

United States Senate

SECURITY MANUAL



Office of Senate Security

NOVEMBER 2020

Ex. F

FOREWORD

In order to fulfill its obligations under the Constitution, the Senate receives, produces and maintains classified information vital to the national defense and foreign relations of the United States. From oversight of intelligence operations to the development of foreign trade policy to the security of America's elections, the daily business of the Senate requires access to information which certain countries and organizations seek to obtain and to use against the interests of the United States. As officers and employees of the Senate, each of us is obligated to safeguard national security information in our possession.

The Office of Senate Security was established to ensure that classified information in the possession of the Senate receives full protection against unauthorized disclosure. This Manual sets forth regulations governing the handling of national security information within the Senate. It is the responsibility of all employees of the Senate to be familiar with and to abide by these regulations.

JULIE E. ADAMS
SECRETARY OF THE SENATE

TABLE OF CONTENTS

SECTION I. GENERAL	PAGE
1. Scope	1
2. Office of Senate Security	1
3. Office Security Managers	1
4. Exemptions	2
 SECTION II. HANDLING OF CLASSIFIED INFORMATION	
A. General	2
1. Policy	2
2. Classification	2
3. Receipt of Classified Material	2
4. Record of Classified Material	3
5. Marking Classified Material	4
6. Production of Classified Material	5
7. Storage and Certification	6
8. Safeguards During Use	7
9. Transmission	8
10. Reproduction	8
11. Destruction	9
12. Removal	9
B. Communications Security	9
1. Telephones	9
2. Discussions/Briefings	9
C. Electronic Processing of Classified Information	10
 SECTION III. PERSONNEL SECURITY	
1. Access	10
2. Staff Security Clearances	10
3. Processing of Security Clearance Requests	12
4. Clearance Standards for Senate Staff	12
5. Levels of Clearance	13
6. Consultants and Contract Personnel	13
7. Terminations of Clearances	13
8. Reinvestigation Program	14
9. Non-Disclosure Agreements	14
10. Security Violations	14

11. Security Education and Awareness15

12. Termination of Security Clearances,
Employment, or Extended Leave17

13. Foreign Travel17

14. Contact Reports17

SECTION IV. CYBERSECURITY19

GLOSSARY21

APPENDIX : SENATE RESOLUTION 24325

SENATE SECURITY MANUAL

The United States Senate is obligated to safeguard the classified information it obtains and produces, and to ensure that Senate personnel entrusted with the Nation's secrets are properly vetted and aware of their solemn responsibilities. To ensure that the Senate lives up to its obligations, this Manual is published to establish uniform security practices within the Senate. The provisions of this Manual are binding upon all employees of the Senate.

SECTION I. GENERAL

1. Scope. This Manual establishes requirements for safeguarding classified information in the possession of the Senate, its offices and its employees. It is the responsibility of every employee of the Senate to be familiar with security requirements and to comply with them. Ultimate responsibility for ensuring that Senate employees comply with the provisions of this Manual lies with the employing Senator. Any questions regarding the proper safeguarding of classified information, or any problems relating to security matters in general, should be directed to the office Security Manager or to the Office of Senate Security for guidance and direction.

2. Office of Senate Security. In order to protect classified information in the possession of the Senate from unauthorized disclosure, an Office of Senate Security (OSS) has been established. The Office is charged with setting forth regulations to govern the handling of classified information by all Senate offices, and with ensuring the implementation and enforcement of such regulations. Those regulations are detailed in this Manual.

3. Office Security Managers. To achieve and maintain a strong security posture, each Senate office which receives, produces or stores classified information, or which employs staff holding a security clearance, shall designate a cleared individual as Security Manager. After initial training and certification by, and under the administrative guidance of the Director of Senate Security, each office Security Manager will be responsible for the following duties:

- a) Implementing the provisions of this Manual within the office, and ensuring that all employees of the office are familiar with those provisions;
- b) Providing security advice and guidance to office personnel; and

c) Serving as the office's liaison to the Office of Senate Security and other Senate offices for security matters.

4. Exemptions. Those Senate offices which have custodial control over large amounts of classified material may be exempted from certain provisions of this Manual after the Director of Senate Security has certified that their policies and procedures for handling classified information fully meet the standards of this Manual.

SECTION II. HANDLING OF CLASSIFIED INFORMATION

A. General

1. Policy. Classified information originated by the Executive Branch and in the possession of the Senate will be handled and safeguarded in accordance with the provisions of this Manual. Any material generated internally, including memoranda and working papers, which contains classified information shall be handled and safeguarded in the same manner.

2. Classification. The assignment of classification involves a determination that certain information requires protection in the interest of national security. There are three categories of classified information – Top Secret, Secret, and Confidential – which require varying degrees of protection (see Executive Order 13526). Access to classified material may be further restricted by special designations and access requirements. Material derived from originally classified information is classified at the same level as the original information.

Definitions of classification designations and supplemental access requirements may be found in the glossary of this manual.

In the event that the classification of any information is questioned or challenged, such information shall be treated as classified until the matter is resolved. In the event of such a question or challenge, the originator of the information shall be contacted first, and asked to provide a written report of the classification status of the information in question. If the question or challenge is not resolved in this manner, the matter shall be referred to the Office of Senate Security, which will pursue the issue with the appropriate agency(ies).

3. Receipt of Classified Material. All classified material intended for

delivery to Senate offices or employees from any source outside the Senate (whether governmental or commercial/industrial) shall be delivered to the Office of Senate Security (SVC-217). Upon receipt, the Office of Senate Security will contact the Security Manager of the office to which the material is addressed and arrange for its delivery or review in SVC-217, as appropriate.

Under no circumstances are Senate offices or committees to take receipt of classified material directly from outside sources, without the prior approval of OSS. Any courier attempting to deliver classified material must be directed to room SVC-217 in the Capitol Visitor Center.

Under no circumstances is classified material to be received by or given to individuals without the proper security clearance. Uncleared personnel must refuse to accept delivery of classified information. Conversely, the identity and security clearance of intended recipients of classified material must be verified before delivery is made. The Office of Senate Security maintains a listing of active security clearances held by Senate personnel and Executive Branch couriers to facilitate such verification.

4. Record of Classified Material.

(a) Accountability Records. The Security Manager of each Senate office that has been authorized to store classified material shall maintain a log of all classified material in the possession of the office. The log shall include all classified material received or produced by, or in the custody of, the office, and shall reflect at a minimum:

- (1) The Office of Senate Security document control number.
- (2) The copy number plus total copy count.
- (3) The office document control number, if different from the OSS Control Number.
- (4) The date of receipt.
- (5) The classification of the material.
- (6) The originating office or agency.
- (7) The number of pages.
- (8) The date of the document.
- (9) The addressee.
- (10) A brief, unclassified description of the material.
- (11) The file where the document is located.

(12) The disposition of the material and the date thereof.

(b) Inventory of Classified Material. The Office of Senate Security shall conduct an annual inventory of classified material in the possession of Senate offices and committees. The Security Manager in each office or committee shall confirm that the hard copy of each item listed in the log of their classified holdings is in their possession. The inventory will be checked against the records of the Office of Senate Security to ensure that all classified material is properly accounted for.

(c) Special Requirements for Secret and Top Secret. The office Security Manager shall maintain contemporaneous records of all persons who are afforded access to Secret and Top Secret information. The records shall list each item of Secret and Top Secret material and show the names of all individuals given access to the item and the date (or inclusive dates) on which access by each individual occurred. Such records shall be forwarded annually to the Office of Senate Security, where they will be retained for a period of three years from the date the material was destroyed, dispatched outside the Senate, declassified, or downgraded to less than Secret.

(d) Annual Review. For the purpose of reducing to a minimum the quantity of classified material on hand at any given time, each Senate office shall, during the annual inventory, review all classified information in its possession or being stored for it by the Office of Senate Security. All Senate offices wishing to dispose of classified information or place it in long term storage may forward it to the Office of Senate Security (using proper receipting procedures) which will assume responsibility for its proper storage or destruction.

(e) Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately (i.e., within 24 hours) report the circumstances to the Office of Senate Security so that a damage assessment may be conducted.

(f) Daily Security Checks. Office Security Managers shall conduct comprehensive security checks at the close of each work day to ensure that all classified material under their control is positively and completely secure. The Office of Senate Security can provide advice on developing and implementing effective security check lists.

5. Marking Classified Material. The originator of material which

contains classified information is responsible for properly marking the security classification of the material. Classification designation by conspicuous marking alerts the holder to the fact that the material contains classified information and to the degree of protection required for that information or material. Therefore, it is essential that all classified material be marked in such a manner as to be clear to the holder what level of classification is assigned to the material.

Whenever possible, documents containing information of varying levels of classification, or containing both classified and unclassified information, should have paragraphs within a document individually marked. The designations “U” (Unclassified), “C” (Confidential), “S” (Secret), “TS” (Top Secret) are placed in parentheses at the beginning or end of each paragraph for this purpose.

(a) Identification Markings. All classified material shall be marked to show the office responsible for its preparation, and the date of preparation. These markings are required on the front cover, title page or first page, as appropriate, of all classified documents.

(b) Overall Markings. The overall classification of a document, or any copy or reproduction thereof, shall be stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), and on the outside of the back cover (if any). If no covers or title pages exist, the overall classification shall be stamped at the top and bottom of the first page and on the back of the last page.

(c) Page Markings. Interior pages of classified documents shall be stamped at the top and bottom with the highest classification of the information appearing thereon, or with the overall classification of the document.

(d) Additional Markings. In addition to the markings specified above, classified material shall be marked, if applicable, with one or more notations which indicate the material is further restricted to special access categories (e.g. Restricted Data notation and Dissemination and Reproduction notices).

6. Production of Classified Material. When an office produces classified material, such material shall be entered into the office log *within one working day*. Such material shall be brought to the Office of Senate Security within one working day for entry into the OSS document control

system. Such material shall be properly marked with the appropriate security classification, as outlined above, and safeguarded in accordance with the provisions of this Manual.

7. Storage and Certification. Senate offices shall not store classified material until they have been certified by the Office of Senate Security as having adequate control procedures and storage capability. Classified material must never be left unattended. It must be secured in an approved storage container or under direct surveillance of an authorized person at all times. The Office of Senate Security will provide storage facilities for any office which does not meet these requirements. Classified material, when not in actual use, shall be stored as follows:

(a) Top Secret and Special Access Material Storage. Top Secret and Special Access material shall be stored in a General Services Administration (GSA) approved container bearing a GSA Test Certification label or in a class-A vault constructed in accordance with the requirements of the Department of Defense Industrial Security Manual.

- Entry to the room in which the container or vault is located shall be controlled by a properly cleared employee in order to restrict admittance to the room during normal working hours.
- The container or vault, as well as the door(s) to the room in which the container or vault is located, shall be locked at the close of business each day.
- The room in which the container or vault is located shall be protected by an intrusion detection system approved by the Office of Senate Security.

Storage of Top Secret or Special Access material in Senators' personal offices is not permitted.

(b) Secret and Confidential Material Storage. Secret and Confidential material may be stored in a GSA-approved container or vault. The container, as well as the door(s) to the room in which the container is located, shall be locked at the close of business each day.

(c) Supervision of Storage Containers. Only a minimum number of authorized persons shall possess the combinations to the storage containers or vaults, or have access to the information stored therein. To

facilitate investigation of a container found open and unattended during non-office hours, a record shall be maintained by the Office of Senate Security of the names, home phone numbers, and addresses of persons having knowledge of the combination. In addition, the combinations of storage containers in Senators' offices shall be maintained, in a sealed envelope, by the Office of Senate Security. Such envelope may be opened only at the direction of the Member or the office Security Manager.

Combinations to security containers shall be changed by OSS personnel having appropriate security clearance whenever:

- the container is placed in use;
- a person knowing the combination is transferred from the office to which the container is assigned;
- a combination has been subjected to possible compromise; or
- at least annually.

A record of the dates of such changes shall be maintained with the container, and shall include the name of the individual making the change.

Current combinations shall be classified no lower than the highest category of classified information authorized for storage in the container concerned. Each security container shall display a conspicuous sign indicating that it is open whenever it is not secured, and shall display a log sheet indicating the time and date of each opening and closing of the container. Cabinets and vaults in which classified information is stored shall be kept locked when not under the direct supervision of an authorized person entrusted with the combination or the contents.

(d) Alternate Storage Location. The Office of Senate Security will provide classified material storage in its facilities for any Senate office or committee that requests it. In the event a cabinet or vault becomes damaged or inoperable in a Senate office or committee, the Office of Senate Security will temporarily provide secure storage until the cabinet or vault is restored to good repair.

8. Safeguards During Use. Classified information is provided to a properly cleared person on the basis of a "need-to-know." Determination of a need-to-know is an individual responsibility. Before divulging any classified information, Senate employees shall make certain of the

recipient's identity, level of clearance, and need-to-know. In order to facilitate such determination, the Office of Senate Security will maintain a list of Senate employees whose level of clearance has been properly established.

Classified material, when not safeguarded as provided for in Section 7, and when in actual use by cleared personnel, shall be protected as follows:

(a) Kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security controls over the material.

(b) Covered, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present.

(c) Returned to storage containers as soon as practical after use.

9. Transmission. Classified information and material shall be enclosed in opaque inner and outer covers before transmittal. The inner cover shall be sealed and plainly marked with the classification level, as well as the address. The outer cover shall be sealed and addressed with no indication of the classification or contents. A receipt shall be attached to or enclosed in the inner cover. The receipt shall identify the sender, addressee, the document and its level of classification, but shall contain no classified information. The receipt shall be signed by the recipient and returned to the sender.

Transmission of classified material between Senate offices shall be accomplished only by employees of the Office of Senate Security. Transmission of classified material outside the Senate shall be accomplished only by OSS personnel or by authorized Executive Branch couriers. Transmission of classified material from any Senate office directly to the Office of Senate Security shall be accomplished by appropriately cleared personnel, with the approval of the office Security Manager.

10. Reproduction. Sensitive Compartmented Information and other Special Access information shall not be reproduced. Documents or portions of documents containing Top Secret information shall not be reproduced without the consent of the originating office. Reproductions of classified material shall be kept to an absolute minimum and shall be marked or stamped with the same classification as the original. Reproduction of

classified material shall be made only on equipment specifically designated by the Office of Senate Security for the reproduction of classified material. Immediately after reproduction of classified material, three (3) blank sheets of paper shall be run through the photocopier used for the reproduction. The Senate office which reproduces classified material is responsible for logging and immediately bringing all copies under proper accountability controls, to include notifying the Office of Senate Security, as provided for in Section 4 above, "Record of Classified Material."

11. Destruction. All classified material shall be returned to the Office of Senate Security as soon as it is no longer needed. All such material will be destroyed, returned to its originator, or archived by the Office of Senate Security. Records of destruction or other disposition will be maintained by the Office of Senate Security. Any document bearing an OSS bar code or document control number must be returned to the Office of Senate Security for destruction.

12. Removal. Under no circumstances shall classified material be removed from approved storage or working areas without the prior written approval of the Office of Senate Security. Personal residences are not approved storage or working areas for classified material. *Violation of this provision may result in termination of security clearances, termination of employment, or criminal prosecution.*

B. Communications Security

1. Telephones. Classified information shall not be discussed over open telephone lines under any circumstances. Foreign intelligence services and other groups or individuals may monitor telephone calls to and from Senate offices. One should not attempt to "talk around" classified information over unsecured telephone lines. There are a number of secure telephones in the Senate, which are approved for discussion of classified information. Should any Senate employee require the use of a secure telephone, the Office of Senate Security can provide assistance.

2. Discussions/Briefings. Discussion or presentation of classified material must take place in the Office of Senate Security, or in another secure area designated by the Office of Senate Security. Classified information may not be discussed in a personal office if a more secure area is available; information classified higher than SECRET may not be discussed in personal offices under any circumstances. Call the Office of

Senate Security at 4-5632 prior to any discussion of classified information outside the Office of Senate Security.

C. Electronic Processing of Classified Information

Classified information may be processed only on Senate computer systems approved by the Office of Senate Security. Privately owned computers must not be used to process classified information. Any equipment which is to be used for the processing of classified information must have an approved security plan in place before any information is processed. Contact the Office of Senate Security for assistance in preparing the security plan.

Do not use any unclassified official government system or device to access, download or attempt to download from a public website any information that is believed to be classified. Doing so would introduce potentially classified information to unclassified networks.

If a document with classification markings as described in paragraph A(5) of this manual is received by electronic mail on any unclassified official government system or device, do not delete, save or forward the electronic mail message. Immediately contact the Office of Senate Security for handling instructions.

Any questions or doubt as to proper procedures for processing or printing classified information should be resolved by contacting the Office of Senate Security before acting.

SECTION III. PERSONNEL SECURITY

1. Access. No person shall be given access to classified information or material unless a favorable determination has been made as to his or her trustworthiness. The determination of eligibility, known as a security clearance, authorizes an individual access to a specific level of classified information. In addition to a security clearance, a person must have a need for access to the particular classified information or material sought in connection with the performance of his or her official duties. The determination of a “need-to-know” shall be made by the person in possession of the information sought.

2. Staff Security Clearances. Requests for staff security clearances must originate with Senators themselves, in the case of personal staff, or in the

case of Senate committee staff, with committee chairmen. Requests for clearances for employees of the Secretary of the Senate and the Sergeant at Arms must originate with the Officers themselves. ***Requests for staff security clearances are to be kept to the absolute minimum required for the conduct of official Senate business.***

(a) Restrictions. The primary mechanism for the protection of classified national security information is a strict limitation on access to such information. The larger the number of people with access to classified information, the greater the risk that such information will be compromised-either intentionally or inadvertently. Therefore, the Senate, in agreeing to Senate Resolution 243, committed itself to reducing the number of staff holding security clearances, and to keeping that number at a minimum thereafter. In order to meet that commitment, the following restrictions on the granting of staff security clearances have been instituted:

(1) Each Senator shall be limited to no more than two cleared employees on his or her personal staff.

(2) Each Senator shall be allowed no more than one Executive Branch Fellow or Detailee who holds a security clearance with his/her employer.

(3) Each Senator shall be allowed one System Administrator cleared to the SECRET level.

(4) Any Senator serving on the Armed Services or Foreign Relations Committees, the Committee on Appropriations Subcommittee on Defense, the Committee on Appropriations Subcommittee on State, Foreign Operations, and Related Programs, or the Committee on Homeland Security and Governmental Affairs, shall be permitted one additional cleared employee to assist such Senator in the performance of his or her official duties in connection with such Committee assignment.

In exceptional circumstances, a Senator may request from the Majority or Minority Leader, depending upon the Senator's party affiliation, a waiver of this staff clearance limitation for a fixed period and a specific purpose.

(b) Eligibility. Senators and committee chairmen must determine which ***positions*** on their staffs require a security clearance. Clearances

will only be granted to employees whose assignments require access to classified information. The Office of Senate Security can provide assistance in determining which staff positions require a clearance.

(1) In order to be eligible for a security clearance, staff must be on the payroll of the Senator or committee requesting or sponsoring the clearance.

(2) Should an individual holding a security clearance be re-assigned, his or her clearance will automatically be deactivated, and will remain inactive until and unless it is determined that the individual's new assignment requires access to classified information.

(3) No member of a retiring Senator's personal staff shall be processed for a security clearance during the last year of such Senator's term of office. In exceptional circumstances, a Senator may request from the Majority or Minority Leader, depending upon the Senator's party affiliation, a waiver of this prohibition for a specific purpose.

3. Processing of Security Clearance Requests. When a Senator, committee chairman or Senate Officer determines that a member of his or her staff requires access to classified information, he or she will relay the request, in writing, to the Director of Senate Security. The Office of Senate Security will provide the staff member with a security clearance application. When the application is completed, it must be returned to the Office of Senate Security. The application then will be referred to the appropriate agency for processing. When a clearance is granted, the employing Senator, Chairman or Officer will be informed, and the Office of Senate Security will schedule an Initial Security Briefing for the staff member concerned. Senate employees must receive an Initial Security Briefing before being granted access to classified information.

Relevant Executive Branch agencies have been informed that they are not to entertain requests for personnel clearances directly from Senate offices. In addition, Senate personnel will not be granted access to classified information unless their clearance(s) are registered with the Office of Senate Security. These restrictions are necessary to ensure that the Senate's registry of personnel clearances remains accurate.

4. Clearance Standards for Senate Staff. The criteria for security clearances require that applicants be individuals:

(a) of excellent character, discretion, trustworthiness, and loyalty to the United States; and

(b) who are citizens of the United States. A Senator may request a waiver of this requirement, in order to request up to a Secret level clearance for a permanent resident alien, if such Senator believes that the individual is uniquely qualified to perform a mission in support of official Senate business. Requests for waiver of this requirement must be made in writing to the Director of Senate Security, who shall make a recommendation to the Majority and Minority Leaders.

To ensure that these criteria are met, Federal agents will conduct an investigation into each applicant's personal, social, professional, educational, and financial background. The extent of such investigations depends upon the level of clearance for which application is made.

5. Levels of Clearance. There are three "levels" of security clearance, which correspond with the three levels of classification: Confidential, Secret and Top Secret. In addition, certain categories of classified information require special clearances and access approval. These special clearances and approvals are granted on a rigidly controlled need-to-know basis, and are not granted to personal staff.

6. Consultants and Contract Personnel. Consultants, "Fellows," contract personnel and other non-Senate employees whose assigned duties require access to classified information will be subject to the same security requirements as Senate staff. Such individuals shall not be granted access to classified information until written verification of the individual's security clearance is obtained by the Office of Senate Security from the employing agency. Access by such individuals to classified information will be limited to that needed in the performance of duty, as specified in the contract or other job description. Any proposed change in the utilization of such individuals requires submission of a request that a new security approval be granted.

7. Terminations of Clearances. The Director of Senate Security will terminate the clearance(s) of an individual if:

- (a) the sponsoring Senator requests such termination;
- (b) the employee terminates employment with the Senate;

(c) the employee is reassigned to a position which does not require access to classified information; or

(d) the Majority and/or Minority Leader so directs.

8. Reinvestigation Program.

(a) Reinvestigation. Reinvestigations of Senate employees holding a security clearance will be conducted at least every five years. The Office of Senate Security will notify Senators and committee chairmen within 120 days when one of their employees is due for reinvestigation.

(b) Requested Reinvestigation. The Director of Senate Security also will initiate reinvestigation of a Senate employee at the request of the sponsoring Senator.

9. Non-Disclosure Agreements. A non-disclosure agreement must be executed by all Senate employees who are granted security clearances. The agreement will contain provisions that prohibit the signer from divulging or releasing classified information to unauthorized individuals.

10. Security Violations.

(a) Investigations. All known, suspected or alleged security violations shall be reported to and investigated by the Office of Senate Security. The formal investigation report will include:

- (1) The predicate for the investigation.
- (2) A finding on whether a probable compromise of classified information occurred.
- (3) A written report of those interviewed.
- (4) A finding as to the person(s) responsible.
- (5) A statement as to the degree of compromise involved.
- (6) The security violation history of each person found responsible.
- (7) Recommendations for remedial action to preclude recurrence of such violation(s).

The Security Manager of the office concerned will be kept fully and timely informed of the investigation by the Office of Senate Security, and

shall receive a copy of the formal investigation report.

(b) Penalties. Any violation of the provisions of this Manual determined by the investigation to be unintentional may result in one or more of the following administrative actions, depending upon the severity of the violation:

(1) Recommendation(s) to the Security Manager of the office involved regarding changes in office security procedures.

(2) Recommendation to the sponsoring Member that a written notice or reprimand and warning of consequences of further violations be issued.

(3) Recommendation to the sponsoring Member that the individual responsible be denied further access to classified information until such individual attends a refresher briefing on security regulations conducted by the Office of Senate Security.

(4) Recommendation to the sponsoring Member, or to the Majority and Minority Leaders that the clearance(s) of the individual(s) responsible be terminated.

(5) Referral of the matter to the Select Committee on Ethics, for disposition according to the Standing Rules and Standing Orders of the Senate and the rules of the Select Committee on Ethics. Any such referral may be accompanied by recommendations including, but not limited to, suspension without pay for a specified period of time, termination of security clearance or termination of Senate employment.

Any incident determined by the investigation to involve willful compromise of national defense information shall be referred to the Select Committee on Ethics and/or to the Department of Justice. (18 USC 792 *et seq.*)

Under no circumstances will penalties for security violations be recommended or imposed on any Senate employee unless and until the investigation procedures set forth in paragraph 10(a), above, are carried out and a determination made as to individual responsibility.

11. Security Education and Awareness. The Office of Senate Security has overall responsibility for the administration of a security education and

awareness program for Senate employees. Participation in the program is mandatory for staff holding security clearances. The Security Awareness Program consists of the following:

(a) Initial Security Briefings. All Senate employees granted a security clearance will, before being allowed access to classified information, be given an Initial Security Briefing by staff of the Office of Senate Security. The briefing will cover the provisions of this Manual, the espionage laws of the United States, techniques employed by hostile intelligence services attempting to gain access to classified information, the individual's security responsibilities, and other pertinent security instructions.

After receiving the Initial Security Briefing, each employee shall sign a statement affirming that he or she has read and understands the Senate Security Manual and agrees to comply with the provisions thereof. All cleared Senate employees shall return the signed statement to the Office of Senate Security within three days of receipt.

(b) Refresher Briefings. Refresher briefings shall be required when a staff member is granted access to classified information of significantly greater sensitivity than his or her previous access permitted, or when security violations are serious or continuing, or at least annually.

(c) Topical Briefings. Briefings on various security related issues will be scheduled on a periodic basis. All employees holding the necessary level of clearance will be informed in advance, and are expected to attend. Subjects to be covered in Topical Briefings include counterintelligence, communications security, foreign intelligence activities on Capitol Hill, influence operations, computer security, and technical surveillance countermeasures.

(d) Foreign Travel Briefings. Senate employees are strongly encouraged to contact the Office of Senate Security before traveling to any foreign country. The Office of Senate Security will provide safety and security information regarding any country whether the intended travel is official or personal. A foreign travel briefing is not required in every instance; however, when conditions warrant, such briefings may be required prior to travel.

(e) Termination Briefings. Staff shall be given a security termination briefing, and shall sign a termination statement upon termination of

employment, withdrawal of clearance, beginning of extended leave (sixty days or more), or reassignment to a position not requiring access to classified information. The briefing will emphasize the individual's continuing responsibility to safeguard classified information against unauthorized disclosure. It shall be the responsibility of the employing Senator to ensure that staff attend Termination Briefings.

(f) Special Briefings. Upon request of a Senator or committee or subcommittee chairman, the Office of Senate Security will prepare and present briefings on security matters of particular concern.

12. Termination of Security Clearances, Employment, or Extended Leave. Those Senate employees whose security clearances have been withdrawn, whose employment has been terminated, who are reassigned to a position not requiring access to classified material, or who are taking extended leave for a period of 60 days or more, shall surrender before departure all classified documents or materials in their possession, and will receive a Security Termination Briefing.

13. Foreign Travel. During foreign travel, Senate personnel may be more vulnerable to common street crime, social unrest, and acts of terrorism. To minimize the threat to the individual, the Office of Senate Security will arrange defensive briefings for persons planning private or official travel to any foreign country. Since any traveler might become involved in an act of terrorism, hijacking, or piracy, guidance on what to expect and how to behave in such situations will be made available to Senators and Senate employees contemplating travel.

14. Contact Reports. The ability of U.S. counterintelligence agencies to identify foreign intelligence officers, their agents and objectives is vital to the protection of national security information. As the United States Senate is known to be a target of certain foreign intelligence services, the following policy governing contacts with foreign nationals has been established by the Senate.

(a) All Senate personnel, whether or not they hold a security clearance, shall immediately report to the Office of Senate Security any contact with **any** individual regardless of nationality, either within or outside the scope of the employee's official activities, in which:

(1) Illegal or unauthorized access is sought to classified information; or

(2) The employee is concerned that he or she may be the target of an attempted exploitation by a foreign entity.

(b) In addition to the requirements of Section 14(a), all Senate personnel having access to classified information shall immediately report to the Office of Senate Security:

(1) Any contact, intentional or otherwise, with an official or representative of a governmental or commercial entity of a *designated* country unless such contact occurs as a function of one's official Senate duties;

(2) Any actual or suspected attempt by an official or representative of a *designated* country to establish social relationships or cultivate friendships;

(3) Any offer, by an official or representative of any country, of money payments or other bribery to obtain information, whether classified or not; or

(4) Any attempt by officials or representatives of any country to:

(i) obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact;

(ii) coerce by blackmail or threat; or

(iii) place one under obligation.

NOTE: The conduct of official Senate business sometimes involves the interaction of Senate employees with representatives of foreign governments, including some that may be considered adversaries of the United States. The guidance in this Manual is not intended to curtail or to discourage such contact. Senate personnel should not be intimidated by this policy, as it is designed only to safeguard classified information, and to protect Senators and their employees from exploitation or embarrassment.

(c) FBI Investigative Guidelines. The guidelines governing the Federal Bureau of Investigation (FBI) counterintelligence program state that activities of the following types will be investigated by the FBI when conducted by *any* foreign power, regardless of the country involved in those activities. Any Senate employee having knowledge or suspicion of such activities shall immediately report it to the Office of Senate Security.

(1) Critical Technology: Foreign intelligence activities directed at U.S. critical or emerging technologies (see list published by the National Security Council staff, National Strategy for Critical and Emerging Technologies, October 2020).

(2) Proprietary Economic Information: Foreign intelligence activities directed at the collection of U.S. industrial proprietary economic information and technology, the loss of which would undermine the U.S. national industrial base.

(3) Clandestine Activity: Clandestine foreign intelligence activity in the United States.

(4) Defense Information: Foreign intelligence activities directed at collection of information relating to defense establishments and related activities of national preparedness.

(5) Proliferation: Foreign intelligence activities involved in the proliferation of special weapons of mass destruction, to include chemical, biological, and nuclear weapons, and delivery systems for such weapons.

(6) Targeting Government Information and Personnel: Foreign intelligence activities involving the targeting of U.S. intelligence or foreign affairs information and U.S. Government officials, including Senate employees.

(7) Active Measures: Foreign intelligence activities involving perception management or influence operations.

(d) Designated Countries. The term “designated countries” as used in this Manual refers to certain nations whose intelligence services are known to conduct intelligence operations against U.S. interests. Information regarding designated countries can be obtained from the Office of Senate Security.

SECTION IV. CYBERSECURITY

U.S. Government computer systems and the information they carry are frequent targets of malicious hackers, criminals, and numerous foreign governments. Maintaining the confidentiality, integrity, and availability of data on office and committee computer systems is the responsibility

of each individual Senate committee and office. The Senate Sergeant at Arms provides guidance and recommendations to Senate offices on best practices for enhancing official and personal cybersecurity. This includes, but is not limited to:

- best practices for secure teleworking
- travel recommendations
- creating and managing strong passwords
- official and personal email security
- securing devices, workstations, and servers; securing social media accounts
- recognizing phishing, spear phishing, and adware

If a user believes they have received a malicious email message, they may email malware@saa.senate.gov for assistance. For all other matters of cybersecurity concern, please contact the Senate Sergeant at Arms Cyber Security Operations Center (CSOC) at csoc@saa.senate.gov or 202-224-2927 option 1.

GLOSSARY

ACCESS—The ability and opportunity to obtain knowledge of classified information. An individual may be able to obtain classified information by being in a place where such information is kept, provided the security measures in effect do not prevent him or her from doing so.

ACTIVE MEASURES—Deceptive activities, the goal of which is to influence the opinions or actions of individuals, governments, or publics. Active measures include: disinformation and forgeries; front groups; and agent-of-influence operations.

AUTHORIZED PERSON—An individual who has established: (1) a need for access to, knowledge of, or possession of classified information; and (2) holds proper clearance to receive classified information. It is the responsibility of the person having control of the classified information to determine that the requester of the information has: (1) a need-to-know the material; and (2) clearance to receive it. (See also “Need-to-Know.”)

CLASSIFICATION—The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

CLASSIFIED INFORMATION—Official information, including foreign classified information, which has been determined, pursuant to statute or executive order, to require protection in the interests of national security.

CLASSIFY—To assign information to one of the three classified categories (Confidential, Secret, or Top Secret) after determination that the information requires protection in the interests of national security.

COMPROMISE—The known or suspected exposure of classified information to an unauthorized person.

CONFIDENTIAL (C)—The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

COUNTERINTELLIGENCE—Information gathered and activities conducted to protect against espionage or other intelligence activities conducted by or on behalf of foreign governments, organizations, or

persons, or international terrorist groups.

COURIER—Any cleared individual who has been authorized in writing to hand carry classified material. Couriers are of two types: (1) those who carry material in connection with a specific trip and task to be accomplished; and (2) those who carry material as a regular part of their work assignment.

CYBERSECURITY—The art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information.

DERIVATIVE CLASSIFICATION—Classification based on or derived from previous, officially classified material or prescribed in a security classification guide.

DOCUMENT—Any record information regardless of its physical form or characteristics, including, without limitation, written or printed material, data processing disks, cards, CDs, DVD, and tapes; maps; charts; paintings; drawings; photographs, engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

FORMERLY RESTRICTED DATA—Data that have been removed from the Restricted Data category upon determination, jointly by the Department of Defense and the Department of Energy, that such data related primarily to the military use of atomic weapons and that can be adequately safeguarded as classified defense information.

INDUSTRIAL SECURITY—That portion of national security concerned with the protection of classified information in the possession of industrial contractors to the Department of Defense or other user agencies.

MATERIAL—Any document, product, or substance on or in which information may be recorded or embodied.

NEED-TO-KNOW — A determination that a prospective recipient of classified information, in the interests of national security, has clearance and a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract approved by a user agency.

OFFICIAL INFORMATION—Information that is owned by, produced by, or is subject to the control of the United States Government.

ORIGINAL CLASSIFICATION—An initial determination that information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure. Such classification is not based on or derived from any previously classified material.

PUBLIC DISCLOSURE—The passing of information and/or material to any member of the public in any manner.

REPRODUCTION—Copying, duplicating, photographing, or otherwise making a facsimile, replica, or counterpart of an original article, regardless of the means used to copy or reproduce.

RESTRICTED DATA—All data (information) covering: (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but not to include data declassified or removed from Restricted Data category pursuant to the provisions of the Atomic Energy Act of 1954.

SECRET (S)—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

SENSITIVE COMPARTMENTED INFORMATION (SCI)—All information and materials requiring special controls indicating restricted handling within present and future intelligence collection programs and their end products. These special controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.

SPECIAL ACCESS PROGRAM (SAP)—Any program imposing need-to-know or access controls beyond those normally prescribed for access to Confidential, Secret, or Top Secret information.

SYSTEM ADMINISTRATOR (SYSADMIN)—A person employed to maintain and operate a computer system and/or network.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)—All of the efforts to prevent or to detect theft of information by active technical means. Systematic measures for the detection and

nullification of technical penetrations or hazards, and physical security weaknesses facilitating such surveillance. Commonly referred to as “sweeps” or “debugging.”

TEMPEST—Unintentional Information-bearing emanations generated by electronic and electromechanical telecommunications and automated information-processing equipment. Countermeasures employed to suppress such emanations also are commonly referred to as TEMPEST.

TOP SECRET (TS)—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

WASTE, CLASSIFIED—Preliminary drafts, carbon sheets, carbon ribbons, stencils, handwritten notes, backing sheets, stenographic notes, worksheets, computer media and similar items containing classified information. Pending destruction, classified and safeguarded according to its classification.

APPENDIX:

SENATE RESOLUTION 243, TO ESTABLISH THE OFFICE OF SENATE SECURITY

100th Congress, 1st Session, July 1, 1987

RESOLVED,

Sec. 1. (a) That there is established, within the Office of the Secretary of the Senate (hereinafter referred to as the “Secretary”), the Office of Senate Security (hereinafter referred to as the “Office”), which shall be headed by a Director of Senate Security (hereinafter referred to as the “Director”). The Office shall be under the policy direction of the Majority and Minority Leaders of the Senate, and shall be under the administrative direction and supervision of the Secretary.

(b) The Director shall be appointed by the Secretary after consultation with the Majority and Minority Leaders.

(1) The Secretary shall fix the compensation of the Director. Any appointment under this subsection shall be made solely on the basis of fitness to perform the duties of the position and without regard to political affiliation.

(2) The Director, with the approval of the Secretary, and after consultation with the Chairman and Ranking Member of the Committee on Rules and Administration of the Senate, may establish such policies and procedures as may be necessary to carry out the provisions of this resolution. Commencing one year from the effective date of this resolution, the Director shall submit an annual report to the Majority and Minority Leaders and the Chairman and Ranking Member of the Committee on Rules and Administration on the status of security matters and the handling of classified information in the Senate, and the progress of the Office in achieving the mandates of this resolution.

Sec. 2. (a) The Secretary shall appoint and fix the compensation of such personnel as may be necessary to carry out the provisions of this resolution. The Director, with the approval of the Secretary, shall prescribe the duties and responsibilities of such personnel. If a Director is not appointed, the Office shall be headed by an Acting Director. The Secretary shall appoint and fix the compensation of the Acting Director.

(b) The Majority and Minority Leaders of the Senate may each designate a Majority staff assistant and a Minority staff assistant to serve as their liaisons to the Office. Upon such designation, the Secretary shall appoint and fix the compensation of the Majority and Minority liaison assistants.

Sec. 3. (a) The Office is authorized, and shall have the responsibility, to develop, establish, and carry out policies and procedures with respect to such matters as:

- (1) the receipt, control, transmission, storage, destruction or other handling of classified information addressed to the United States Senate, the President of the Senate, or Members and employees of the Senate;
- (2) the processing of security clearance requests and renewals for officers and employees of the Senate;
- (3) establishing and maintaining a current and centralized record of security clearances held by officers and employees of the Senate, and developing recommendations for reducing the number of clearances held by such employees;
- (4) consulting and presenting briefings on security matters and the handling of classified information for the benefit of Members and employees of the Senate;
- (5) maintaining an active liaison on behalf of the Senate, or any committee thereof, with all departments and agencies of the United States on security matters; and
- (6) conducting periodic review of the practices and procedures employed by all offices of the Senate for the handling of classified information.

(b) Within 180 days after the Director takes office, he shall develop, after consultation with the Secretary, a Senate Security Manual, to be printed and distributed to all Senate offices. The Senate Security Manual will prescribe the policies and procedures of the Office, and set forth regulations for all other Senate offices for the handling of classified information.

(c) Within 90 days after taking office, the Director shall conduct a survey to determine the number of officers and employees of the Senate that have security clearances and report the findings of the survey to the

Majority and Minority Leaders and Secretary of the Senate together with recommendations regarding the feasibility of reducing the number of employees with such clearances.

(d) The Office shall have authority --

(1) to provide appropriate facilities in the United States Capitol for hearings of committees of the Senate at which restricted data or other classified information is to be presented or discussed;

(2) to establish and operate a central repository in the United States Capitol for the safeguarding of classified information for which the Office is responsible; which shall include the classified records, transcripts, and materials of all closed sessions of the Senate; and

(3) to administer and maintain oaths of secrecy under paragraph (2) of rule XXIX of the Standing Rules of the Senate and to establish such procedures as may be necessary to implement the provisions of such paragraph.

Sec. 4. Funds appropriated for the fiscal year 1987 which would be available to carry out the purposes of the Interim Office of Senate Security but for the termination of such Office shall be available for the Office of Senate Security.

Sec. 5. (a) All records, documents, data, materials, rooms, and facilities in the custody of the Interim Office of Senate Security at the time of its termination on July 10, 1987, are transferred to the Office established by subsection (a) of the first section of this resolution.

(b) This resolution shall take effect on July 11, 1987.