORMATION:

A Brief Overview

Harold C. Relyea
Specialist in American National Government
Government Division

August 3, 1979

The Congressional Research Service works exclusively for the Congress, conducting research, analyzing legislation, and providing information at the request of Committees, Members and their staffs.

The Service makes such research available, without partisan bias, in many forms including studies, reports, compilations, digests, and background briefings. Upon request, the CRS assists Committees in analyzing legislative proposals and issues, and in assessing the possible effects of these proposals and their alternatives. The Service's senior specialists and subject analysts are also available for personal consultations in their respective fields of expertise.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300120010-3

ABSTRACT

While Congress does not utilize the same information protection arrangements such as are found within the executive branch, it has a functional need to safeguard various types of sensitive materials and has various options available to it to achieve this end.

The author wished to credit Cheryl J. Scott and Sandra M. Wallace for the secretarial production of this report.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300120010-3

C O N T E N T S

CONGRESS AND PROCEDURES FOR PROTECTING SECURITY OR INTELLIGENCE INFORMATION:

A Brief Overview

Executive Summary

Congressional requests for and receipt of executive branch information and documents occur in a continuously changing political environment and against a background of constitutionally separated powers. In receiving sensitive information -- knowledge, the premature disclosure of which, if detected, could result in the conveyance of some type of undesired advantage -- from the departments or agencies, a congressional committee may elect to protect such material, regardless of whether or not it is regulated or under security classification, in order to guard against assertions that it was disclosed improperly by the panel. Without a good faith effort on the part of a committee to safeguard sensitive documents, the executive branch may allege that such records have been managed irresponsibly by Congress. When information provided by the departments and agencies is labeled as to its classified or offically secret status, then any plea of ignorance as to its sensitivity is irradicated and its transmittal to a committee may be predicated upon the understanding that it will be protected from disclosure.

As part of the good faith effort to assure the executive branch that sensitive information will be properly safeguarded, many committees of Congress have adopted special rules and procedures regarding the management of

such materials. This discussion focuses upon problems confronting committees attempting to protect sensitive information and documents, often under classification restrictions, supplied by the departments and agencies. While the matters explored here may have relevance for less specifically denoted security considerations, this narrative is not necessarily concerned with the management of confidential materials originated within Congress.

CONGRESS AND PROCEDURES FOR PROTECTING SECURITY AND/OR INTELLIGENCE INFORMATION:

A Brief Overview

Part I. Historical Framework

Although Congress does not make use of a formal system of security classification arrangements such as is found within the executive branch, it has a functional need, nevertheless, to protect various types of sensitive information, whether provided by other official entities, acquired from from private sources, or originated in Congress. Such materials may be supplied voluntarily with an understanding that no legislative branch disclosure will occur or, as recently happened, 1/ information may be transmitted grudgingly to Congress with only a fervent hope that its confidentiality will be maintained.

In abstract terms, "sensitive information" is temporal in nature -- its importance may lessen with the passage of time. Its character is such that its premature disclosure, if detected, could result in the conveyance of an unwanted advantage -- e.g., political, economic, or both -- to others.

1/ A private corporation, having supplied confidential business information to the Federal Trade Commission, was unsucesful in its efforts to enjoin the anticipated disclosure of this material to Congress by the agency; see Ashland Oil, Inc. v. F.T.C., 409 F. Supp. 297 (D.D.C. 1976), affirmed 548 F.2d 977 (D.C. Cir. 1976); for a discussion of the possible consequences of this decision, see Barbara J. Smith. Congressional Treatment of Confidential Business Information: Proposals to Avert Unwarranted Disclosure. Indiana Law Journal, v. 52, Summer, 1977: 769-791.

Or such release might be regarded as an unwarranted violation of a fundamental value -- e.g., "invasion of personal privacy" or "contrary to sound business practice" -- of a given society or political culture.

In more specific terms, existing legal authorities suggest types or information which appear to warrant protection within the executive branch and, therefore, might be regarded as "sensitive" within Congress. These materials, so identified, pertain to or include: national defense or foreign policy, 2/ national security, 3/ classified information, 4/ diplomatic codes, 5/ intelligence sources and methods, 6/ law enforcement investigatory files, 7/ trade secrets, 8/ commercial or financial matters, 9/ or personal privacy. 10/ While other such references un-

---

2/ See 5 U.S.C. 552(b)(1).

3/ See E.O. 12065.

4/ See 18 U.S.C. 798, 50 U.S.C. 783.

5/ See 18 U.S.C. 952.

6/ See 50 U.S.C. 403(d)(3), 403g.

7/ See 5 U.S.C. 552(b)(7).

8/ See 18 U.S.C. 1905.

9/ See 5 U.S.C. 552(b)(4), 552(b)(8); a study by the Department of Justice has identified a multiplicity of laws regarding executive branch protection of business information held by the departments and agencies; see U.S. Commission on Federal Paperwork. Confidentiality and Privacy. Washington, U.S. Govt. Print. Off., 1977, pp. 26-27.

10/ See 5 U.S.C. 552(b)(6), 5 U.S.C. 552a.

doubtedly could be added to this list, these examples are among the more obvious concepts conveying a sense of "sensitive" information. 11/

While a variety of ways exist for identifying sensitive information, at least one type of record is presented to Congress with a clear indication of its protected status. Classified documents are marked with identification labels -- "Top Secret," "Secret," and "Confidential" --by executive branch personnel, indicating that their contents met prescribed standards for the creation of official secrets.

Today, after many years of evolution, various congressional committees have specific rules for managing classified materials. Others have developed procedures for safeguarding various types of sensitive data. The following paragraphs explore some of the matters which confront a congressional committee attempting to effectively manage classified and sensitive information and documents furnished to them directly or indirectly by Federal departments or agencies, other committees, other governments, or private sources. Congress also has demonstrated its concern about -- or has been criticized regarding -- disclosure of other types of sensitive information by Members or staff including classified documents obtained directly from a source outside Congress, confidential committee studies or hearing materials, and Senate and House closed session matters. This overview may be relevant to such disclosures, but

---

11/ For example, this list overlooks "restricted data," a particular type of sensitive atomic energy information defined by the Atomic Energy Act (see 42 U.S.C. 2161-2166).

concentrates on the problems confronting committees in protecting sensitive information and records in their possession, particularly those supplied and formally classified by Federal entities. Before embarking upon that discussion, however, the emergence and contemporary context of executive branch classification policy and practice, together with related administrative control procedures, are briefly considered; the implications of committee receipt of regulated records from a department or agency are assessed in terms of executive-congressional relations; and existing congressional rules regarding sensitive or classified documents are reviewed.

Emergence of executive branch policy and practice

Although members of the United States armed forces were, from the time of the Revolution, prohibited from communicating with the enemy, and spying during wartime similarly had been condemned since that era, no directives regarding the protection of defense information or guarding against foreign intelligence intrusions were issued until after the Civil War. 12/ The first of these instructions appeared in War Department General Orders of 1869. The thrust of these regulations, which evolved into a document protection system by the turn of the century, was to provide for the protection of coastal defenses and fortresses

12/ For a detailed history of the evolution of security classification policy see U.S. Congress. Senate. Committee on Government Operations. Government Secrecy. Hearings, 93rd Congress, 2d Session. Washington, U.S. Govt. Print. Off., 1974. pp. 843-884.

against unwanted observers. These arrangements were confined to the Army and the Navy until the eve of World War II. On March 22, 1940, President Franklin D. Roosevelt issued an order (E.O. 8381) extending information protection procedures beyond the armed forces institutions to potentially embrace all information, regardless of its governmental unit of origin or storage, critically bearing upon the Nation's defense. And, in 1951, President Harry S. Truman authorized (E.O. 10290) the utilization of information protection arrangements by all agencies of the Federal Government having a role in "national security" matters. This scope, with regard to classification use, generally has remained in effect unto the present time: security classification procedures are employed by both military and non-military policy entities to protect information pertaining to "national security," a broadly interpreted referent generally regarded as including matters beyond more narrowly understood "national defense" concerns. Indeed, because "national security" has never been strictly defined in law and has proven, in practice, to be a concept of sweeping scope, a preference for more precise language, to prevent the over-zealous production of offical secrets, has been expressed officially by one congressional panel having recognized expertise in this policy sphere. 13/

13/ See U.S. Congress. House. Committee on Government Operations. Executive Classification of Information -- Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552). Washington, U.S. Govt. Print. Off., pp. 61-64. (93rd Congress, 1st Session. House Report No. 93-221)

Authority to apply security classification to information within the executive branch generally can be attributed to a handful of currently operative authorities. 14/ Foremost among these references is the President's standing Executive order (E.O. 12065) prescribing classification criteria and procedures. This instrument also provides an administrative mechanism for the implementation of other information security authorities. Both atomic energy data and intelligence materials may be protected by law apart from the President's classification order, but, nevertheless, bear markings and are otherwise main-

---

14/ Constitutional provisions usually cited by the Chief Executive in issuing an executive order regarding security classification matters include Article II, section 1, vesting executive power in a President of the United States; Article II, section 2, naming the President as Commander-in-Chief of the Army and Navy of the United States; and Article II, section 3, requiring that the President take care that the laws be faithfully executed (see concurring opinion of Justice Black in New York Times Co. v. United States, 403 U.S. 713, 718 (1971) and of Justice Stewart with whom Justice White concurred, ibid., pp. 727-728.)

Statutes normally cited by the executive branch as authority for establishing security classification policy include the Espionage Laws (18 U.S.C. 792 et seq.), the National Security Act (61 Stat. 496), section 4(b) of the Internal Security Act (50 U.S.C. 783(b)), the Atomic Energy Act (42 U.S.C. 2162(c)), and the Freedom of Information Act (5 U.S.C. 552). In his concurring opinion in the Pentagon Papers Case, (supra, p. 741), Justice Marshall states:

> In these cases there is no problem concerning the President's power to classify information as 'secret' or 'top secret'. Congress has specifically recognized Presidential authority, which has been formerly exercised in Executive Order 10501, (1953) to classify documents and information. See e.g., 18 U.S.C. 798; 50 U.S.C. 783, (and see footnote 3 on p. 743).

tained in accordance with procedures provided by that directive. Another authority in this policy area is E.O. 10865 of 1960 which establishes the industrial security classification system used by defense contractors.

The Atomic Energy Act of 1946 (42 U.S.C. 2161-2166) provides for the protection of sensitive information, referred to as "restricted data," regarding the production of atomic energy.

Under the authority of the National Security Act of 1947 (50 U.S.C. 403(d)(3) and 403g) the Director of the Central Intelligence Agency bears a responsibility for protecting intelligence sources and methods. This authority implies an information security arrangement.

And, under the terms of certain regional defense treaties and international organization affiliations, the United States is required to maintain information received from allies in a protected status. Thus, treaties and executive agreements may serve as authority for a classified information arrangement. 15/

With regard to executive branch discretion for establishing policy in this area, Congress has not only deferred to Presidential initiative in certain expressions of classification policy, but has also given recognition to the existence of such policy in statutory pronouncements.

15/ See Herbert Lewis. Safeguarding Classified Information. Defense Management Journal, v. 9, Oct. 1973: 29-31, 62.

Nevertheless, the legislative branch maintains it has not relinquished its initiative to act on these matters or diminished its authority for ultimately determining policy regarding security classification procedures. 16/

In addition to national security classification markings and protection procedures, executive branch departments and agencies use a variety of additional labels and attendant information control practices which either supplement the arrangements prescribed in the President's classification order or constitute a parallel regulation system of administrative safeguards. 17/ There is no clear statutory authorization for these markings and protection procedures. Arguments have been offered that the President's classification order, by not directly prohibiting such supplemental labels, allows their creation and use. Administrative control markings, so the rationale goes, are a logical development of records management discretion granted to the executive branch in the "housekeeping" statute (5 U.S.C. 301), the Federal Records Act (44 U.S.C. 3101-3107), or both. These markings,

---

16/ See U.S. Congress. House. Committee on Government Operations. Security Classification Reform. Hearings, 93rd Congress, 2d session. Washington, U.S. Govt. Print. Off., 1974, pp. 289-294.

17/ Samples of these markings are identified in U.S. Congress. House. Committee on Government Operations. U.S. Government Information Policies and Practices -- Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7). Hearings, 92d Congress, 2d session. Washington, U.S. Govt. Print. Off., 1972, pp. 2929-2938.

their control systems, and their basis of creation, in many regards, are of little significance outside of the executive branch. Fairly definite legal authority must exist to prohibit the disclosure of information. 18/ Such labels as those discussed here, at best, are indicators that a record or document, so marked, has been deemed "sensitive" and precautions against its general circulation may be warranted.

Three essential considerations underlie contemporary security classification and information regulation efforts. First, criteria must be determined which connote what types of information are deserving of protection and the reasons for such limitations. Thus, personally identifiable information might be safeguarded for reasons of personal privacy in the case of the individual citizen, national security in the case of an intelligence operative, or law enforcement in the case of an undercover investigator or an informer.

Next, the duration of control must be determined. What is a reasonable period of time to officially protect information -- for the life of a particular record or file, for the normal longevity of a human being, until events either indirectly usurp the substance or directly reveal the details of a secret? A few years ago, a panel

---

18/ The denial of information under the Freedom of Information Act (5 U.S.C. 552) requires the identification of legal authority justifying such action, including specific statutes apart from the F.O.I. Act's own exemptions.

of experts at the Defense Department, recognizing the technological and scientific capabilities of the major world powers as well as modern intelligence techniques, concluded "that it is unlikely that classified information will remain secure for periods as long as five years, and it is more reasonable to assume that it will become known by others in periods as short as one year through independent discovery, clandestine disclosure or other means." 19/ The President's current order (E.O. 12065) on security classification prescribes separate control periods for every document and divorces temporal protection considerations from the application of sensitivity labels ("Top Secret," "Secret," and "Confidential").

Third, having established that certain information has become an official secret, how is such material to be regulated in terms of its availability? Two considerations must be addressed regarding this point: what "need-to-know" justifications are in order to warrant access to protected materials and what amount or kinds of physical safeguarding are appropriate?

Because perceptions and judgments on these three concerns may well differ, the President has issued an Executive order on security classification to assure a degree of unity in administration on such matters.

19/ U.S. Department of Defense. Office of the Director of Defense Research and Engineering. Report of the Defense Science Board Task Force on Secrecy. Washington, Department of Defense, 1970, p. 1.

Congress, of course, is not bound by this Executive order and committees within the two Chambers may have differing views from those of the executive branch regarding the creation and maintenance of Government secrets. Such attitudes have consequences for the transfer of sensitive information from the departments and agencies to the Legislature.

Development of executive-congressional relations concerning committee receipt of controlled information

Congressional requests for and receipt of executive branch records and documents occur in a continuously changing political environment and against a background of constitutionally separated powers which are subject to a degree of interpretation and modification. Oftentimes the political elements of a controversy between the Legislature and the President cannot be distinguished from the constitutional aspects, or vice versa. No where is this blur of arguments more apparent than in matters of information transfer by the executive to Congress. It may be argued that the heat and furor of such disputes rises in relationship to the degree of sensitivity of the records in dispute, reaching an explosive crescendo with a congressional subpoena duces tecum confronting a Presidental claim of "Executive privilege." Such constitutional tumults are both classic and rare: they depict the Executive and Congress in their full power, but they are usually avoided through political accommodations and compromise.

In receiving sensitive information from the executive branch, a congressional committee may elect to protect such material, regardless of whether or not it is regulated or classified, in order to guard

against assertions that it was disclosed improperly -- leaked--by the panel. Without a good faith effort on the part of a committee to safeguard sensitive documents, the executive branch, for a variety of noble or ignoble reasons, may allege that such records have been managed irresponsibly and Congress is untrustworthy. When material is labeled as to its classified or regulated status, then any plea of ignorance as to its sensitivity is irradicated. Thus, when certain protected information was thought to have been leaked by the House Select Committee on Intelligence, President Ford formally invoked executive privilege on September 12, 1975, refusing to further supply copies of classified documents to the panel, disallowing any executive branch witness to again testify before the unit on matters under security safeguard, and demanding the return of classified items then in the Committee's possession.

As part of the good faith effort to assure the executive branch that sensitive information will be protected properly, many committees of Congress have adopted special rules regarding the management of such materials. Some panels receive sensitive documents under executive session procedures, avoiding questions about the propriety of or reasons for executive branch classification or regulation. 20/

20/ When and under what circumstances congressional committees began using executive sessions is uncertain. According to one authoritative commentator, secret committee meetings were a carry-over from the British experience and we are reminded that public committee proceedings of any kind are a relatively recent phenomenon: "Committees frequently open their meetings to the public, which results in wide publicity before their recommendations are presented to the House, but in general the old practice of Parliament is followed and committee meetings are not public." Asher C. Hinds. Hinds' Precedents of the House of Representatives of the United States., v. IV. Washington, U.S. Govt. Print. Off., 1907, p. 926n.

Other committee rules appear to accept the condition that if a record is classified, it must be protected.

Less a matter of good faith and more a precondition to receiving classified materials, congressional committee staff handling safeguarded documents undergo background checks certifying their good character. This practice has troublesome implications of a separation-of-powers nature: should investigative agencies of the executive branch -- such as the Federal Bureau of Investigation or the Defense Investigative Service -- be given a mandate to probe the private lives of congressional staff who may be pursuing oversight, authorization, or appropriation activities bearing upon these same entities? To avoid this imbroglio, Rep. Jack Brooks, Chairman of the House Committee on Government Operations, developed an alternative staff clearance procedure early in the 94th Congress:

> Instead of having the Defense Department investigate and clear staff members, the committee uses the Civil Service Commission to gather information about them, and the General Accounting Office to evaluate that information. The clearance is then granted or denied by the committee chairman.
>
> All the reports and papers generated by the field investigation and the evaluation are turned over to the chairman and stored in the committee's security safe. 21/

Since this procedure went into effect in August, 1975, only one agency has questioned its validity and that doubt was eased when the the White House indicated its full faith in the arrangement. Today

---

21/ House Government Operations Issues Own Security Clearances, Staff, v. 1, 95th Congress, Issue 5:1.

the Committee on Government Operations, the Committee on Interstate and Foreign Commerce, and the Committee on House Administration utilize this approach to staff security clearances for some segment of their personnel. (The details of the process and its cost appear infra.)

One additional consideration might be entertained in this overview of congressional committee management of sensitive information in the context of overall executive-congressional relations. Capitol Hill leaks of classified information not only can stimulate damaging charges of irresponsibility having an adverse effect upon public opinion, but may prompt the President to invoke a claim of executive privilege against Congress whenever official secrets are sought. This was the position taken by President Ford in his September, 1975, cut-off of classified materials for the House Select Committee on Intelligence. The Supreme Court also seemed to suggest in United States v. Nixon that "a claim of need to protect military, diplomatic or sensitive national security secrets" might constitute a special type of executive privilege plea which the Court would regard more favorably than other justifications for the President's injunction. 22/ While the Court was addressing "only the conflict between the President's assertion of a generalized privilege

---

22/ United States v. Nixon, 418 U.S. 683, 706 (1974).

of confidentiality against the constitutional need for relevant evidence in criminal trials" in this opinion, 23/ there is an implication posited which may go untested without harm to any branch as long as the basic security expectations of the executive branch are met by congressional committees.

House, Senate and committee rules

While virtually any congressional committee may find itself in need of executive branch information under security classification or in some other type of protected status, about twenty-nine panels of the 95th Congress appear to have had rules directly bearing upon the management of such material when it was in their possession. A total of forty-one committees of the same Congress had rules regarding executive sessions, signifying that sensitive information could be safeguarded under this procedure. These panels and their relevant rules are identified in Table I. 24/

23/ See Ibid., p. 712 at note 19.

24/ See Appendix A for the text of these and other relevant committee rules.

TABLE I
Principal Committee Rules Regarding Sensitive Information Management
95th Congress

Committee	Executive Session	Specific Management
H. Agriculture	Sec. IIe	Sec. III k
H. Appropriations	Sec. IIIh, IIIk Sec. 4(d) Sec. 5(a), (b)(1)	
H. Armed Services		
Full committee	Rule 13	Rule 7
Subcommittees	Rule IV, XIII	Rule XIII
H. Banking, Finance & Urban Affairs	Rule II(f), VII	Rule VII(g)(7)
H. Budget	Rule 3, 10, 20	Rule 20
H. District of Columbia	Rule G, J(7)	Rule J(7)
H. Education and Labor	Rule 1(d)	
H. House Administration	Rule 3, 8(f)(7)	Rule 8(f)(7)
H. Interior and Insular Affairs	Rule 2(c), 5(b)	
H. International Relations (Foreign Affairs)	Rule 4	Rule 19
H. Interstate and Foreign Commerce	Rule 2(e)	
H. Judiciary	Rule IId	
H. Merchant Marine and Fisheries	Rule II(B), V(A)	Rule V(A)
H. Post Office and Civil Service	Rule 3(d)	Rule 20
H. Public Works and Transportation	Rule II(f), VII (g)(7)	Rule VII(g)(7)
H. Rules	Rule 1(c)	
H. Science and Technology	Rule B22, B23	
H. Small Business	Rule 4(A)	Rule 15
H. Standards of Official Conduct		Rule 15

Table I - continued

Committee	Executive Session	Specific Management
H. Veterans' Affairs	Rule II(c)	
H. Select Aging	Rule 16	
H. Select Assassinations	Rule 2.3, 3.3(7)	Rule 3.3(7), 10, 11.1-11.5
H. Select Congressional Operations	Rule 7, 9, 14	Rule 9
H. Ad Hoc Energy	Rule 3, 8(e)(7)	Rule 8(e)(7)
H. Select Ethics	Rule II(e)	
H. Select Intelligence	Rule 3, 8	Rule 8, 9, 10
H. Select Narcotics Abuse and Control	Rule 4(b)	
H. Ad Hoc Select Outer Continental Shelf	Rule IIA, IVA	Rule IVA
S. Armed Services	Rule 4, 9(d), 9(f)	Rule 9(f)
S. Banking, Housing and Urban Affairs	Rule 2(c), 3(e), 8	Rule 2(3), 3(e)
S. Budget	Rule 1(2)	
S. Energy and Natural Resources	Rule 10	Rule 10
S. Environment and Public Works	Rule 3	
S. Foreign Relations	Rule A2, E, G9(d)	Rule E, F, G9(d)
S. Governmental Affairs	Rule 5B	
S. Rules and Administration	Title I-2	
S. Select Ethics	Rule 11	Rule 11
S. Select Indian Affairs		Rule 9
S. Select Intelligence	Rule 10.5-10.8	Rule 9, 10.5-10.8
S. Select Nutrition and Human Needs	Rule 2, 3(b), 3(d)	Rule 3(d)
S. Select Small Business	Rule 3(3)	Rule 3(e)
Jt. Defense Production	Rule 4	Rule 4
Jt. Economic	Rule 8, 12	Rule 12, 16, 23

In addition, the Senate, but not the House of Representatives, has a general rule requiring that confidential communications made by the President to the chamber shall be kept secret by its Members and officers. 25/ The comparable House rule sets procedures for receiving confidential communications but, unlike the Senate counterpart, contains no provision requiring that such information shall be kept secret by Members. 26/

25/ Rule 36, clause 3; appears as Section 36.3 in the Senate Manual for the 95th Congress; this rule was adopted (Senate Executive Journal, December 22, 1800, p. 361) in the midst of controversy surrounding President John Adams' convention with France and was, therefore, initially designed to regulate treaties and attendant papers submitted to the Senate by the Chief Executive; see U.S. Congress. Senate. The United States Senate, 1787-1801 by Roy Swanstrom. Washington, U.S. Govt. Print. Off., 1961, pp. 191-192. (87th Congress, 1st session. Senate. Document No. 87-64)

In addition, in 1953, the Senate adopted a resolution requiring a loyalty check to be made on any person appointed to serve as a Senate employee, thus initiating a minimal security investigation of every individual working for a Senator, Senate committee, or Senate officer (see Senate Journal, 83rd Congress, 1st session, p. 144). Loyalty checks, their frequency and relationship to security clearances, are discussed infra.

26/ See Rules of the House of Representatives, 95th Congress, Section 914 (Rule 29); according to annotations on the rule, it was initially adopted in a somewhat different form in 1792 (Journal of the House of Representatives [Gales and Seaton ed.], February 17, 1792, p. 510) and secret sessions "continued to be held at times with considerable frequency until 1830" but the rule rarely has been used since that time; see Hinds, op. cit., vol. V, section 7247; also see Clarence Cannon. Canon's Precedents of the House of Representatives of the United States. v. VI. Washington, U.S. Govt. Print. Off., 1935, section 434.

In January, 1820, the Senate agreed that when "acting on confidential or executive business" the chamber should be cleared of all persons except the senators themselves, the secretary, the sergeant-at-arms, and other necessary officers. A new rule adopted in May, 1844, provided that a member of the Senate convicted of disclosing for publication any written or printed matter designated by the Senate as confidential would be liable to expulsion. Any officer guilty of such an offense would be subject to dismissal. In 1868 an amendment to the rules specifically enjoined secrecy upon remarks, votes, and proceedings dealing with treaties, as well as upon the actual texts and relevant communications from the President. At the same time the Senate voted to require that all of its officers be

---

Another rule of the House which is of interest here is Section 706(c) (Rule 11, 2, (e), (2)) which, in relevant part, reads:

> . . .committee. . .records shall be the property of the House and all Members of the House shall have access thereto, except that in the case of records in the Committee on Standards of Official Conduct respecting the conduct of any Member, officer, or employee of the House, no Member of the House (other than a member of such committee) shall have access thereto without the specific, prior approval of the committee.

According to annotations on the rule, this paragraph "derives from section 202(d) of the Legislative Reorganization Act of 1946 (60 Stat. 812), was made a part of the rules on Jan. 3, 1953 (H. Res. 5, 83rd Congress, p. 24), and was amended on Jan. 4, 1977 (H. Res. 5, 95th Cong., p. -) to restrict the access of Members to certain records of the Committee on Standards of Official Conduct."

A later portion of the annotation notes: "While all Members have access to committee records under this clause, testimony or evidence taken in executive sessions of a committee is under the control and subject to the regulation of the committee and, under Rule XI, cl. 2(k)(7) §712, (infra, cannot be released without the consent of the committee (Speaker pro tempore Mills, June 26, 1961, p. 11233). See also Deschler's Procedure (93d Cong.), ch. 17, §15."

> sworn to secrecy when acting on confidential or executive business. A few years later even the lamplighter functioning in "the loft over the Senate Chamber during executive sessions" was required to take a similar oath. 27/

In addition to these efforts regarding the Senate chamber, by 1884 at least one committee had inaugurated special precautions for safeguarding privileged treaty materials: the Committee on Foreign Relations required that each member of the panel sign a receipt before obtaining a copy of the proposed agreement with Nicaragua providing for the construction of an interoceanic canal across its territory. 28/ Later, the panel's members were denied access to this document and attendant papers except during a committee meeting; at the conclusion of each session on the treaty, the materials were locked in the chairman's safe. 29/

> Despite the precautions which it took prior to 1929 the Senate was never wholly successful in keeping matters related to its executive sessions secret. A systematic, though by no means exhaustive, survey of the leading newspapers of the country, checked against official records now available to the public, has revealed the fact that in literally hundreds of cases news of such proceedings had been published long before the injunction of secrecy was removed. To determine the exact number, even if it were possible, would serve no useful purpose whatever. 30/

27/ R. Earl McClendon. Violations of Secrecy in Re Senate Executive Sessions, 1789-1929, American Historical Review, v. 51, October, 1945: 36.

28/ Ibid., p. 45.

29/ Ibid., p. 46.

30/ Ibid., p. 37.

While public sources do not immediately reveal any cases when a Member or staff of the Senate were punished for disclosing protected committee papers, there are two recorded instances when a Senator was censured for revealing documents confidentially communicated to that chamber by the Chief Executive. Having read a letter from French Foreign Minister Charles Talleyrand to his colleagues in open session, even though the communique was still under an injunction of secrecy, Senator Timothy Pickering was censured on January 2, 1811, for violating the rules of the Senate. Three decades later, Senator Benjamin Tappan was censured on May 10, 1844, and nearly expelled, for having given a confidential letter from President John Tyler, pertaining to the Texas annexation treaty and received in executive session, to another individual for subsequent publication in the New York Evening Post. Because Tappan apologized to his colleagues for his offense, efforts to expel him were withdrawn. However, as a consequence of this case, the Senate adopted an amendment to its executive session rule (Rule 36.4) providing that, when the secret or confidential business or proceedings of the Senate are disclosed, an offending Senator would be liable to expulsion and a Senate officer might suffer dismissal and punishment for contempt. 31/

31/ See U.S. Congress. Senate. Committee on Rules and Administration. Senate Election, Expulsion and Censure Cases from 1793-1972 by Richard D. Hupman, comp. Washington, U.S. Govt. Print. Off., 1972, pp. 6-7, 13-15. (92nd Congress, 1st session. Senate. Document No 92-7.)

While there have not been any censure actions in the House of Representatives with regard to a Member revealing documents confidentially communicated to that chamber by the President, there was concern evidenced a short time ago that a Member of that body might have improperly purchased classified information from persons not authorized to possess or otherwise sell such material. 32/ After exploring the matter, the House Armed Services Committee reported: "In view of the absence of any evidence which would support the allegations, we must conclude that there never were any classified documents, or materials extracted from classified documents, sold to Congressman [Harold] Runnels." 33/

In response to another matter involving a Member and classified information, the House Committee on Armed Services, in executive session, adopted a motion on June 10, 1975, which (1) obligated the chairman "to direct a formal request to the Committee on Standards of Official Conduct requesting guidance from that Committee as to the criteria which should apply for future access by Members of Congress to testimony received by the Committee [on Armed Services] in executive session and classified in-

---

32/ See U.S. Congress. House. Committee on Armed Services. Alleged Purchase of Classified Information by a Member of Congress. Hearings, 93rd Congress, 1st session. Washington, U.S. Govt. Print. Off., 1973.

33/ See U.S. Congress. House. Committee on Armed Services. Alleged Purchase of Classified Information by a Member of Congress: a Report. Committee print, 93rd Congress, 1st session. Washington, U.S. Govt. Print. Off., 1973, p. 10.

formation provided the Committee and maintained in the Committee files" and (2) established that, "pending an official response from the Committee on Standards of Offical Conduct to the Committee request, Congressman [Michael] Harrington be denied access to any committee files or classified information maintained therein because of his previous refusal to honor House and Committee Rules regarding material received by the the Committee [on Armed Services] in executive session." 34/ The chairman of the Armed Services Committee placed these matters before the Committee on Standards of Official Conduct in a letter dated June 11, 1975. A response, dated November 12, 1975, indicated that the Committee on Standards of Official Conduct "feels that to speak to a question involving the internal operation of a co-equal Committee of the House is a matter beyond its authority under House Rules." 35/ Under the terms of the Armed Services Committee motion of June 10, this offical response from the Committee on Standards of Official Conduct theoretically reinstated Representative Harrington's access to classified material held by the House Armed Services Committee. On November 6, 1975, the Committee on Standards of Official Conduct, by a 7-3 vote, dismissed a formal complaint against Representative Harrington for disclosing classified

---

34/ See U.S. Congress. House. Committee on Armed Services. Report to the Full Committee on Access by Member of Congress to Classified Material. Committee print. 94th Congress, 1st session. Washington, U.S. Govt. Print. Off., 1975, p. 2.

35/ Ibid., p. 3.

information, arguing that no rules of Congress had been violated because the session of the Armed Services Committee from which classified information derived had occurred in violation of House rules. 36/

One other point pertaining to congressional rules and their bearing upon the receipt and maintenance of classified information by the House or Senate derives from a precedent where the House refused to be bound by a Senate declaration of secrecy with regard to confidential communications, raising the possibility that one chamber might reveal information which the other body regarded as in some way protected. 37/

Part II. Toward a Model

The Gravel decision and the Senate Special Committee Report, 1973

In establishing new procedures regarding the management of classified information within the legislative branch, guidance may be drawn from a congressional interpretation of the United States Supreme Court's decision in Gravel v. United States, which still stands. 38/ The Senate Special Committee to Study Questions Related to Secret and Confidential Government Documents, in a 1973 report, said of the case:

> On the basis of the Gravel decision, it would seem possible to construct several categories of activities and conduct in which an individual Member may safely engage when he pos-

---

36/ New York Times, November 7, 1975.

37/ Hinds, op. cit., vol. V, section 7249.

38/ 408 U.S. 606 (1972).

sesses a classified document. However, before considering protected and proscribed conduct some analysis of the Gravel decision is in order.

Article I, section 6, clause 1, of the United States Constitution provides as follows:

> The Senators and Representatives shall receive a Compensation for their Services, to be ascertained by Law, and Paid out of the treasury of the United States. They shall in all Cases, except Treason, Felony, and Breach of the Peace, be privileged from Arrest during their Attendance at the Session of their respective Houses, and in going to and returning from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.

In writing for the Court majority, Mr. Justice White indicated that the Privilege from Arrest, guaranteed by the Article, extends only to a privilege from civil arrest (a practice common at the time the Constitution was adopted), and does not immunize Members from the operation of the ordinary criminal laws. Gravel v. United States, 408 U.S. 606, 614-615 (1972). Thus, a Member would be generally bound by the operation of those criminal laws which regulate conduct with respect to the handling of classified documents.

The Court's analysis of the scope of protection afforded Members by the last clause of Article 1, section 6, clause 1 (Speech and Debate Clause), however, has important implications for an individual Member in possession of a classified document. Explaining that the Speech and Debate Clause does not broadly exempt that which the Privilege from Arrest Clause allows (i.e., that Members are subject to the operation of the ordinary law), the Court nevertheless indicated that the former Clause was intended to protect the integrity of the legislative process and "assure a co-equal branch of the governmentwide freedom of speech, debate, and deliberation without intimidation or threats from the Executive Branch." Id., at 616. Moreover, this protection is broad enough to immunize Members "against prosecutions that directly impinge upon or threaten the legislative process." Id.

It is important to note that although a Member may be immune from the operation of the criminal law where his conduct is within the "sphere of legitimate legislative activity" (Id. at 624), the fact that a particular act in some way "related to" the legislative process is not necessarily a justification for immunity. Protection under the Speech and Debate Clause is available only where the Member's act is "clearly a part of the legislative process -- the due functioning of the process." United States v. Brewster, 408 U.S.,

515-516 (1972). The test for determining what conduct is within the protected "sphere of legitimate legislative activity" under the the Speech and Debate Clause was stated by Justice White as follows:

> Legislative acts are not all-encompassing. The heart of the Clause is speech or debate in either house. Insofar as the Clause is construed to reach other matters, they must be an integral part of the deliberative and communicative processes by which Members participate in committee and House proceedings with respect to the consideration and passage or rejection of proposed legislation or with respect to other matters which the Constitution places within the jurisdiction of either House. As the Court of Appeals put it, the courts have extended the privilege beyond pure speech or debate in either House, but "only when necessary to prevent indirect impairment of such deliberation." United States v. Doe, 455 F. 2d, at 760. Gravel v. United States, 408 U.S. 606, 625 (1972). 39/

The Gravel decision also determined that the scope of immunity available to a Member's aide is coextensive with that of the Member. 40/ Thus, any action by a Member's aide which would constitute a protected legislative act if done by the Member himself is immunized by this interpretation of the scope of the speech and debate clause. 41/ This

---

39/ U.S. Congress. Senate. Special Committee to Study Questions Related to Secret and Confidential Government Documents. Questions Related to Secret and Confidential Documents. Washington, U.S. Govt. Print. Off., 1973, pp. 9-10. (93rd Congress, 1st session. Senate. Report No. 93-466)

40/ Gravel v. United States, 408 U.S. 616-617 (1972); reaffirmed in Eastland v. United States Servicemen's Fund, 421 U.S. 491 (1975).

41/ In 1973, in Doe v. McMillian, 412 U.S. 306 (1973), the Supreme Court declared that the scope of immunity under the clause was applicable to committee employees to the same extent as that of Members.

should be borne in mind, the Special Committee stated, when considering certain types of behavior by a Member with regard to utilizing classified materials.

> In light of these conditions it seems appropriate to suggest several types of conduct which, in the case of an individual Member having possession of a classified document, should be protected under the Speech and Debate Clause. The following list is not intended to be exhaustive:
>
> 1. Any speech or debate on the Senate floor concerning the classified document.
> 2. Any speech during a committee meeting, hearing, etc.
> 3. Any reading from the classified document either on the Senate floor or in a committee meeting.
> 4. Any speech concerning the classified document in committee reports, hearings, or in resolutions.
> 5. Any placing of a classified document into the public record.
> 6. Any conduct at a committee meeting or on the Senate floor with respect to the classified document and any motive or purpose behind such conduct.
> 7. Any communications between a Member and aide during the term of the aide's employment with respect to the classified document if related to a committee meeting or other legislative act of the Member.
>
> As to those types of conduct for which it would seem no Speech or Debate Clause protection exists, the following, also not intended to be exhaustive, are illustrative:
>
> 1. Any act with respect to a classified document in preparation for a hearing which may be relevant to the investigation of third-party crime.
> 2. Any act with respect to a classified document in preparation for a hearing which is itself criminal, e.g., gathering defense information (18 U.S.C. Sec. 793).
> 3. Any act arranging for the private publication of a classified document.
> 4. Any act publishing a classified document privately.
> 5. Any speech or debate concerning the classified document delivered or conducted outside Congress; i.e., not in a committee or on the Senate floor.

6. Any transmittal or communication concerning the classified document in newsletters or news releases to constituents or in answering constituent mail.
7. Any disclosure of the classified document on radio or television appearances. 42/

In addition, the Senate Special Committee offered the following regarding the legal rights of individual Members with respect to documents or information received from foreign emissaries:

> Although it might be useful in some cases, to distinguish between information and documents received from foreign emissaries which have been classified by the United States government [see 50 U.S.C. secs. 783 (b) (c) and 18 U.S.C. sec. 798] and information and documents which are either unclassified or classified by a foreign government without a reclassification by the United States, it is perhaps equally important to note generally that under the Espionage and Censorship provisions of the Federal criminal code (18 U.S.C. secs. 792-799) it is a criminal act for any unauthorized possessor of any document "relating to the national defense" either 1) willfully to communicate or cause to be communicated that document to any person not entitled to receive it, or 2) willfully to retain the document and fail to deliver it to an officer of the United States entitled to receive it [see 18 U.S.C. sec 793 (e)]. Thus, under this prohibition both the source and the classification of the document are immaterial and any unauthorized possessor thereof faces grave risks.
>
> It may be concluded that where an individual member has received a document or information from a foreign emissary, and where such document or information may be within the intendment of applicable criminal provisions, there would seem to be two alternatives under the present law: 1) the member may use the document or information to the extent that his immunity from the criminal law under the Speech and Debate

---

42/ U. S. Congress. Senate. Committee to Study Questions Related to Secret and Confidental Government Documents. Questions Related to Secret and Confidental Documents. Washington, U.S. Govt. Print. Off., 1973, pp. 10-11. (93rd Congress, 1st. session. Senate Report No. 93-466)

Clause allows, or 2) he may comply with sections 4 (c) and (d) of Executive Order 11652, 37 Fed. Reg. (1972)... 43/

And with regard to declassification procedures, the Senate Special Committee said:

> The question of the method by which an individual member may declassify a document in his possession seems to yield two approaches under the present law. First, the member may effect a kind of "declassification" by utilizing the document in accordance with his privilege under the Speech and Debate Clause. A member could, for example, read from the classified document at a committee meeting as was done in Gravel. Strictly speaking of course, this protected conduct on the part of a member does not technically "declassify" the document but it does make the document public, effectively defeating the classification. However, experience indicated that such effective declassification may contribute to a marked reluctance on the part of executive department officials to tender restricted information in the future.
>
> A second alternative under present law for a member desiring to declassify a document in his possession is to submit the document to the appropriate government authority in accordance with section 1(d) of E.O. 11652.... Section 5 of E.O. 11652, contains the general declassification and downgrading guidelines.

43/ Ibid., p. 13; in addition, in P.L. 92-403, 1 U.S.C. 112b (1972), Congress sets limits on congressional access to international agreements, other than treaties, where, in the opinion of the President, public disclosure would be prejudicial to the national security of the United States. In such event, such agreements "shall not be transmitted to the Congress but shall be transmitted to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives under an appropriate injunction of secrecy to be removed only upon due notice from the President".

The Senate took no formal action with regard to this report.

House Committee on Committees Report, 1974

Shortly after the Senate Special Committee released its report, the House Select Committee on Committees offered the following new clause to Rule X in its 1974 report:

Handling of Classified Information

5. (a) All information and data whether written or oral received by any committee or Member of the House which is classified Secret or higher as a national security matter by the originator shall be deemed to have been received in executive session, and shall be subject to all the rules and procedures of the House which restrict the disclosure of activities conducted and matters presented in executive session. No such information or data shall be disclosed to any person other than a Member, except to those House employees who have been properly cleared and can demonstrate a need to have such information or data in the performance of their official duties as such.

(b) Any Member or employee receiving such classified information or data shall be notified of its classification and the restrictions on its disclosure. If in the judgment of the person providing the information or data there is special sensitivity (or in the case of a Member receiving the information otherwise than in the normal course of his committee participation) the Member or employee may be required to sign an acknowledgement that he or she understands and will abide by the restrictions on disclosure.

(c) Each Member or employee who receives or may receive classified national security information or data shall be provided with a security manual governing its use and protection, together with copies of applicable statutes on the protection of official secrets and penalties for unauthorized disclosure thereof. Such manual and the clearance standards and procedures for the House (which shall meet the same standards of protection as those applied in the executive branch) shall be prepared by the special committee on intelligence and concurred in by the Speaker and the minority leader.

(d) House employees (whether on committee staffs or on personal staffs of Members), before they may receive or be exposed to classified national security information or data, must be cleared by a process of investigation and certification which is appropriate to the level of sensitivity involved, following the criteria which apply in the executive branch.

(e) (1) When a Member receives classified national security information or data otherwise than in the course his or her committee activities, and believes it is over- or under-classified, he or she may request of the special committee on intelligence that such information or data (in the House) be declassified, or reclassified at another level, as appropriate.

(2) When a Member receives classified national security information or data in the course of his or her committee activites, and believes it is over- or under-classified, he or she may request consideration of a change in classification by the committee. If the committee by majority vote agrees to the change, it may request such change of the special committee on intelligence.

(3) The special committee on intelligence, if it agrees with any change requested under subparagraph (1) or (2), shall report its agreement with such change to the Speaker and the minority leader, and if they concur, the change shall automatically be made. If the decision of the special committee or the leadership is adverse to such change, an appeal may be taken to the floor, in closed door session, at the direction of a majority of any committee.

(4) Prior to any action by a Member or committee or the special committee on intelligence with respect to the reclassification of any information or data under this subparagraph, such reclassification shall be requested of the originator of the information, or data, with a response requested within a period of seven legislative days. Such action shall not be taken prior to the conclusion of such period except in case of an emergency requiring immediate consideration by the House. 44/

44/ U.S. Congress. House. Select Committee on Committees. Committee Reform Amendments of 1974. Washington, U.S. Govt. Print. Off., 1974, pp. 97-98. (93rd Congress, 2d session. House. Report No. 93-316)

While neither this provision nor a substitute was adopted by the House, the clause constitutes one of the fullest statements of possible procedure pertaining to the handling of security and/or intelligence information by Congress.

House Ethics Committee Report, 1976

Late in the 94th Congress, the House Committee on Standards of Official Conduct, in the course of reporting on its investigation into the unauthorized publication of the final report of the House Select Committee on Intelligence, offered the following recommendations:

> Legislation Dealing With Classification and Declassification of Security Information
>
> This Committee recommends that the Leadership of the House assign a Committee to promptly initiate research and study which will lead to establishing a classification system. This task should begin immediately.
>
> Disputes about classification and declassification of national security information will continue to cause difficulties, conflicts and confrontations, and impede the flow of vital information among the three Branches of Government unless there is a vehicle for resolving these disputes in an orderly manner.
>
> Specific criteria should be established to define the type of information which can be classified, how and when it can be declassified, and the selection of persons authorized to carry out these functions.
>
> Thought also should be given to providing a system whereby conflicts between the Branches over declassification can be resolved to preclude unilateral release of security information.
>
> House Rules Governing Classified Information
>
> This Committee recommends that the Leadership of the House direct an appropriate Committee to promptly undertake the drafting of new House rules applicable to all Members, Committees and employees of the House, concerning obtaining, retaining and using classified information.

> To insure uniformity in the execution of whatever rules result, this Committee suggests a small staff of professionals be recruited and trained as security officers, to function under the authority of the Speaker or perhaps the Sergeant-at-Arms. These individuals could be responsible for obtaining and controlling all classified documents sought by or in the possession of the House, its Members, Committees and employees.
>
> Secure depositories should be constructed within the House complex for the storage of all such records, to replace the current patchwork system whereby every Committee, old or new, has to devise its own ways and means and whereby individual Members and their staffs frequently have virtually no secure means of retaining classified data.
>
> The professional staff of security officers also could take over the responsibility of screening those applicants for security clearance in the House, again to replace the current system whereby Members and/or Committee Chairmen make the decision.
>
> This professional staff also could be used to conduct inquiries into leaks of information within the House, there being no present organization to handle this function.
>
> This Committee recommends the House consult the Executive Branch in establishing the proposed rules and suggested professional staff to draw on its knowledge and expertise in the area of security. 45/

There was no formal House action regarding this recommendation.

Senate Office of Classified National Security Information

The most recent congressional reform effort regarding the management of sensitive information is now an accomplished fact. In

---

45/ U.S. Congress. House. Committee on Standards of Official Conduct. Report on investigation pursuant to H. Res. 1042 concerning unauthorized publication of the report of the Select Committee on Intelligence. Washington, U.S. Govt. Print. Off., 1976, pp. 43-44. (94th Congress, 2d session. House Report No. 94-1754)

1977, in anticipation of the abolition of the Joint Committee on Atomic Energy and the attendant problem of what to do with the panel's collection of classified atomic energy "restricted data," an administrative office of the United States Senate was created to serve as a repository for this protected material. 46/ Given a two-year mandate, the Office of Classified National Security Information was granted authority:

> (1) upon application of any committee of the Senate, to perform the administrative functions necessary to classify and declassify information relating to the national security considerations of nuclear technology in accordance with guidelines developed for restriced data by the responsible executive agencies;
> (2) to provide appropriate facilities for hearings of committees of the Senate at which restricted data or other classified information is to be presented or discussed; and
> (3) to establish and operate a central repository in the United States Capitol for the safeguarding of restricted data and other classified information for which such Office is responsible.

By provision in the Legislative Branch Appropriations Act of 1978, the Office has been chartered until the end of 1980. 47/ Operating in the Capitol office of the defunct Joint Committee, the facility is under the direction of George F. Murphy, Jr., former executive director of the Atomic Energy panel, and has a staff of about a half dozen individuals.

46/ Created by S. Res. 252 adopted August 5, 1977.

47/ See 92 Stat. 772, Sec. 105.

Committee management considerations

The foregoing paragraphs discuss the background to considerations of congressional committee management of sensitive information: the executive branch has developed procedures for the identification of and administration of sensitive materials; relevant congressional rules and statutes exist bearing upon the handling of such records; 48/ a number of committees of Congress have adopted rules directly or indirectly regulating sensitive documents; 49/ and efforts at reform in this area also are apparent. In this narrative, attention is now devoted to the more finite concerns of congressional committee management of sensitive information. Particular points to be explored include protection practices, Member responsibilities, staff responsibilities, enforcement mechanisms and procedures, and archival considerations.

Protection practices

Having determined that it must have access to a sensitive document held by the executive branch, a congressional committee, in order to use the record in question, may have to pledge to protect its contents from public disclosure. If no such precondition is set, then the committee must determine whether or not the information at issue warrants safeguarding and, if so, if this should be accomplished by inspecting the material

---

48/ See Appendices B and C respectively.

49/ See Appendix A.

at its executive branch source rather than removing it or accepting a copy or facsimile and protecting it in committee offices. In the Senate there is also the alternative of depositing a sensitive document with the Office of Classified National Security Information.

If such sensitive records are kept in committee offices, the following physical safeguards may be pursued in whole or in part:

-- maintenance of a secure room or storage area
    -- with limited means of entry and exit;
    -- contained by locked doors;
    -- protected against unauthorized entry by alarms;
    -- resistant to fire or entry other than through doorways; and
    -- free of unauthorized surveillance devices.
-- maintenance of secure files
    -- with protective locks;
    -- resistant to fire or other than a determined effort at physical penetration;
    -- protected against unauthorized entry by alarms; and
    -- secured to the floor or wall.
-- sensitive document identification
    -- name of committee of custody imprinted on document;
    -- sensitivity indicator such as a
        -- warning label; and/or a
        -- control number.

These options are available for the physical management of sensitive information. In addition to these, there are certain administrative or monitor safeguards which also may be pursued in whole or in part, including:

-- appointment of a document clerk or security officer to specifically manage sensitive documents;

-- guards for the secure room or storage area with authority to check visitor identification and maintain a visitor log;

-- maintenance of a document log for each protected record indicating each document's committee issued control number and

  -- source of item;

  -- receipt date; and/or

  -- users of document with date and purpose of inspection;

-- on-site inspection only of committee held sensitive documents with no allowance for copying or reproduction of same;

-- limitations on staff access to sensitive materials by designating a small number of authorized users with others having a need-to-know criterion for access; and

-- periodic clearance of document log, sensitive documents no longer needed by committee either being returned to Executive Branch source or being properly destroyed (date and manner of disposal noted on document log).

Member responsibilities

A foremost consideration with regard to committee management of sensitive information is that protected records must be entrusted to Members of Congress serving on the panel in order that they may effectively utilize the information contained in such documents. The public

release of such safeguarded material contrary to the rules of either the House or the Senate or the particular committee in question of either chamber can result in the punishment of an offending Member by his or her colleagues. 50/ However, when sensitive papers are not clearly protected under any rules of the House or Senate, a Member may elect to publicly disclose such documents even though they are under some type of safeguard by executive branch standards and their release by a Member may prompt conflict between the branches over future congressional access to such material. Such disclosure could be accomplished without legal repercussions if it fell within the ambit of the Constitution's speech and debate clause (Article I, section 6, clause 1). The courts have construed this immunity narrowly, viewing it as extending to "speech or debate in either House" and matters which are "an integral part of the deliberative and communicative processes by which Members participate in committee and House proceedings with respect to the consideration and passage or rejection of proposed legislation or with respect to other matters which the Constitution places within the jurisdiction of either House." 51/ The Senate Special Committee to Study Questions Related to Secret and Confidential Government Documents does

---

50/ As will be discussed later, a Member, depending upon the manner in which protected information is disclosed, may be subject to criminal prosecution as well as punishment within his or her House of Congress.

51/ Gravel v. United States, 408, U.S. 606, 625 (1972).

not appear to have questioned this interpretation of the speech and debate clause in its 1973 report. 52/ The Joint Committee on Congressional Operations, however, was not favorably disposed to this view. After holding hearings on the legislative role of Congress in gathering and disclosing information, the panel pointedly noted:

> Such an attempt by the Court to tell the Congress what is its business reflects an unreasonable, if not unknowing, point of view. It likely reflects, as well, the fact that no Justice now sitting on the Court has ever held elective, legislative office. 53/

This divergency of opinion serves to indicate that the applicability of the immunity protection of the speech and debate clause in situations where it is invoked or said to apply with regard to the release of safeguarded information -- and here we are referring to records classified by the executive branch -- by a Member of Congress is somewhat unclear.

In terms of committee management of sensitive records, Members serving on the panel should be informed in each case that a document is protected and should be apprised of the nature of the relevant authorities

---

52/ See note 39.

53/ U.S. Congress. Joint Committee on Congressional Operations. The Constitutional Immunity of Members of Congress. Washington, U.S. Govt. Print. Off., 1974, p. 2 (93rd Congress, 2d session. Senate Report No. 93-896); also see -----. Constitutional Immunity of Members of Congress. Hearings, 93rd Congress, 1st session. Washington, U.S. Govt. Print. Off., 1973. 2 v.

conveying this privileged status -- i.e., executive branch order or regulation, congressional chamber and/or committee rule, and statutory provisions of law. Members, in turn, are responsible for knowing of the disclosure restrictions placed on information held by a committee on which they serve. 54/

Staff responsibilities

Continuing on the point discussed above, the leadership of a congressional committee bears a responsibility to identify sensitive information obtained from the executive branch and to inform both Members serving on the panel and committee employees as to which records are protected and the nature of the authorities conveying this privileged status. There is an additional obligation, as well, to establish and promulgate general rules or procedures regarding staff responsibilities in the use or handling of protected materials.

Usually the chairman and ranking minority member of a committee or, by delegation, the staff director or subcommittee leadership, determine which employees will have unrestricted access to safeguarded documents held by the committee and which personnel will have limited or need-to-know access to such material. While the ideal model would seem to be one

---

54/ As noted at the outset of this discussion, the focus here is upon problems confronting committees in protecting sensitive information and documents supplied by and often under classification restrictions of Federal departments and agencies and is not necessarily concerned with safeguarding confidential materials originated within Congress.

of designating a minimal number of individuals with unrestricted access privileges, basic management considerations recommend that the staff director, leader of the minority staff, chief counsel, certain supporting counsels, chief clerk, and certain supporting clerks of the full committee have unrestricted access as well as the staff director, counsel, chief clerk and a supporting clerk of each subcommittee. This arrangement establishes an operational foundation facilitating committee use of protected executive branch records. In brief, if the occasion suddenly arises wherein the committee must make use of safeguarded documents held by the departments or agencies, there are a minimal number of staff available to receive and manage such materials for Members serving on the panel. The determination as to which committee and subcommittee personnel shall have what type of access to sensitive papers is conditioned by the rigidity of secrecy desired, the volume of protected documents handled, and the suitability of staff for receiving safeguarded records for whatever purpose.

The personal suitability of employees for handling or actually using sensitive information held by a committee involves at least two different judgments. The first of these is a determination within the committee that an individual is trustworthy, i.e., that he or she is honest, can maintain confidences which may derive from the working environment, and will otherwise function in conformity with committee and House or Senate rules as well as the laws of the United States.

The second judgment usually pertains to official secrets created by the executive branch. In order to receive this type of material, a committee employee obtains a security clearance. Under present arrangements, the committee chairman presents the applications of staff members deemed to require such a clearance to the Federal Bureau of Investigation (FBI) which conducts the appropriate background investigation. 55/ When a congressional committee staff member seeks classified information from a department or agency, the suitability of that individual for receiving such sensitive material largely rests upon the background findings developed by the FBI. 56/ According to the Bureau, the average cost for a security investigation is approximately $2,200 per application but may be considerably higher if extensive field inquiries are necessary. This cost is borne by each committee for its own staff.

Because security clearances are expensive, the leadership of a committee with a large staff may wish to carefully identify only a limited number of personnel who will be authorized to handle executive branch classified documents.

55/ These are full field investigations which are suitable for granting the highest level of security clearance.

56/ Suitability alone does not guarantee access to classified materials; other factors involved in the determination to provide protected records might be the "need-to-know" justification for making the documents available or a determination that sensitive intelligence information is involved which requires absolute protection (see 50 U.S.C. 403(d)(3)).

If a committee seeks access to classified materials held only by the Department of Defense, then applications for staff security clearance may be submitted directly to it for processing. A background check is conducted by the Defense Investigative Service and, on the basis of these findings, a clearance may be issued.

As noted earlier, there was some concern in the House over the propriety of the FBI investigating congressional staff, for whatever purpose, and maintaining dossiers on these personnel. Seeking an alternative arrangement to the one involving the FBI, Chairman Jack Brooks of the House Committee on Government Operations established a different security clearance plan in 1975 using the Civil Service Commission (CSC) and involving the General Accounting Office (GAO).

> Under the Government Operations Committee procedure, the chairman requests necessary clearance investigations (top secret). The requests are channeled through GAO (a legislative branch agency) to CSC as GAO's agent in performing national security checks and full-field investigations on a reimbursable basis.
>
> Upon completion of the national security check, GAO advises the chairman for interim clearance or employment purposes.
>
> Upon completion of the full-field investigation, all reports and papers generated by CSC are sent to the Security Office of GAO. That office reviews the file and provides a written advisory opinion to the chairman as to the suitability of the individual for clearance. This opinion is based on criteria established in Executive Order No. 10450 issued in 1953, and as subsequently amended.
>
> The opinion -- and the file -- are sent to the chairman, who issues or declines clearance for the individual.

> In turn, the staff member is advised of the decision, in writing, by the chairman. A copy, for reference control purposes, is forwarded to GAO.
>
> Executive Branch agencies requiring security clearance verification receive it by contacting the Security Office at GAO. 57/

The average cost for such an investigation, which is charged to the committee requesting it, is, according to the Security Office at GAO, approximately $800 per application. This figure increases in direct proportion to the amount of time and field inquiry necessary to complete the background check.

In addition to these judgments of the suitability of congressional employees for handling or actually using sensitive information held by a committee, the Standing Orders of the Senate have contained a provision since 1953 requiring that:

> . . .when any person is appointed as an employee of any committee of the Senate, of any Senator, or of any office of the Senate the committee, Senator, or officer having authority to make such appointment shall transmit the name of such person to the Federal Bureau of Investigation, together with a request that such committee, Senator, or officer be informed as to any derogatory and rebutting information in the possession of such agency concerning the loyalty and reliability for security purposes of such person, and in any case in which such derogatory information is revealed such committee, Senator, or officer shall make or cause to be made such further investigation as shall have been considered necessary to determine the loyalty and reliability for security purposes of such person.

57/ House Government Operations Issues Own Security Clearances, Staff, v. 1, 95th Congress, Issue 5:1.

> Every such committee, Senator, and officer shall promptly transmit to the Federal Bureau of Investigation a list of the names of incumbent employees of such committee, Senator, or officer together with a request that such committee, Senator, or officer be informed of any derogatory and rebutting information contained in the files of such agency concerning the loyalty and reliability for security purposes of such employee. 58/

The information resulting from this investigation could be utilized by a Senate committee in determining whether or not a prospective employee is trustworthy. The loyalty check authorized by this provision is not necessarily considered in security clearances of congressional committee staff to receive classified information from the executive branch but the loyalty of an individual, in and of itself, is examined in any security clearance investigation. Accurate information as to the extent to which loyalty checks, as required by the Standing Orders, are pursued is not available but it would appear that there is not a high degree of compliance with this provision.

As an additional condition of employment, committee staff may be required to sign an oath to the effect that they will not reveal sensitive information held by their panel in a protected status. This is not an agreement with any governmental entity outside of the legislative branch, thereby avoiding any breach of the separation of powers doctrine of the Constitution. Any failure to honor such an oath creates a breach of con-

---

58/ During the past few Congresses, this provision has appeared as Section 76 of the Senate Manual.

tract and can result in immediate punishment including a dismissal from employment. Both the House Permanent Select Committee on Intelligence and the Senate Committee on Intelligence use an information secrecy oath arrangement.

Finally, the leadership of a committee staff bears a responsibility to provide, and the personnel bear a responsibility to acquire, training regarding the proper handling and use of protected records and documents. Such an education might focus not only upon factual and procedural matters, but could include some appreciation, as well, for the purposes of and criteria for security classification as practiced within the executive branch, the reasons why sensitive information is safeguarded by the committee, and the consequences for publicly disclosing such materials.

Enforcement mechanisms and procedures

Efforts at disciplining or punishing a Member of Congress for improperly disclosing protected information held by a congressional committee undoubtedly will be conditioned by the circumstances of the release and the nature of the authority which has been violated. In light of the broad view of the speech and debate clause expressed by the Joint Committee on Congressional Operations in its 1974 report on the constitutional immunity of Members, 59/ it does not seem likely that a Represen-

---

59/ See note 53.

sentative or Senator would be challenged by colleagues on the propriety of disclosing protected records so long as such an action appeared to be within the ambit of the immunity clause and neither breached a congressional rule safeguarding the material in question nor resulted in a criminal conviction. As noted earlier, in two instances Senators were called to question and censured by their colleagues for disclosing information protected under the rules of the chamber. In this regard, the importance of having specific rules on this matter and using them, in both the House and the Senate as well as their committees, becomes apparent.

Depending upon the circumstances of the situation, a disclosure of properly classified documents by a Member of Congress in an action outside of the ambit of the immunity clause of Article I of the Constitution could subject a Senator or Representative to criminal prosecution. 60/ Upon conviction, a Member of the House of Representatives could suffer the loss of certain privileges as set forth in H. Res. 128 of 1973 as follows:

> Resolved, That it is the sense of the House of Representatives that any Member of, Delegate to, or Resident Commissioner in, the House of Representatives who has been convicted by a court of record for the commission of a crime for which a sentence of two or more years' imprisonment may be imposed should refrain from participation in the business of each committee of which he is then a member and should refrain from voting on any question at a meetings of the House, or of the Committee of the Whole House, unless or until judicial or executive proceedings result in reinstatement

---

60/ See Appendix C, particularly 18 U.S.C. 793, 18 U.S.C. 794, and 18 U.S.C. 798.

> of the presumption of his innocence or until he is reelected to the House after the date of such conviction. This resolution shall not affect any other authority of the House with respect to the behavior and conduct of its Members. 61/

There is no comparable limitation prescribed for a Senator convicted of a criminal act.

Questions as to whether or not a Member improperly has handled protected information must be carefully considered in the House by its Commmittee on Standards of Official Conduct.

In the Senate, the Select Committee on Ethics may exercise this responsibility under its authority in the Standing Orders "to receive complaints and investigate allegations of improper conduct which may reflect upon the Senate, violations of law, and violations of rules and regulations of the Senate, relating to the conduct of individuals in the performance of their duties as Members of the Senate, or as officers or employees of the Senate...." 62/ But only in the instance of a sworn complaint of such improper conduct, and in the case of unauthorized disclosure of intelligence information in the possession of the Select Committee on Intelligence, is the Ethics Commmittee compelled to probe improper releases of protected information by a Senator or Senate employee. Actions pursuant to a sworn complaint against a Member,

---

61/ See Congressional Record, v. 119, November 14, 1973: 36943-36944.

62/ During the past few Congresses, this provision has appeared in Section 79 of the Senate Manual.

officer, or staff person are conducted under specific and measured procedures. The Temporary Select Committee to Study the Senate Committee System noted its the April 1977, "Second Report" that "the Ethics Committee does not have explicit authority to investigate unauthorized disclosures by other [besides the Intelligence Committee] Members or offices of the Senate." "Nor, for that matter," the report said, "does any other committee." The panel concluded, saying:

> Not only do several Senate committees other than the Intelligence Committee routinely handle classified and confidential documents but also individual Senators and employees may receive such information independently of committees. Furthermore, it may be impossible to identify the source of a disclosure before an investigation is undertaken. For these reasons the Select Committee believes that responsibility in this area should be broadened and consolidated in a single committee. 63/

In the absence of clear and applicable Senate-wide rules governing the protection of sensitive information, it is possible an individual committee could establish procedures for handling violations of secrecy conditions by its own members. Nevertheless, no panel has done this and it is more likely that meaningful disciplining of Members committing such offenses would come from Senate-wide rules. The principal congressional deficiency in this regard, however, appears to be the lack of Sen-

---

63/ U.S. Congress. Senate. Temporary Select Committee to Study the Senate Committee System. Second Report with Recommendations - Operation of the Senate Committee System: Staffing, Scheduling, Communications, Procedure, and Special Functions. Committee print, 94th Congress, 2d session. Washington, U.S. Govt. Print. Off., 1977, p. 13.

ate guidelines for the handling of protected materials. Since the adoption of such prescriptions for the whole chamber does not seem to be imminent, the void, to some extent, may be filled by individual concerned committees establishing their own protection practices and policies.

Congressional staff employees are embraced by the immunity clause of Article I of the Constitution only to the extent they are assisting a Member in the performance of duties governed by the provision. 64/ If a legislative branch employee was to release protected information held by a committee on his or her own initiative, then that individual would be subject to disciplinary action by the chamber served, by the committee in question, or under the relevant laws of the United States. Committee personnel found to be improperly disclosing information under the panel's control could be punished directly by the committee or brought before either the House Committee on Standards of Official Conduct or, in the case of alleged release of Intelligence Committee materials, the Senate Select Committee on Ethics for investigation and recommendation of appropriate discipline. The Senate Ethics Committee considers complaints against employees, even sworn complaints, "according to procedures it deems appropriate." Punishment in such cases will depend upon findings and the gravity of the infraction and may include, but not be limited to, dismissal, suspension, or the forwarding of findings to the Justice Department for action.

64/ See Gravel v. United States, 408 U.S. 606 (1972); also see Doe v. McMillan, 412 U.S. 306 (1973).

In most cases involving an infraction against a particular committee's rules (excepting the Senate Intelligence Committee), the chairman of the panel involved would probably take direct action with regard to his or her own employees. Where a congressional staff member outside of a committee has breached information protection conditions established by that body, the matter is likely to be referred to the appropriate ethics committee for necessary action.

Archival considerations

At the close of each Congress, committees of the House of Representatives submit their records to the Clerk of the House in order that they may be deposited at the National Archives; Senate committees are under no requirement to so transmit their business papers but, as a matter of good records management, many panels regularly submit such materials to the Archives as well. Congressional committees maintain control over access and use of documents so entrusted to the National Archives and may recall items from their deposit at any time for whatever reason. As a final consideration in the matter of committee management of sensitive information, it may be desirable, for reasons of efficient document protection, to purge files of all safeguarded materials -- returning them to executive branch sources or destroying them -- before sending retired files to the Archives, preserving only those items deemed absolutely essential to the panel for direct future reference.

A document log will facilitate this process, identifying all sensitive records, their final disposition, and their historical relevance to the activities and operations of the committee.

Appendix A.

Selected Committee Rules Regarding the Management of Sensitive Information

Part I. Defunct Rules

House Committee on Foreign Affairs, 94th Congress, Rule 15

15. ACCESS TO CLASSIFIED INFORMATION

Access to classified information supplied to the Committee and attendance at closed sessions of the Committee or its subcommittees shall be limited to Members, and to members of the Committee staff and stenographic reporters who have appropriate security clearance when the Chairman determines that such access or such attendance is essential to the functioning of the Committee.

Notice of the receipt of classified documents submitted to the Committee by the Executive will be sent to Committee Members. Classified documents will be kept in the Committee safe and will be available to Members in the Committee office.

The Chairman of the full committee shall establish such other procedures as in his judgment may be necessary to prevent the unauthorized disclosure of any national security information received by the Committee classified as secret or higher. Such procedures shall, however, insure access to this information by any Member of the Committee or any other Member of the House of Representatives who has requested the opportunity to review such material. Such security procedures as are established by the Chairman may be modified or waived in any or all particulars by a majority vote of the full Committee.

House Committee on House Administration, 94th Congress, Rule 15

15. ACCESS TO CLASSIFIED INFORMATION

Access to classified information supplied to the Committee and attendance at closed sessions of the Committee or its subcommittees shall be limited to Members, and to members of the Committee staff and stenographic reporters who have appropriate security clearance when the Chairman determines that such access or such attendance is essential to the functioning of the Committee.

Notice of the receipt of classified documents submitted to the Committee by the Executive will be sent to Committee Members. Classified documents will be kept in the Committee safe and will be available to Members in the Committee office.

The Chairman of the full Committee shall establish such other procedures as in his judgment may be necessary to prevent the unauthorized disclosure of any national security information received by the Committee classified as secret or higher. Such procedures shall,

however, insure access to this information by any member of the Committee or any other Member of the the House of Representatives who has requested the opportunity to review such material. Such security procedures as are established by the Chairman may be modified or waived in any or all particulars by a majority vote of the full Committee.

House Committee on the Judiciary, 93rd Congress, Special Rules

PROCEDURES FOR HANDLING IMPEACHMENT INQUIRY MATERIAL

1. The chairman, the ranking minority member, the special counsel, and the counsel to the minority shall at all times have access to and be responsible for all papers and things received from any source by subpena or otherwise. Other members of the committee shall have access in accordance with the procedures hereafter set forth.

2. At the commencement of any presentation at which testimony will be heard or papers and things considered, each committee member will be furnished with a list of all papers and things that have been obtained by the committee by subpena or otherwise. No member shall make the list or any part thereof public unless authorized by a majority vote of the committee, a quorum being present.

3. The special counsel and the counsel to the minority, after discussion with the chairman and the ranking minority members, shall initially recommend to the committee the testimony, papers, and things to be presented to the committee. The determination as to whether such testimony, papers, and things shall be presented in open or executive session shall be made pursuant to the rules of the House.

4. Before the committee is called upon to make any disposition with respect to the testimony or papers and things presented to it, the committee members shall have a reasonable opportunity to examine all testimony, papers, and things that have been obtained by the inquiry staff. No Member shall make any of that testimony or those papers or things public unless authorized by a majority vote of the committee, a quorum being present.

5. All examination of papers and things other than in a presentation shall be made in a secure area designated for that purpose. Copying, duplicating, or removal is prohibited.

6. Any committee member may bring additional testimony, papers, or things to the committee's attention.

7. Only testimony, papers, or things that are included in the record will be reported to the House; all other testimony, papers, or things will be considered as executive session material.

RULES FOR IMPEACHMENT INQUIRY STAFF

1. The staff of the impeachment inquiry shall not discuss with anyone outside the staff either the substance or procedure of their work or that of the committee.

2. Staff offices on the second floor of the Congressional Annex shall operate under strict security precautions. One guard shall be on duty at all times by the elevator to control entry. All persons entering the floor shall identify themselves. An additional guard shall be posted at night for surveillance of the secure area where sensitive documents are kept.

3. Sensitive documents and other things shall be segregated in a secure storage area. They may be examined only at supervised reading facilities within the secure area. Copying or duplicating of such documents and other things is prohibited.

4. Access to classified information supplied to the committee shall be limited by the special counsel and the counsel to the minority to those staff members with appropriate security clearance and a need to know.

5. Testimony taken or papers and things received by the staff shall not be disclosed or made public by the staff unless authorized by a majority of the committee.

6. Executive session transcripts and records shall be available to designated committee staff for inspection in person but may not be released or disclosed to any other person without the consent of a majority of the committee.

House Select Committee on Intelligence, 94th Congress, Rule 7

RULE 7. PROTECTION OF PAPERS AND DOCUMENTS

7.1 All material and testimony received or obtained pursuant to House Resolution 138, 94th Congress, shall be deemed to have been received by the committee in executive session and shall be given appropriate safekeeping.

7.3 The Chairman in consultation with the ranking Minority Member of the committee shall, with the approval of the committee, establish such procedures as in his judgment may be necessary to prevent the unauthorized disclosure of all material and testimony received or obtained pursuant to House Resolution 138, 94th Congress. Such procedures shall, however, insure access to this information by any Member of the committee under such procedures as may be established by the committee.

7.3 Until such time as the committee has submitted its final report to the House, classified or other sensitive information in the committee records and files shall not be made available or disclosed to other than the committee membership and the committee staff, except as may be otherwise determined by the committee.

Senate Select Committee on Presidential Campaign Activities, 92nd Congress, Rule 27 and 40

Rule No. 27 - No testimony taken or material presented in executive session, or any summary or excerpt thereof shall be made available to other than the committee members and committee staff and no such material or testimony shall be made public or presented at a public hearing, either in whole or in part, unless authorized by a majority of the committee members or as otherwise provided for in these rules.

Rule No. 40 - All information developed by or made known to any member of the committee staff shall be deemed to be confidential. No member of the committee staff shall communicate to any person, other than a member of the committee or another member of the committee staff, any substantive information with respect to any substantive matter related to the activities of the committee. All communications with the press and other persons not on the committee staff in respect to confidential substantive matters shall be by members of the committee only. Official releases of information to the press on behalf of the committee shall be made only with the express consent of the Chairman and Vice Chairman.

Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, 94th Congress, Rule 7 and portions of Rule 9

RULE 7. PROCEDURES FOR HANDLING CLASSIFIED OR SENSITIVE MATERIAL

7.1 Committee staff offices on the first floor of the Dirksen Office Building shall operate under strict security precautions. At least one security guard shall be on duty at all times by the entrance to control entry. All persons before entering the offices shall identify themselves. At least one additional security guard shall be posted at night for surveillance of the secure area where sensitive documents are kept.

7.2 Sensitive or classified documents and material shall be segregated in a secure storage area. They may be examined only at secure reading facilities. Copying, duplicating, or removal from the Committee staff offices of such documents and other material is prohibited except as is necessary for use in, or preparation for, interveiws or Committee meetings, including the taking of testimony, and in conformity with Section 9.2 hereof.

7.3. Each member of the Committee shall at all times have access to all papers and other material received from any source. The Staff Director shall be responsible for the maintenance, under appropriate security procedures, of a registry which will number and identify all papers and other materials in the possession of the Committee, and such registry shall be available to any member of the Committee.

7.4. Access to classified information supplied to the Committee shall be limited to the Staff Director, the Chief Counsel and the Counsel to the Minority, and to those staff members with appropriate security clearances and a need-to-know.

7.5. No testimony taken including the names of witnesses testifying or material presented at an Executive Session, or classified papers, and other material received by the staff or its consultants while in the employ of the Committee shall be made public, in whole or in part or by way of summary, or disclosed to any person outside the Committee unless authorized by a majority vote of the entire Committee, or after the termination of the Committee, in such manner as may be determined by the Senate.

7.6. Before the Committee is called upon to make any disposition with respect to the testimony, papers, or other materials presented to it, the Committee members shall have a reasonable opportunity to examine all pertinent testimony, papers and other materials that have been obtained by the Committee staff. No member shall release any such testimony, papers, or other materials, or any information contained in such testimony, papers, or other materials, to the public or any person outside the Committee unless authorized by a majority vote of the entire Committee, or after the termination of the Committee, in such manner as may be determined by the Senate.

RULE 9. STAFF

9.3 The staff of the Committee shall not discuss either the substance or procedure of the work of the Committee with anyone other than a member of the Committee, or other Committee personnel. Upon termination of employment by the Committee, each member of the staff, or consultant, shall surrender all classified and other material relating to the work of the Committee which came into his possession while in the employ of the Committee.

9.4 The employment of any member of the staff or consultant who fails to conform to any of these Rules shall be immediately terminated.

Joint Committee on Atomic Energy, 94th Congress

Section 206. Classification of Information - The Joint Committee may classify information originating within the committee in accordance with standards used generally by the executive branch for classifying Restricted Data or defense information.

Section 207. Records - The Joint Committee shall keep a complete record of all committee actions, including a record of the votes on any question on which a record vote is demanded. All committee records, data, charts, and files shall be the property of the Joint Committee and shall be kept in the offices of the Joint Committee or other places as the Joint Committee may direct under such security safeguards as the Joint Committee shall determine in the interest of the common defense and security.

Joint Committee on Congressional Operations, 94th Congress, Rule 21

The information contained in any books, papers, or documents furnished to the committee by any individual, partnership, corporation, or other legal entity shall, upon the request of the individual, partnership, corporation, or entity furnishing the same, be maintained in strict confidence by the members and staff of the committee, except that any such information may be released outside of executive session of the committee if the release thereof is effected in a manner which will not reveal the identity of such individual, partnership, corporation, or entity: Provided, that the committee by majority vote may authorize the disclosure of the identity of any such individual, partnership, corporation, or entity in connection with any pending hearing or as a part of a duly authorized report of the committee if such release is deemed essential to the performance of the functions of the committee and is in the public interest.

Joint Committee on Defense Production, 94th Congress, Rule 4

4. No confidential testimony taken on confidential material presented at an executive hearing of the committee or subcommittee or any report of the proceedings of such an executive hearing shall be made public, either in whole or in part by way of summary, unless authorized by a majority vote of the committee.

Part II - Operative Committee Rules of 95th Congress

House Committee on Agriculture, Section III

No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the Committee.

House Committee on Armed Services, Full Committee Rule 7

Any prepared statement to be presented by a witness to the committee or a subcommittee shall be submitted to the committee at least 48 hours in advance of presentation and shall be distributed to all members of the committee or subcommittee at least 24 hours in advance of delivery. If a prepared statement contains security information bearing a classification of secret or higher, the statement shall be made available in the committee room to all members of the committee at least 24 hours in advance of delivery; however, no such statement shall be removed from the committee offices. The requirement of this rule may be waived upon a majority vote of the full committee or any subcommittee, a quorum being present.

All national security information bearing a classification of secret or higher which has been received by the committee or a subcommittee of the Committee on Armed Services shall be deemed to have been received by the committee in executive session and shall be given appropriate safekeeping.

The chairman of the full committee shall, with the approval of the full committee, establish such procedures as in his judgment may be necessary to prevent the unauthorized disclosure of any national security information received by the committee classified as secret or higher. Such procedures shall, however, insure access to this information by any member of the committee or any other Member of the House of Representatives who has requested the opportunity to review such material.

House Committee on Armed Services, Subcommittee Rule XIII

No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the committee (subcommittee). (House rule XI, clause 2(k)(7).)

(c) In the case of subcommittee majority staff, by the Chairman of the subcommittee;

(d) In the case of the subcommittee minority staff, by the ranking minority Member of the subcommittee.

No other individual shall be considered authorized persons, unless so designated by the Committee Chairman.

Designated persons--Each Committee Member is permitted to designate one member of his or her staff as having the right of access to classified information in the "confidential" category. Such designated persons must have the proper security clearance and a "need to know" as determined by his or her principal. Upon request of a Committee Member in specific instances, a designated person shall also be permitted access to information classified "secret" which has been furnished to the Committee pursuant to Section 36 (b) of the Arms Export Control Act, as amended. Designation of a staff person shall be by letter from the Committee Member to the Committee Chairman.

Location--Classified information will be kept in secure safes in the Committee rooms. All materials bearing the designation "top secret" must be kept in secured safes located in the main Committee offices, 2170 Rayburn Building. "Top Secret" materials may not be taken from that location for any purpose.

Materials bearing designations "confidential" or "secret" may be taken from Committee offices to other Committee offices and hearing rooms by Members of the Committee and authorized Committee staff in connection with hearings and briefings of the Committee or its sub-units for which such information is deemed to be essential. Removal of such information from the Committee offices shall be only with the permission of the Chairman of the full Committee, under procedures designed to insure the safe handling and storage of such information at all times.

Notice--Notice of the receipt of classified documents received by the Committee from the Executive will be sent promptly to Committee Members. The notice will contain information on the level of classification.

Access--Except as provided for above, access to classified materials held by the Committee will be in the main Committee offices in a designated "reading room". The following procedures will be observed:

(a) Authorized or designated persons will be admitted to the reading room after inquiring of the Chief of Staff or an assigned staff member. The reading room will be open during regular Committee hours.

(b) Authorized or designated persons will be required to identify themselves, to identify the documents or information they wish to view, and to sign the Classified Materials Log, which is kept with the classified information.

(c) No photocopying or other exact reproduction, oral recording, or reading by telephone, of such classified information is permitted.

(c) In the case of subcommittee majority staff, by the Chairman of the subcommittee;

(d) In the case of the subcommittee minority staff, by the ranking minority Member of the subcommittee.

No other individual shall be considered authorized persons, unless so designated by the Committee Chairman.

Designated persons--Each Committee Member is permitted to designate one member of his or her staff as having the right of access to classified information in the "confidential" category. Such designated persons must have the proper security clearance and a "need to know" as determined by his or her principal. Upon request of a Committee Member in specific instances, a designated person shall also be permitted access to information classified "secret" which has been furnished to the Committee pursuant to Section 36 (b) of the Arms Export Control Act, as amended. Designation of a staff person shall be by letter from the Committee Member to the Committee Chairman.

Location--Classified information will be kept in secure safes in the Committee rooms. All materials bearing the designation "top secret" must be kept in secured safes located in the main Committee offices, 2170 Rayburn Building. "Top Secret" materials may not be taken from that location for any purpose.

Materials bearing designations "confidential" or "secret" may be taken from Committee offices to other Committee offices and hearing rooms by Members of the Committee and authorized Committee staff in connection with hearings and briefings of the Committee or its sub-units for which such information is deemed to be essential. Removal of such information from the Committee offices shall be only with the permission of the Chairman of the full Committee, under procedures designed to insure the safe handling and storage of such information at all times.

Notice--Notice of the receipt of classified documents received by the Committee from the Executive will be sent promptly to Committee Members. The notice will contain information on the level of classification.

Access--Except as provided for above, access to classified materials held by the Committee will be in the main Committee offices in a designated "reading room". The following procedures will be observed:

(a) Authorized or designated persons will be admitted to the reading room after inquiring of the Chief of Staff or an assigned staff member. The reading room will be open during regular Committee hours.

(b) Authorized or designated persons will be required to identify themselves, to identify the documents or information they wish to view, and to sign the Classified Materials Log, which is kept with the classified information.

(c) No photocopying or other exact reproduction, oral recording, or reading by telephone, of such classified information is permitted.

(d) The assigned staff member will be present in the reading room at the option of the authorized person. Such staff member will be responsible for maintaining a log which identifies (1) authorized and designated persons seeking access, (2) the classified information requested, and (3) the time of arrival and departure of such persons. The assigned staff member will also assure that the classified materials are returned to the proper location.

(e) The Classified Material Log will contain a statement acknowledged by the signature of the authorized or designated person that he or she has read the Committee rules and will abide by them.

Divulgence--Any classified information to which access has been gained through the Committee on International Relations may not be divulged to any unauthorized person in any way, shape, form or manner. Apparent violations of this rule should be reported to the Chairman of the full Committee at once, and by him to the full Committee as promptly as possible.

Other regulations--So long as they do not conflict with any of the rules herein set down, the Chairman of the full Committee may establish other regulations and procedures as in his judgment may be necessary to safeguard classified information under the control of the Committee. Members of the Committee will be given notice of any such regulations and procedures promptly. They may be modified or waived in any or all particulars by a majority vote of the full Committee. Furthermore, any additional regulations and procedures should be incorporated into the written rules of the Committee at the earliest opportunity.

House Committee on Merchant Marine and Fisheries, Rule V(A)

Records and transcripts of open hearings before the Committee shall not be available to the public for quotation of any Member until after such Member has had an opportunity to examine and approve such records. Closed session transcripts and records shall be available to Members of the House and Committee staff for inspection in the office of the Committee, but may not be taken from the Committee offices by anyone.

House Committee on Post Office and Civil Service, Rule 20

(a) All classified material received by the committee or by a subcommittee shall be deemed to have been received in executive session and shall be given appropriate safekeeping.

(b) The chairman of the committee shall establish such procedures as in his judgment may be necessary to prevent the unauthorized disclosure of any such classified material. Such procedures shall, however, insure access to this information at the committee offices by any member of the committee or any other Member of the House of Representatives who has requested the opportunity to review such material.

House Committee on Public Works and Transportation, Rule VIII(g)(7)

No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the committee.

House Committee on Small Business, Rule 15

Access to classified information supplied to the committee and attendance at closed sessions of the committee or its subcommittees shall be limited to Members, and to members of the committee staff and stenographic reporters who have appropriate security clearance when the chairman determines that such access or such attendance is essential to the functioning of the committee.

The procedure to be followed in granting access to those hearings, records, data, charts, and files of the committee which involve classified intelligence information or information deemed by a subcommittee to be sensitive shall be as follows:

(a) Only Members of the House of Representatives may have access to such information.

(b) Members who desire to read materials that are in the possession of the committee should notify the clerk of the committee or the subcommittee possessing the materials.

(c) The clerk will maintain an accurate access log which identifies without revealing the material examined, the staff member involved, and the time of arrival and departure of all Members having access to the information.

(d) If the material desired is material which the committee or subcommittee deems to be sensitive enough to require special handling, before receiving access to such information, Members of the House will be required to identify the information they desire to read and sign an access information sheet acknowledging such access and that the Member has read these procedures.

(e) Such material shall not be removed from the room.

(f) A staff representative shall insure that the documents used by the Member are returned to the proper custodian or to original safekeeping as appropriate.

(g) No notes, reproductions or recordings may be made of any portion of such information.

(h) The contents of such information shall not be divulged to any person in any way, form, shape, or manner and shall not be discussed with any person who has not received the information in an authorized manner either under these rules or the laws or rules in effect for officials and employees of the executive branch.

(i) When not being examined in the manner described herein, such information will be kept in secure safes in the committee rooms.

(j) These procedures only address access to information the committee or a subcommittee deems to be sensitive enough to require special treatment.

(k) If a Member believes the material should not be classified or considered restricted as to dissemination or use, the Member may ask the committee or subcommittee to so rule; however, as far as materials and information in the custody of the Small Business Committee is concerned, the classification of materials as determined by the executive branch shall prevail unless affirmatively changed by the committee or the subcommittee involved, after consultation with the appropriate executive agencies.

(l) Other materials in the possession of the committee are to be handled in accordance with the normal practices and traditions of the committee and its subcommittees.

House Committee on Standards of Official Conduct, Rule 15

(a) the Chairman of the Committee shall, with the approval of the Committee, establish such procedures as in his judgment may be necessary to prevent the unauthorized disclosure of any information or testimony received by the Committee or its staff.

(b) Unless otherwise authorized by the Committee, the contents of a complaint and the fact of its filing shall not be disclosed publicly by any Member of the Committee or by the staff unless or until the Committee directs service of a copy of the complaint on the respondent under Rule 7(a)(1) for the purpose of obtaining a formal response or directs transmission of a statement of alleged facts and violation under Rule 9(b) for that purpose.

House Select Committee on Assassinations, Rule 3.3(7), portions of Rule 10, and 11.1-11.5

3.3(7) No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the Committee.

10.1 Before the commencement of any presentation at which testimony will be heard or papers and things considered, each Committee Member will be furnished with a list of all papers and things that have been obtained by the Committee by subpoena or otherwise. No Member shall make the list or any part thereof public unless authorized by a majority vote of the committee, a quorum being present.

10.2 The chief counsel, after discussion with the chairman and the ranking minority Member, shall initially recommend to the Committee the testimony, papers, and things to be presented to the Committee. The determination as to whether such testimony, papers, and things shall be presented in open or executive session shall be made pursuant to the rules of the House and of this Committee.

10.3 Before the Committee is called upon to make any disposition with respect to the testimony or papers and things presented to it, the Committee Members shall have a reasonable opportunity to examine all testimony, papers, and things that have been obtained by the inquiry staff. No Member shall make any of that testimony or those papers or things public unless authorized by a majority vote of the Committee, a quorum being present.

10.4 All examinations of papers and things other than in a presentation shall be made in a secure area designated for the purpose. Copying, duplicating, or removal of classified or other material deemed sensitive by the Committee is prohibited except where authorized by a Member.

10.6 Only testimony, papers, or things that are included in the record will be reported to the House; all other testimony, papers, or things will be considered as executive session material.

In addition to rules of conduct for staff contained in other rules of this Committee and the House, the following rules shall apply:

11.1 Staff offices of the Committee shall operate under strict security precautions. One guard shall be on duty at all times to control entry. All persons entering the Committee area shall identify themselves.

11.2 Classified or other materials the Committee deems sensitive shall be segregated in a secure storage area. Copying or duplicating of such documents and other things is prohibited except upon the authorization of a Committee Member.

11.3 Access to classified information supplied to the committee shall be limited by the Committee and chief counsel to those Committee staff members with appropriate security clearances and a need to know and to a designated personal staff member of each Committee Member, that personal staff member also having the appropriate security clearances and a need to know.

11.4 Testimony taken or papers and things received by the staff shall not be disclosed or made public by the staff unless authorized by a majority of the Committee.

11.5 Executive session transcripts and records shall be available to designated staff for inspection in person but may not be released or disclosed to any other person without the consent of a majority of the Committee.

House Select Committee on Congressional Operations, Rule 9

Testimony received in executive hearings shall not be released or included in any report without the approval of a majority of the committee.

House Ad Hoc Committee on Energy, Rule 8(e)(7)

No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the committee.

House Permanent Select Committee on Intelligence, Rule 8,9, and 10

RULE 8

The members of the Committee staff shall not discusss either the substance or procedure of the work of the committee with any person not a member of the committee or the committee staff for any purpose or in connection with any proceeding, judicial or otherwise, either during his tenure as a member of the committee staff or at any time thereafter except as directed by the committee in accordance with Section 7 of House Resolution 658 of the 95th Congress and the provisions of these rules, or, in the event of the termination of the committee, in such a manner as may be determined by the House.

No member of the committee staff shall be employed by the committee unless and until such a member of the committee staff agrees in writing, as a condition of employment, not to divulge any classified information which comes into his possession while he is a member of the committee staff or any information which comes into his possession by virtue of his position as a member of the committee staff to any person not a member of the committee or the committee staff, either during his tenure as a member of the committee staff or

at any time thereafter except as directed by the committee in accordance with section 7 of House Resolution 658 of the 95th Congress and the provisions of these rules, or in the event of the termination of the committee, in such manner as may be determined by the House.

The committee shall immediately consider disciplinary action to be taken in case any member of the committee staff fails to conform to any of these rules. Such disciplinary actions may include, but shall not be limited to, immediate dismissal from the committee staff.

RULE 9

In the case of any information classified under established security procedures and submitted to the committee by the executive or legislative branch, the committee's acceptance of such information shall constitute a decision by the committee that it shall not be disclosed unless the committee, by rollcall vote, determines that it wishes to disclose publicly a part or all of such information under the procedures set forth in clause 7 of Rule XLVII of the Rules of the House. For purposes of receiving information from either the executive or legislative branch, the staff director of the committee, or the chief counsel in his absence, may accept information on behalf of the committee.

RULE 10

Committee staff offices shall operate under strict security precautions. At least one security guard shall be on duty at all times by the entrance to control entry. Before entering the office all persons shall identify themselves.

Sensitive or classified documents and material shall be segregated in a secure storage area. They may be examined only at secure reading facilites. Copying, duplicating, or removal from the committee offices of such documents and other materials is prohibited except as is necessary for use in, or preparation for, interview or committee meetings, including the taking of testimony and in conformity with these rules.

Each member of the committee shall at all times have access to all papers and other material received from any source. The staff director shall be responsible for the maintenance under appropriate security procedures, of a registry which will number and identify all classified papers and other classified materials in the possession of the committee, and such registry shall be available to any member of the committee.

Pursuant to clause 7(c)(2) of House Rule XLVIII and to clause 2(e)(2) and clause 2(g)(2) of House Rule XI, Members who are not members of the committee shall be granted access to such hearings, records, data, charts and files of the committee and be admitted on a nonparticipatory basis to hearings of the committee, which involve classified material, on the basis of the following provisions:

(1) Members who desire to examine materials in the possession of the committee should notify the clerk of the committee in writing.

(2) Each such request by a member must be considered by the committee, a quorum being present, at the earliest practicable opportunity. The committee must determine by record vote whatever action it deems necessary in light of all the circumstances of each individual request. The committee shall take into account, in its deliberations, such considerations as the sensitivity of the information sought to the national defense or the confidential conduct of the foreign relations of the United States, the likelihood of its being, directly or indirectly disclosed and such other concerns--constitutional and otherwise--as affect the public interest of the United States. Such actions as the committee may take include, but are not limited to: (i) approving the request, in whole or part; (ii) denying the request; (iii) providing in different form than requested information or material which is the subject of the request.

(3) In matters touching on such requests, the committee may, in its discretion, consult the Director of Central Intelligence and such other officials as it may deem necessary.

(4) In the event that the member making the request in question does not accede to the determination or any part thereof of the committee as regards the request, that member should notify the committee in writing of the grounds for his or her disagreement. The committee shall subsequently consider the matter and decide, by record vote, what further action or recommendation, if any, it will take.

Whenever the select committee makes classified material available to any other committee of the House or Member of the House not a member of the committee, the clerk of the committee shall be notified. The clerk shall at that time provide a copy of the applicable portions of these rules and House Resolution 658 to such members or such committee and insure that the conditions contained therein under which the classified materials provided are clearly presented to the recipient. The clerk of the committee shall also maintain a written record identifying the particular information transmitted and the committee or Members of the House receiving such information. The staff director of the committee is further empowered to provide for such additional measures as he deems necessary in providing material which the committee has determined to make available to a Member of the House or a committee of the House.

Access to classified information supplied to the committee shall be limited to those committee staff members with appropriate security clearances and a need-to-know, as determined by the committee, and under the committee's direction, the staff director.

No member of the committee or of the committee staff shall disclose, in whole or in part or by way of summary to any person not a member of the committee or the committee staff for any purpose or in connection with any proceeding, judicial or otherwise, any testimony given before the committee in executive session, or the contents of any papers or other materials or other information received by the committee except as authorized by the committee in accordance with section 7 of House Resolution 658 of the 95th Congress and the provisions of these rules, or in the event of the termination of the committee, in such a manner as may be determined by the House.

Before the committee makes any decision regarding a request for access to any testimony, papers, or other materials in its possession, the committee members shall have a reasonable opportunity to examine all pertinent testimony, papers, and other materials that have been obtained by the committee.

House Ad Hoc Select Committee on the Other Continental Shelf, Rule IV.A

Records and transcripts of open hearings before the Select Committee shall not be available to the public for quotation of any Member until after such Member has had an opportunity to examine and approve such hearing records. Closed session transcripts and records shall be available to Members of the House and Select Committee staff for inspection, but may not be released or divulged to any other person without the consent of the Chairman or a majority of the Select Committee. In no event shall executive session or mark-up transcripts and records be taken from the possession of the Select Committee.

Senate Committee on Armed Services, Rule 9(f)

Confidential testimony taken or confidential material presented in a closed hearing of the committee or subcommittee or any report of the proceedings of such hearing shall not be made public in whole or in part or by way of a summary unless authorized by a majority vote of the committee or subcommittee.

Senate Committee on Banking, Housing and Urban Affairs, Committee Rule 2(c) and Subcommittee Rule 3(e)

2(c) Confidential testimony--No confidential testimony taken or confidential material presented at an executive session of the committee or any report of the proceedings of such executive session shall be made public either in whole or in part by way of summary, unless specifically authorized by the chairman of the committee and the ranking minority member of the committee or by a majority vote of the committee.

3(e) Confidential testimony--No confidential testimony taken or confidential material presented at an executive session of the subcommittee or any report of the proceedings of such executive session shall be made public, either in whole or in part or by way of summary, unless specifically authorized by the chairman of the subcommittee and the ranking minority member of the subcommittee, or by a majority vote of the subcommittee.

Senate Committee on Energy and Natural Resources, Rule 10

No confidential testimony taken by or confidential material presented to the committee or any subcommittee, or any report of the proceedings of a closed committee or subcommittee hearing or business meeting, shall be made public, in whole or in part or by way of summary unless authorized by a majority of the members of the committee at a business meeting called for the purpose of making such a determination.

Senate Committee on Foreign Relations, Rule E, F, and G9(d)

E. TRANSCRIPTS

1. The Committee on Foreign Relations shall keep verbatim transcripts of all committee and subcommittee meetings and such transcripts shall remain in the custody of the full committee, unless a majority of the committee decides otherwise. Publication of transcripts of public hearings by the committee shall be at the discretion of the chairman.

2. Maintenance and security of classified transcripts:
   (a) The chief clerk of the committee shall have responsibility for the maintenance and security of the classified transcripts.
   (b) A record shall be maintained of each use of the classified transcripts.

(c) Classified transcripts shall be kept in locked combination safes in the committee offices except when in active use by authorized persons. They must never be left unattended and must be returned to the chief clerk promptly when no longer needed.

(d) Classified transcripts shall be permitted to leave the committee offices only in the possession of authorized persons. Delivery and return shall be made only by authorized persons. They shall not be permitted to leave the city or the country unless adequate assurances are made to the chairman for their security.

(e) Transcripts classified secret or higher shall not be permitted to leave the committee offices.

(f) Extreme care should be exercised to avoid taking notes or quotes from classified transcripts.

3. Persons authorized to use classified transcripts:

(a) Members and staff of the committee, in the committee rooms, or, by permission of the chairman, in their offices.

(b) Senators not members of the committee and designated personal representatives of members of the committee with appropriate security clearances, in the committee's Capitol office, by permission of the chairman.

4. Declassification of executive transcripts and other executive records:

Executive transcripts and other executive records of the committee shall be released to the National Archives and Records Service for unclassified use in accordance with the policies of that Agency. However, no such transcripts or other executive records shall be declassified within a period of 12 years except by majority vote of the committee and with the permission of surviving members of the committee, at the time such transcripts or records were made and with the permission of the executive department, if any, concerned. After 12 years from the date such transcripts or records were made, they shall be declassified unless the committee by majority vote shall decide otherwise.

F. REGULATION FOR THE USE OF CLASSIFIED MATERIAL (OTHER THAN TRANSCRIPTS)

Receipt and distribution of classified material.

1. All classified material received or originated by the committee shall be keyed in at the committee's offices in the Dirksen Senate Office Building, and except for the material classified as "Top Secret" shall be filed in the Dirksen Senate Building offices for committee and use and safekeeping.

2. Each such piece of classified material received or originated shall be card indexed and serially numbered, and where requiring onward distribution shall be distributed by means of an attached indexed form approved by the chairman. If such material is to be distributed outside the committee offices, it shall, in addition to the attached form, be accompanied also by an approved signature sheet to show onward receipt.

3. Distribution of classified material among offices shall be by committee members or authorized staff only. All classified material sent to members' offices, and that distributed within the working offices of the committee, shall be returned to Room 4229, Dirksen Senate Office Building. No classified material is to be removed from the offices of the members or of the committee without permission of the chairman. Such classified material will be afforded safe handling and safe storage at all times.

4. Material classified "Top Secret," after being indexed and numbered, shall be sent to the committee's Capitol office for use by the members and authorized staff in that office only.

5. The chief of staff is authorized to make such staff regulations as may be necessary to carry out the provisions of these regulations.

G. STAFF REGULATIONS

The following concepts will guide the staff in its activities:
(d) The staff must under no circumstances discuss with anyone the proceedings of the committee in executive session or conversations with individual Senators without specific advance permission from the committee or the Senator concerned.

Senate Select Committee on Ethics, Rule 11

All testimony or action take in executive session shall be kept secret and shall not be released for public information without the approval of a majority of the committee.

Senate Select Committee on Indian Affairs, Rule 9

No confidential testimony taken by or confidential material presented to the committee or any report of the proceedings of a closed committee hearing or business meeting, shall be made public, in whole or in part or by way of summary, unless authorized by a majority of the members of the committee at a business meeting called for the purpose of making such a determination.

Senate Select Committee on Intelligence, Rule 9 and 10.5-10.8

RULE 9. PROCEDURES FOR HANDLING CLASSIFIED OR SENSITIVE MATERIAL

9.1 Committee staff offices shall operate under strict security precautions. At least one security guard shall be on duty at all times by the entrance to control entry. Before entering the office all persons shall identify themselves.

9.2 Sensitive or classified documents and material shall be segregated in a secure storage area. They may be examined only at secure reading facilities. Copying, duplicating, or removal from the the committee offices of such documents and other materials is prohibited except as necessary for use in or preparation for, interviews or committee meetings, including the taking of testimony, and in conformity with section 10.3 hereof.

9.3 Each member of the committee shall at all times have access to all papers and other material received from any source. The staff director shall be responsible for the maintenance, under appropriate security procedures, of a registry which will number and identify all classified papers and other classified materials in the possession of the committee.

9.4 Whenever the Select Committee on Intelligence makes classified material available to any other committee of the Senate or to any member of the Senate not a member of the committee, the clerk of the committee shall be notified. The clerk of the committee, shall maintain a written record identifying the particular information transmitted and the committee or members of the Senate receiving such information.

9.5 Access to classified information supplied to the committee shall be limited to those committee staff members with appropriate security clearances and a need-to-know, as determined by the committee, and under the committee's direction, the staff director and minority staff director.

9.6 No member of the committee or of the committee staff shall disclose, in whole or in part or by way of summary, to any person not a member of the committee or the committee staff for any purpose or in connection with any proceeding, judicial or otherwise, any testimony given before the committee in executive session including the name of any witness who appeared or was called to appear before the committee in executive session, or the contents of any papers or other materials or other information received by the committee except as authorized by the committee in accordance with section 8 of Senate Resolution 400 of the 94th Congress and the provisions of these rules, or in the event of the termination of the committee, in such a manner as may be determined by the Senate.

9.7 Before the committee makes any decision regarding the disposition of any testimony, papers, or other materials presented to it, the committee members shall have a reasonable opportunity to examine all pertinent testimony, papers, or other materials that have been obtained by the members of the committee or the committee staff.

RULE 10. STAFF

10.5 The members of the committee staff shall not discuss either the substance or procedure of the work of the committee with any person not a member of the committee or the committee staff for any purpose or in connection with any proceeding, judicial, or otherwise, either during his tenure as a member of the committee staff or at any time thereafter except as directed by the committee in accordance with section 8 of Senate Resolution 400 of the 94th Congress and the provision of these rules, or in the event of the termination of the committee, in such a manner as may be determined by the Senate.

10.6 No member of the committee staff shall be employed by the committee unless and until such a member of the committee staff agrees in writing, as a condition of employment to abide by the conditions of the nondisclosure agreement promulgated by the Senate Select Committee on Intelligence pursuant to section 6 of Senate Resolution 400 of the 94th Congress, 2d Session.

10.7 No member of the committee staff shall be employed by the committee unless and until such a member of the committee staff agrees in writing, as a condition of employment, to notify the committee or in the event of the committee's termination the Senate of any request for his testimony, either during his tenure as a member of the committee staff or at any time thereafter with respect to information which came into his possession by virtue of his position as a member of the committee staff. Such information shall not be disclosed in response to such requests except as directed by the committee in accordance with section 8 of Senate Resolution 400 of the 94th Congress and the provisions of these rules, or in the event of the termination of the committee, in such manner as may be determined by the Senate.

10.8 The committee shall immediately consider action to be taken in the case of any member of the committee staff who fails to conform to any of these rules. Such disciplinary action may include, but shall not be limited to, immediate dismissal from the committee staff.

Senate Select Committee on Nutrition and Human Needs, Rule 3(d)

No confidential testimony taken or confidential material presented in an executive hearing of the committee or any report of the proceedings of such an executive hearing shall be made public, either in whole or in in part or by way of summary, unless authorized by a majority of the members of the committee.

Senate Select Committee on Small Business, Rule 3(e)

No confidential testimony taken or confidential material presented in a closed hearing of the committee or any report of the proceedings of such a closed hearing shall be made public, either in whole or in part or by way of summary, unless authorized by a majority of the members of the committee.

Joint Committee on Defense Production, Rule 4

No confidential testimony taken or confidential material presented at an executive hearing of the committee or subcommittee or any report of the proceedings of such an executive hearing shall be made public, either in whole or in part by way of summary, unless authorized by a majority vote of the committee.

Joint Economic Committee, Rule 12, 16, and 23

RULE 12

Testimony received in executive hearings shall not be released or included in any report without the approval of a majority of the committee.

RULE 16

No summary of a committee report, prediction of the contents of a report, or statement of conclusions concerning any investigation shall be made by a member of the committee or of the committee staff prior to the issuance of a report of the committee.

RULE 23

The information contained in any books, papers, or documents furnished to the committee by any individual, partnership, corporation, or other legal entity shall, upon the request of the individual, partnership, corporation, or entity furnishing the same, be maintained in strict confidence by the members and staff of the committee, except that any such information may be released outside of executive session of the committee if the release therof is effected in a manner which will not reveal the identity of such individual, partnership, corporation, or entity: Provided, That the committee by majority vote may authorize the disclosure of the identity of any such individual, partnership , corporation, or entity in connection with any pending hearing or as a part of a duly authorized report of the committee if such release is deemed essential to the performance of the functions of the committee and is in the public interest.

Appendix B.

Selected House and Senate Rules Regarding

the Management of Sensitive Information

Rules of the House of Representatives, 95th Congress

Rule XI

Section 712. Investigative hearing procedures

(k)(7) No evidence or testimony taken in executive session may be released or used in public sessions without the consent of the committee.

Rule XXIX

Secret Session

Whenever confidential communications are received from the President of the United States, or whenever the Speaker or any Member shall inform the House that he has communications which he believes ought to be kept secret for the present, the House shall be cleared of all persons except the Members and officers thereof, and so continue during the reading of such communications, the debates and proceedings thereon, unless otherwise ordered by the House.

Rule XLIII

Code of Official Conduct

There is hereby established by and for the House of Representatives the following code of conduct, to be known as the "Code of Official Conduct":

2. A Member, officer, or employee of the House of Representatives shall adhere to the spirit and the letter of the Rules of the House of Representatives and to the rules of duly constituted committees thereof.

Senate Manual, 95th Congress

Rule XXXVI

Section 36.3. Executive Sessions

3. All confidential communications made by the President of the United States to the Senate shall be by the Senators and the officers of the Senate kept secret; and all treaties which may be laid before the Senate, and all remarks, votes, and proceedings thereon shall also be kept secret, until the Senate shall by their resolution, take off the injuction of secrecy, or unless the same shall be considered in open Executive session.

Section 36.4.

4. Any Senator or officer of the Senate who shall disclose the secret or confidential business or proceedings of the Senate shall be liable, if a Senator, to suffer expulsion from the body; and if an officer, to dismissal from the service of the Senate, and to punishment for contempt.

Section 36.5

5. Whenever, by the request of the Senate or any Committee thereof, any documents or papers shall be communicated to the Senate by the President or the head of any department relating to any matter pending in the Senate, the proceedings in regard to which are secret or confidential under the rules, said documents and papers shall be considered as confidential, and shall not be disclosed without leave of the Senate.

Section 76. Standing Orders of the Senate

Loyalty Checks on Senate Employees

Resolved, That hereafter when any person is appointed as an employee of any committee of the Senate, of any Senator, or of any office of the Senate the committee, Senator, or officer having authority to make such appointment shall transmit the name of such person to the Federal Bureau of Investigation, together with a request that such committee, Senator, or officer be informed as to any derogatory and rebutting information in the possession of such agency concerning the loyalty and reliability for security purposes of such person, and in any case in which such person, and in any case in which such derogatory information is revealed such committee, Senator, or officer shall make or cause to be made such further investigation as shall have been considered necessary to determine the loyalty and reliability for security purposes of such person.

Every such committee, Senator, and officer shall promptly transmit to the Federal Bureau of Investigation a list of the names of the incumbent employees of such committee, Senator, or officer together with a request that such committee, Senator, or officer be informed of any derogatory and rebutting information contained in the files of such agency concerning the loyalty and reliability for security purposes of such employee.

Appendix C.

Selected Provisions of Statutory Law

Regarding Classified Information

Title 18, U.S. Code

§793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to beieve, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, mode, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communi-

delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer --

shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (June 25, 1948, ch. 645, 62 Stat. 736; Sept. 23, 1950, ch. 1024, title I, §18, 64 Stat. 1003.)

§794. Gathering or delivering defense information to aid foreign government.

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of

a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more of such persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (June 25, 1948, ch. 645, 62 Stat. 737; Sept. 3, 1954, ch. 1261, title II, § 201, 68 Stat. 1219.)

§798. Disclosure of classified information.

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States for the benefit of any foreign government to the detriment of the United States any classified information --

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes --

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section --

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof. (Added Oct. 31, 1951, ch. 655, § 24 (a), 65 Stat. 719.)

§ 799. Violation of regulations of National Aeronautics and Space Administration.

Whoever willfully shall violate, attempt to violate, or conspire to violate any regulation or order promulgated by the Administrator of the National Aeronautics and Space Administration for the protection or security of any laboratory, station, base or other facility, or part thereof, or any aircraft, missile, spacecraft, or similar vehicle, or part thereof, or other property or equipment in the cus-

in the custody of the Administration, or any real or personal property or equipment in the custody of any contractor under any contract with the Administration or any subcontractor of any such contractor, shall be fined not more than $5,000, or imprisoned not more than one year, or both. (Added Pub. L. 85-568, title III, § 304 (c) (1), July 29, 1958, 72 Stat. 434.)

§ 952. Diplomatic codes and correspondence.

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both. (June 25, 1948, ch. 645, 62 Stat. 743.)

§ 957. Possession of property in aid of foreign government.

Whoever, in aid of any foreign government, knowingly and willfully possesses or controls any property or papers used or designed or intended for use in violating any penal statute, or any or the rights or obligations of the United States under any treaty or the law of nations, shall be fined not more than $1,000 or imprisoned not more than ten years, or both. (June 25, 1948, ch. 645, 62 Stat. 745.)

Title 42, U.S. Code

Subchapter XVI. -- Joint Committee on Atomic Energy

§ 2256. Classification of information.

The Joint Committee may classify information originating within the committee in accordance with standards used generally by the executive branch for classifying Restricted Data or defense information (Aug. 1, 1946, ch. 724, § 206, as addeded Aug. 30, 1954, ch. 1073, § 1, 64 Stat. 957).

Subchapter XVII. -- Enforcement of Chapter

§ 2271. General provisions.

(a) To protect against the unlawful dissemination of Restricted Data and to safeguard facilities, equipment, materials, and other property of the Commission, the President shall have authority to utilize the services of any Government agency to the extent he may deem necessary or desirable.

(b) The Federal Bureau of Investigation of the Department of Justice shall investigate all alleged or suspected criminal violations of this chapter.

(c) No action shall be brought against any individual or person for any violation under this chapter unless and until the Attorney General of the United States has advised the Commission with respect to such action and no such action shall be commenced except by the Attorney General of the United States: Provided, however, That no action shall be brought under section 2272, 2273, 2274, 2275, or 2276 of this title except by the express direction of the Attorney General: And provided further, That nothing in this subsection shall be construed as applying to administrative action taken by the Commission. (Aug. 1, 1946, ch. 724, § 221 as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 958, and amended Dec. 24, 1969, Pub. L. 91-161, § 5, 83 Stat. 445.)

§ 2272. Violation of specific sections.

Whoever willfully violates, attempts to violate, or conspires to violate, any provision of sections 2077, 2122, or 2131 of this title, or whoever unlawfully interferes, attempts to interfere, or conspires to interfere with any recapture or entry under section 2138 of this title, shall, upon conviction thereof, be punished by a fine of not more than $10,000 or by imprisonment for not more than ten years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation shall, upon conviction thereof, be punished by impris-

onment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both. (Aug. 1, 1946, ch. 724, § 222, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 958, and amended Dec. 24, 1969, Pub. L. 91-161, §§ 2, 3(a), 83 Stat. 444.)

§ 2273. Violation of sections generally.

Whoever willfully violates, attempts to violate, or conspires to violate, any provision of this chapter for which no criminal penalty is specifically provided or or any regulation or order prescribed or issued under section 2095 or 2201 (b), (i), or (o) of this title shall, upon conviction thereof, be punished by a fine or not more than $5,000 or by imprisonment for not more than two years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation, shall, upon conviction thereof, be punished by a fine of not more than $20,000 or by imprisonment for not more than twenty years, or both. (Aug. 1, 1946, ch. 724, § 223, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 958, and amended Dec. 14, 1967, Pub. L. 90-190, § 12, 81 Stat. 578; Dec. 24, 1969, Pub. L. 91-161, § 6, 83 Stat. 445.)

§2274. Communication of Restricted Data.

Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data --

(a) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction thereof, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000, or both;

(b) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both.

(Aug. 1, 1946, ch. 724, § 224, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 958, and amended Dec. 24, 1969, Pub. L. 91-161, § 3(b), 83 Stat. 444.)

§2275. Receipt of Restricted Data.

Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, acquires, or attempt or conspires to acquire any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data, shall upon conviction thereof, be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both. (Aug. 1, 1946, ch. 724, § 225, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 959, and amended Dec. 24, 1969, Pub. L. 91-161, § 3(b), 83 Stat. 444.)

§ 2276. Tampering with Restricted Data.

Whoever, with intent to injure the United States or with intent to secure an advantafe to any foreign nation, removes, conceals, tampers with, alters, mutilates, or destroys any document, writing, sketch, photograph, plan, model, instrument, appliance, or note involving or incorporating Restricted Data and used by any individual or person in connection with the production of special nuclear material, or research or development relating to atomic energy, conducted by the United States, or financed in whole or in part by Federal funds, or conducted with the aid of special nuclear material, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both. (Aug. 1, 1946, ch. 724, § 226, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 959, and amended Dec. 24, 1969, Pub. L. 91-161, § 3(b), 83 Stat. 444.)

§ 2277. Disclosure of Restricted Data.

Whoever, being or having been an employee or member of the Commission, a member of the Armed Forces, an employee of any agency of the United States, or being or having be a contractor of the Commission or of an agency of the United States, or being or having been an employee of a contractor of the Commission or of an agency of the United States, or being or having been a licensee of the Commission, or being or having been an employee of a licencee of the Commission, knowingly communicates, or whoever conspires to communicate or to receive, any Restricted Data, knowing or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data pursuant to the provisions of this chapter or under rule or regulation of the Commission issued pursuant thereto, knowing or having reason to believe such person is not so authorized to receive Restricted Data shall, upon conviction thereof, be punishable by a fine of not more than $2,500. (Aug. 1, 1946, ch. 724, § 227, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 959.)

§ 2278. Statute of limitations.

Except for a capital offense, no individual or person shall be prosecuted, tried, or punished for any offense prescribed or defined in sections 2274 to 2276 of this title unless the indictment is found or the information is instituted within ten years next after such offense shall have been committed. (Aug. 1, 1946, ch. 724, § 228, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 959.)

Title 50, U.S. Code

§ 783. Offenses.

(b) Communication of classified information by Government officer or employee.

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in the whole or in major part by the United States or any department or agency thereof, to communicate in any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer of employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer of employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

(c) Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information.

It shall be unlawful for any agent or representative of any foreign government, or any officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, knowingly to title, knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major party by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of

any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

(d) Penalties for violation.

Any person who violates any provision of this section shall, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than 10 years, or by both such fine and such imprisonment, and shall, moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

(e) Limitation period.

Any person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after the commission of such offense, notwithstanding the provisions of any other statute of limitations: Provided, That if at the time of the commission of the offense such person is an officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, such person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after such person has ceased to be employed as such officer or employee.

§ 797. Security regulations and orders; penalty for violation.

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident

Next 1 Page(s) In Document Exempt

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300120010-3