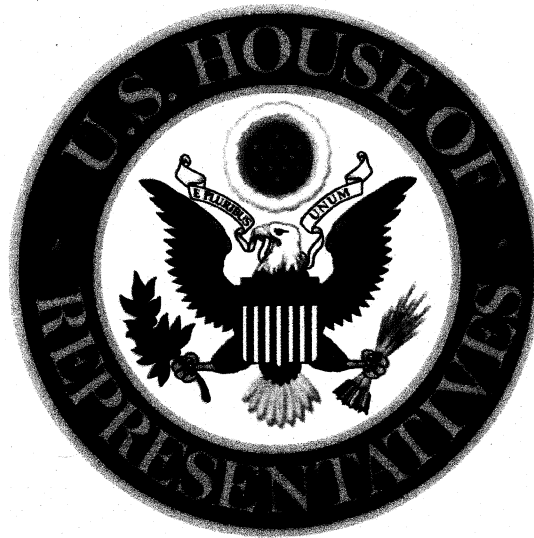


United States House of Representatives

SECURITY POLICY MANUAL



House Sergeant at Arms

Revised October 24, 2017

Foreword

The United States House of Representatives Security Policy Manual is a compilation of the best security practices and standards, written as guidance for Members and staff who hold a clearance and handle classified information. The Security Policy Manual outlines the role of the Office of the Sergeant at Arms House Security Division and specifies the regulations for handling classified information and proper security clearance protocols.

The Security Policy Manual is intended to assist offices in ensuring that sensitive and classified information is utilized solely for its intended purpose. It further delineates safeguards to guarantee the proper storage of classified information.

These security requirements and procedures are applicable to House Committees and Member offices to provide a uniform degree of protection for information that has been deemed classified in the interests of national security. These guidelines and procedures may also be supplemented by individual Committee and Member offices who currently maintain the best practices of the Intelligence Community.

Table of Contents

I.	General	4
a.	Purpose	4
b.	Scope	4
c.	Office Security Managers	5
d.	Exemptions	5
II.	Handling of Classified Information	6
a.	General	6
b.	Records of Classified Material	7
c.	Marking Classified Material	8
d.	Cover Sheets	9
e.	Production of Classified Material	9
f.	Storage and Certification	9
g.	Sensitive Compartmented Information Facility	9
h.	Secret and Confidential Cabinets	10
i.	Supervision of Storage Containers	10
j.	Alternate Storage Locations	10
k.	Safeguards During Use	11
l.	Transmission	11
m.	Reproduction	11
n.	Destruction	12
o.	Archive and Burn Runs	12
p.	Removal	12
q.	Communications Security	12
r.	Technical Security Counter Measures (TSCM)	13
s.	Information Security (INFOSEC)	13
t.	Operations Security (OPSEC)	13
III.	Personnel Security	15
a.	Access	15
b.	Staff Security Clearances	15
c.	Processing of Security Clearance Requests	15
d.	Clearance Standards for Staff	16
e.	Levels of Clearance	16
f.	Consultants and Contract Personnel	17
g.	Termination of Security Clearances	17
h.	Reinvestigation Program	17
i.	Secrecy Agreements	18
j.	Security Violations	18
k.	Security Education and Awareness	20
l.	Termination of Security Clearances, Employment, or Extended Leave	21
m.	Contact Reports	21
n.	National Security Threat List	22
IV.	Glossary	24

House Security Policy Manual

The U.S. House of Representatives must safeguard the classified information it obtains and reproduces. Accordingly, this Manual establishes uniform security guidelines applicable to the House. Cleared staff will follow and abide by the provisions of this Manual.¹

I. General

- a. **Purpose.** The Office of the Sergeant at Arms (SAA) House Security Division (HSD) will:
 - i. Oversee the issuance, administration, operation, and verification of House staff security clearances within its responsibility
 - ii. Serve as a central repository for classified information when requested by Members, Committees, and their staff, or when proper storage for classified material is not available
 - iii. Establish recommendations and procedures for the possession and transmittal of classified information
 - iv. Issue regulations and guidance on receiving, controlling, transmitting, storing, and destroying classified information
 - v. Assist with the implementation of the regulations as they pertain to the handling of classified material
 - vi. Educate Members and House staff on the protocols and responsibilities for handling and storing classified materials
 - vii. Manage the counterintelligence program for the U.S. House of Representatives
 - viii. Coordinate counterintelligence investigations, investigations of security violations, and other investigations
 - ix. Develop an Operation Security Program (OPSEC) for the U.S. House of Representatives
- b. **Scope.** This Manual establishes recommendations for safeguarding classified information in the possession of the House, its offices, and its employees. Each cleared employee of the House should be familiar with the security recommendations and should comply with them. Responsibility for ensuring that House staff comply with the provisions of this Manual is with the employing House Member. Any questions regarding the proper safeguarding of classified information or any other problems relating to security matters in general should be directed to the respective office security manager or to HSD for guidance or direction.

¹ The House Permanent Select Committee on Intelligence and the House Committee on Appropriations have additional rules and regulations for handling classified information based on various levels of classified information to include Special Access Programs and Compartmented programs.

While this Manual contains guidance on handling and storing classified information, failure to comply with this Manual could result in a security violation and a referral by HSD to the Committee Chair or the Member to determine whether any violation of law or rule has occurred.

- c. Office Security Managers.** In order to achieve and maintain a strong security posture, a security manager should be assigned to each personal office, support office, and committee. After initial training and certification, and under the administrative guidance of the Director of House Security, each office security manager will be responsible for the following duties:

 - i.** Implementing the recommendations of this Manual within the office and ensure that all employees of the office are familiar with these provisions.
 - ii.** Attending biannual briefings presented by the SAA and providing security advice and guidance to office personnel.
 - iii.** Serving as the office's liaison to the SAA for security matters.
 - iv.** Conducting daily security checks and reporting security violations to the SAA.
- d. Exemptions.** Those House offices with custodial control over large amounts of classified information may be exempted from certain provisions of this Manual. The Director of House Security will review the respective policies and procedures for handling classified information to ensure such policies fully meet or exceed the standards of this Manual.

II. Handling of Classified Information

a. General

- i. **Policy.** Information retained by the House that is classified in accordance with *Executive Orders 13526* and *12333* as amended and the *Atomic Energy Act of 1954* should be handled and safeguarded in accordance with the provisions of this Manual. This includes memoranda and working papers. Any material generated internally containing classified information should be handled and safeguarded in the same manner. Failure to properly handle and safeguard classified information may result in violations, investigations, and penalties identified in *Section III, Subsection E.9, "Security Violations."*
- ii. **Classification.** Certain information must be controlled in the interest of national security. Such information is assigned one of three levels of classification according to *LAW Executive Order 13526, "Classified National Security Information."* The classifications are as follows:

TOP SECRET: Information that if disclosed without authorization could reasonably be expected to cause exceptionally grave damage to the national security.

SECRET: Information that if disclosed without authorization could reasonably be expected to cause serious damage to the national security.

CONFIDENTIAL: Information that if disclosed without authorization could reasonably be expected to cause damage to the national security.

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.

"For Official Use Only (FOUO)," "Law Enforcement Sensitive," and "Sensitive but Unclassified" are document designations, not classifications. These designations are used by the Department of Defense and a number of other federal agencies to identify information or material which, although unclassified, may not be appropriate for public release. However, such information can be shared with individuals with a "need-to-know" of the content, while still under the control of the individual possessing the document or product. The material should then be returned to the originating government office and be properly retained or destroyed. Whenever possible, FOUO information should not be passed over unencrypted communications lines (e.g., open phones, non-secure fax, and personal e-mails). If no secure communications are available for transmission, FOUO material may be sent via unprotected means, with the approval of the SAA.

In the event that the classification of any information is questioned or challenged, such information will be treated as classified at the highest designated level until the matter is resolved. In the event of such a question or challenge, the originator of the information will 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 will be referred to the SAA House Security Division, which will pursue the issue with the appropriate agency(s).

b. Records of Classified Material

- i. **Accountability Records.** The office security manager will maintain a log of all classified material received, produced by, or in the custody of the office, which shall reflect at a minimum:
 1. The office document control number
 2. The date of receipt
 3. The classification of the material
 4. The originating office or agency
 5. The date of the document
 6. The addressee
 7. A brief, unclassified description of the material
 8. The file where the document is located
- ii. **Inventory of Classified Material.** The SAA House Security Division will conduct a periodic inventory check of classified material in the possession of House offices and Committees. The inventory will consist of the actual sighting of each item listed in the office's log of classified holdings. The inventory will be checked against the records of the SAA House Security Division to ensure that all classified material is properly accounted for.
- iii. **Special Requirements for Secret and Top Secret Material.** It is essential that the office security manager maintain an up-to-date record of all persons who are afforded access to Secret and Top Secret material. The office security manager should also maintain a record of each item identified as Secret and Top Secret, the names of all individuals given access to the item, and the date on which access was granted. Such records will be periodically forwarded to the SAA House Security Division where they will be retained for a period of two years from the date the material was destroyed, dispatched outside the House, declassified, or downgraded to less than Secret.
- iv. **Annual Review.** For the purpose of minimizing the quantity of classified material on hand at any given time, each House office should annually review all classified information. Offices may place classified material in long-term storage or may forward it to the SAA House Security Division (using proper custodial procedures), which will assume responsibility for its proper storage or destruction in coordination with the House office.
- v. **Loss or Possible Compromise.** Any person who has knowledge of the loss or possible compromise of classified information should immediately

report the circumstances to either the office security manager or the SAA so that a damage assessment may be conducted.

- vi. **Daily Systems Checks.** Office security managers should implement a system of security checks at the close of each working day to ensure that all classified material under their control is completely secure. The SAA can provide advice regarding the establishment of such a system. *Standard Forms 701 and 702* are available by request for assistance in documenting daily safe and area checks.
 - vii. **Derivative Classification.** Derivative classification involves incorporating, paraphrasing, restating, or generating a new form of information that is already classified, marking the new material consistent with the classification markings that apply to the source information. This includes the classification of information based on an existing classification guide.
 - viii. **Original Classification Authority (OCA).** An OCA is an individual authorized to classify information in the first instance including individuals who are designated in writing as “acting” officials in any of the delegated positions. An OCA may not be delegated beyond these positions.
- c. **Marking Classified Material.** The originator of material containing 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. Therefore, it is essential that all classified material be clearly marked so that the holder knows which level of classification is assigned to the material.
- i. **Portion Markings.** Paragraphs within documents containing information of varying levels of classification or containing both classified and unclassified information should be individually marked. The designations “U” (Unclassified), “C” (Confidential), “S” (Secret), and “TS” (Top Secret) are placed in parentheses at the beginning of each paragraph for this purpose.
 - ii. **Identification Markings.** All classified material should be marked to show both 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.
 - iii. **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, on the title page, and on the outside of the back cover. If no covers or title page exist, the overall classification should be stamped at the top and bottom of the first page and on the back of the last page.
 - iv. **Page Markings.** Interior pages of classified documents should be stamped at the top and bottom with the highest classification of the information appearing thereon, or with the overall classification of the document.

- v. **Additional Markings.** In addition to the markings specified above, classified material should be marked, if applicable, with one or more notations which indicate the material is further restricted to special access categories (e.g., "Restricted Data" and "Dissemination and Reproduction" notices).
- d. **Cover Sheets.** When removing classified information/material from storage a cover sheet must be provided according to the level of classification. The *Standard Forms 703, 704, and 705* are available for documentation.
- e. **Production of Classified Material.** When an office creates classified material, such material should be entered into the office log. Such material should be brought to the SAA House Security Division for entry into the SAA document control system. Such material should be properly marked with the appropriate security classification, as outlined above, and safeguarded in accordance with the provisions of this Manual.
- f. **Storage and Certification.** Member offices should not store classified material unless they have been certified by the SAA House Security Division as having adequate control procedures and storage capability. Classified material must never be left unattended. It must be maintained in a General Services Administration (GSA) approved security container or under direct surveillance of an authorized person at all times. The SAA will provide storage facilities for any office which does not meet these requirements.
- g. **Sensitive Compartmented Information Facility (SCIF).** The SAA House Security Division will provide SCIF accommodations upon request for CLASSIFIED meetings. The SCIF may only be used by U.S. citizens with the proper clearances. Please call (202) 226-2044 to request the use of a SCIF.

Classified material, when not in actual use, shall be stored as follows:

- i. Top Secret and Special Access material should be stored in a GSA approved safe 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*.
- ii. Entry to the room in which the container is located must be controlled by a properly cleared employee in order to restrict admittance to the room during normal working hours.
- iii. The container, as well as the door(s) to the room in which the container is located, must be locked at the close of business each day.
- iv. The room in which the container is located must be protected by an intrusion detection system approved by the SAA.

Note: Storage of Top Secret and Special Access material in a room not certified as a SCIF is not permitted in accordance with *Intelligence Community Directive 705*.

- h. Secret and Confidential Cabinets.** Secret and Confidential material must be stored in a GSA approved security container. Storage of classified material in a steel file cabinet secured by a steel bar and a three-position changeable combination lock is no longer permitted. All classified documents removed for approved storage must have *Standard Forms 703, 704, and 705* as a cover sheet.
- i. Supervision of Storage Containers.** Only a minimum number of authorized persons may possess the combinations to the storage containers or vaults or have access to the information stored therein. The SAA will maintain a record of the names, phone numbers, and addresses of persons having knowledge of the combination in order to facilitate investigations of containers found open and/or unattended during non-office hours. In addition, the combinations of all storage containers will be stored on a classified network maintained by the House Security Division.

Combinations to security containers shall be changed by Chief Administrative Officer (CAO) personnel only and under the direction of House Security Division personnel having appropriate security clearances. The combination shall be changed when:

- i.** The container is placed in use
- ii.** A person knowing the combination is transferred from the office to which the container is assigned
- iii.** A combination has been possibly compromised
- iv.** Annually

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

Current combinations should be classified no lower than the highest category of classified information authorized for storage in the container concerned. Each security container should display a conspicuous sign indicating that it is open whenever it is not secured and should 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 must be kept locked when not under the direct supervision of an authorized person entrusted with the combination or the contents. CAO personnel will work jointly with the SAA House Security Division to provide access to safe combinations when necessary.

- j. Alternate Storage Location.** The SAA will provide classified material storage in its facilities for any Member or Committee office upon request. In the event a cabinet or vault becomes damaged or inoperable in a Member or Committee office, the SAA, Division of House Security will provide secure storage until the

cabinet or vault is restored. The SAA House Security Division will conduct a security assessment of a Member or Committee office to determine whether the office space is eligible for storage of classified information.

- k. **Safeguards During Use.** Classified information may be provided only to a properly cleared person on the basis of need-to-know. Determination of need-to-know is an individual responsibility. Before divulging any classified information, House staff should make certain of the recipient's identity, level of clearance, and need-to-know. In order to facilitate such determination, the SAA House Security Division will maintain a list of House staff whose level of clearance has been properly established.
 - i. **Need-to-know:** Applies to individuals requesting access to sensitive and/or classified material. The authorized holder of the classified/sensitive information determines whether access to the material is required so that another appropriately cleared individual may perform his/her official duties. This measure was developed to prevent unauthorized disclosure of classified/sensitive information. Classified material, when not safeguarded as provided for in *Section 6* and when in actual use by cleared personnel, must be:
 - 1. Kept under the constant surveillance of an authorized person who is in physical proximity to and can exercise direct security controls over the material
 - 2. Covered, turned face down, placed in storage containers, or otherwise protected when unauthorized persons are present
 - 3. Returned to storage containers as soon as practical after use
- l. **Transmission.** Classified material should be enclosed in opaque inner and outer covers before transmittal. The inner cover should be sealed and plainly marked with the classification level, delivery address, and recipient. The outer envelope should be sealed and addressed to an office or group, with no indication of the classification, contents, or recipient's name. Receipt of classified material shall identify the sender, the addressee, the document, and its classification level, but should contain no classified information. The receipt should be signed by the recipient and returned to the sender. The SAA House Security Division is available to transmit classified material between House offices. Transmission of classified material outside the House should be accomplished only by SAA personnel or other authorized federal agency couriers. Transmission of classified material between House offices or directly to the SAA should be accomplished by appropriately cleared and briefed personnel.
- m. **Reproduction.** Documents marked ORCON require permission from the originator to reproduce. Sensitive Compartmentalized Information and other Special Access information *shall not* be reproduced. Reproductions of classified material should be kept to an absolute minimum and should be marked or stamped with the same classification as the original. Reproduction of classified material should be made only on equipment specifically designated by the SAA

for the reproduction of classified material. Offices are reminded that immediately after reproduction of classified material, three (3) blank sheets of paper should be run through the photocopier used for the reproduction. The House office which reproduces classified material is responsible for bringing all copies under proper accountability controls and should notify the SAA of the particulars as provided for in *Section 4, "Record of Classified Material."*

- n. **Destruction.** All classified material should be returned to the SAA House Security Division as soon as it is no longer needed so that it can be properly disposed of pursuant to this Manual. At the office's request, all such material will be destroyed, returned to its originator, or archived by the SAA. Records of destruction or other disposition will be maintained by the SAA. Any document bearing an SAA bar code or document control number must be returned to the SAA for destruction. Before destroying any classified material, please call the SAA House Security Division at (202) 226-2044.
- o. **Archive and Burn Runs.** The SAA will provide archive and burn runs for House offices. These burn runs are for classified documents only. All classified papers should be placed in a marked burn bag. The weight of the bag cannot exceed 10 pounds. Classified documents to be destroyed must not contain items such as staples, paper clips, binder clips, etc.
- p. **Removal.** Under no circumstances is classified material to be taken to a personal residence, or otherwise removed from approved storage or working areas, without prior written approval of the SAA. Violation of this provision may result in termination of an individual's security clearance, and the individual may be subject to criminal prosecution.
- q. **Communications Security (COMSEC).** Measures and controls taken to deny unauthorized persons access to information derived from telecommunications. COMSEC includes crypto-security, transmission security, emission security, traffic-flow security, and physical security of COMSEC material.
 - i. **Telephones.** Classified information should not be discussed over open telephone lines. Foreign intelligence services and other groups or individuals may monitor telephone calls to and from House offices. One should not attempt to "talk around" classified information over unsecured telephone lines. There are a number of secure telephones in the House which are approved for discussion of classified information. The SAA House Security Division can assist cleared House staff in accessing secure telephones.
 - ii. **Discussions/Briefings.** Discussion or presentation of classified material must take place in the offices of the Division of House Security or in another accredited secure area. Classified information should not be discussed in a personal office. Information pertaining to policy decisions and classified information available to the Members and House staff is highly desirable to various individuals, organizations, and foreign

governments.

- r. **Technical Security Counter Measures (TSCM).** The U.S. Capitol Police (USCP) Technical Security Counter Measures (TSCM) team is available on a case-by-case basis when requested by a Member or Committee office security manager to provide a secure environment where sensitive and classified information can be discussed. The TSCM sweep is a systematic evaluation and inspection of a room, area, or item and is designed to detect and deter the installation of electronic listening devices. Due to time constraints and the cost of manpower to perform a TSCM sweep, the inspection by the USCP TSCM team can only provide a limited measure of security. An accredited Sensitive Compartmented Information Facility is the only way to ensure complete security for a classified meeting. Requests for TSCM sweeps prior to a sensitive hearing or meeting should be scheduled 24 hours in advance through the SAA at (202) 226-2044.
- s. **Information Security (INFOSEC).** Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Classified information may be processed only on approved House computer systems. Privately owned computers must not be used to process classified information. Equipment used to process classified information must have an approved security plan in place before any information is processed. For assistance in preparing the security plan, contact the SAA, Division of House Security at (202) 226-2044. **Any questions or concerns regarding proper procedures for processing or printing classified information should be resolved by contacting the SAA prior to acting. Furthermore, the Chief Information Security Officer should be contacted for guidance on protecting computer systems.**
- t. **Operations Security (OPSEC).** Identifying and protecting information that might provide a competitor or adversary with clues regarding domestic plans or capabilities and thereby enable the competitor or adversary to thwart a planned operation or activity. OPSEC is critical at all agencies. Given the nature of the work being performed by the House, House staff should know which types of House information are critical and should be protected and not discussed in open spaces. Examples of critical information include but are not limited to personally identifiable information, sensitive information, and draft legislation.

The House faces constant threats, and some target House employees. House staff are encouraged to mitigate risk utilizing the following five-step OPSEC process:

OPSEC Process:

- i. Identification of critical information
- ii. Analysis of threats
- iii. Analysis of vulnerabilities

- iv. Assessment of risks
- v. Application of countermeasures

III. Personnel Security

- a. **Access.** No person will be given access to classified information or material without a security clearance. 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 need-to-know shall be made by the person in possession of the information sought.
- b. **House Staff Security Clearances.** Requests for House staff security clearances must originate with the employing Member, or in the case of Committee staff, with the Chair. Requests for clearances for employees of House Officers/Officials must originate with the employing Officer/Official. Requests for House staff security clearances are to be kept to the absolute minimum required for the conduct of official House business. The following restrictions govern the request for a House staff security clearance:
 - i. Each Member of the House shall have no more than two cleared staff.
 - ii. Members and Committee Chairmen must determine which positions on their staff require security clearances. Clearances will only be granted to House staff whose assignments require access to classified information. The SAA can provide assistance in determining which staff positions require clearances.
 - iii. In order to be eligible for a security clearance, House staff must be on the payroll of the Member or Committee requesting or sponsoring the clearance. Shared staff are considered to be under the Member's personal office.
 - iv. Should an individual holding a security clearance be reassigned, his or her clearance will automatically be deactivated, and will remain inactive unless it is determined that the individual's new assignment requires access to classified information.
 - v. No personal staff of a retiring Member shall be processed for a security clearance during the last year of such Member's term of office.
 - vi. Interim Security Clearances are not granted for House staff.
 - vii. If a security clearance investigation results in a denial, the Department of Defense will notify the applicant of the denial and the proper steps to appeal the decision. The SAA is available to assist in the appeal process but cannot appeal on the applicant's behalf.
- c. **Processing of Security Clearance Requests.** When a Member, Committee Chair, House Officer, or House Official determines that a member of his or her staff requires access to classified information, he or she will submit the request in writing to the House Sergeant at Arms. A sample Security Clearance Request Letter can be found at the SAA's website:
 (<http://saa.house.gov/ohs/requesting-a-new-clearance.shtml>)

The SAA will provide the House staff with a security clearance application. The security clearance application must be completed within 30 days of the date on the request letter through the Office of Personnel Management's (OPM) *Electronic Questionnaire for Investigations Processing (E-QIP)*. Instructions for the login process are provided via e-mail from the SAA House Security Division. When the application is completed, the applicant must call the SAA to set up an appointment. The applicant will sign the *DOD Secrecy Agreement* along with the *Request for Check of Criminal History Records (CP-491)*. The applicant will also be given a copy of an excerpt from the *Espionage Act*. The application then will be referred to the appropriate agency for processing. A Tier 5 or Tier 3 background investigation can be a lengthy process but is necessary to properly investigate the full scope of an individual's background. When a clearance is granted, the SAA will schedule an initial security briefing. House staff must receive an initial security briefing before being granted access to classified information.

If the application is not completed within 30 days, the clearance process will be terminated, and the individual will be required to submit a new request letter. Applicants who fail to complete the application on 3 separate occasions must wait a full calendar year before reapplying.

Persons requiring the transfer of their security clearance from an agency, Committee, or personal office to a new office within the House of Representatives must submit a *Transfer of Clearance Form*. A template can be found at the SAA website (<http://saa.house.gov/ohs/requesting-a-clearance-transfer.shtml>).

- d. Clearance Standards for House staff.** All applicants for security clearances must be:
- i. Of excellent character, discretion, trustworthiness, and loyalty to the United States.
 - ii. Citizens of the United States. However, House staff may request a waiver of the citizenship requirement for a permanent resident alien seeking citizenship, an admitted refugee, an individual granted asylum who will be seeking citizenship, or a person who owes allegiance to the United States. Individuals must be uniquely qualified to perform a mission in support of official House business as determined by the Member. Requests for waiver of this requirement must be made in writing to the Director of House Security, who will make a recommendation to the Speaker and Minority Leader. A waived individual may seek a Secret-level clearance only.

To ensure that these criteria are met, Federal agents will conduct an investigation into each applicant's personal, social, professional, educational, and financial background.

- e. **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 controlled need-to-know basis and are not granted to personal office staff.

i. **Other Clearances:**

1. **Sensitive Compartmented Information (SCI).** SCI clearances will be granted in accordance with CIA guidelines and may only be granted to full-time Committee staff, Leadership staff, and House Officer staff. Personal office staff may not obtain or hold an SCI clearance.
2. **Department of Energy Clearance (DOE).** A DOE clearance will be granted in accordance with the Department of Energy guidelines. Staff must provide written justification indicating why they require DOE access (i.e., Committee work or having a nuclear facility in the Member’s district).
3. **Executive Order 13556 – Controlled Unclassified Information (CUI).** Standardizes the way the Executive Branch handles information which requires protection but is not classified. This classification mandates a government-wide uniform program to identify and protect Sensitive but Unclassified (SBU) information and requires identification of all SBU materials be marked as such. The authority of such markings should also be identified, i.e., law, regulation, government-wide policy. Markings must be reviewed to identify areas for consolidation or elimination of redundancy. All categories, subcategories, and markings should be defined.

- f. **Consultants and Other Personnel.** Consultants, fellows, detailees, contract personnel, and other non-House employees whose assigned duties require access to classified information will be subject to the same security requirements as House staff. Such individuals should not be granted access to classified information until written verification of the individual’s security clearance is obtained by the SAA from the employing agency.

- g. **Termination of Clearances.** The Director of House Security will terminate the clearance(s) of an individual if:
- i. The sponsoring Member requests such termination
 - ii. The employee terminates employment with the House
 - iii. The employee is reassigned to a position which does not require access to classified information
 - iv. Termination is recommended by the Speaker and Minority Leader

h. **Reinvestigation Program.**

- i. Reinvestigations of House employees holding a security clearance will be conducted every five years for a Top Secret and every ten years for a

Secret clearance. The SAA will notify House staff when they are due for reinvestigation.

- ii. The Director of House Security will initiate reinvestigation of House staff at the request of the sponsoring Member, Committee Chair, or House Officer.

- i. **Secrecy Agreements.** A Department of Defense secrecy agreement must be executed by all House staff who are granted security clearances. The agreement will contain provisions that prohibit the signer from divulging or releasing classified information to unauthorized individuals.

- j. **Security Violations.** A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, regardless of whether a compromise occurs. No matter how minor, any security infraction must be reported immediately to the SAA or the office security manager so that the incident may be evaluated and any appropriate action taken. The following are examples of behaviors that are of particular concern and may affect a security clearance:

- i. **Violations:**

- 1. Leaving a classified file or security container unlocked and unattended either during or outside normal working hours
 - 2. Keeping classified material in a desk or unauthorized cabinet, container, or area
 - 3. Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or outside normal working hours
 - 4. Reproducing or transmitting classified material without proper authorization
 - 5. Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know
 - 6. Discussing classified information over a non-secure telephone
 - 7. Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard
 - 8. Carrying safe combinations or computer passwords (identifiable as such) on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer
 - 9. Failure to properly mark classified documents
 - 10. Failure to follow appropriate procedures for destruction of classified material

- ii. **Major Violations.** The significance of a security violation does not depend upon whether information was actually compromised. It depends upon the intentions and attitudes of the individual who committed the violation. Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining a security

clearance. Infrequent and accidental minor violations sometimes occur and will be dealt with accordingly. However, deliberate or repeated failure to follow the rules will not be tolerated. Repeated violations may be a symptom of underlying attitudes or emotional or personality problems that are a serious security concern. The following behaviors are examples of particular concern and may affect a security clearance:

1. A pattern of routine security violations due to inattention or carelessness or a cynical attitude toward security discipline
2. Taking classified information home or carrying it while traveling without proper authorization
3. Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any attempt to gain unauthorized access to computer systems, information, or databases.
4. Intoxication while carrying classified materials
5. Deliberate revelation of classified information to unauthorized persons
6. Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
7. Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one's own work area is a potential indicator of unauthorized copies being made.
8. Failing to report requests for classified information from unauthorized individuals
9. Failure to report a security violation is itself a security violation and may be a very serious concern.

iii. **Investigations.** All known, suspected, or alleged security violations should be reported to the SAA House Security Division. Upon the consent of the Committee Chair or Member (when it pertains to his or her office), the SAA will investigate the allegations. The formal investigation report will include:

1. A finding on whether a probable compromise of classified information occurred
2. A written report of those interviewed
3. A finding as to the person(s) responsible
4. A statement as to the degree of compromise
5. The security violation history of each person found responsible
6. Recommendations for remedial action to preclude recurrence of such violation(s). Investigations shall be coordinated with the security manager of the office concerned, who shall receive a copy of the investigation report.

iv. **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 that a written notice of reprimand and warning of consequences for further violations be issued to the sponsoring Member, Committee Chairman, House Officer, or Official
3. Recommendation to the sponsoring Member that the House staff responsible be denied further access to classified information until such individual attends a refresher briefing on security regulations conducted by the SAA.

Any incident determined by the investigation to involve *willful* compromise of classified information will be referred to the Office of the General Counsel and/or House Ethics Committee, who may impose sanctions or make recommendations that the House impose sanctions, including criminal penalties. In addition, the SAA may recommend to the Member or the Committee Chair internal administrative sanctions as a result of its investigation, up to and including termination of employment.

Under no circumstances will penalties for security violations, as described in this subsection, be imposed by the SAA. However, if the matter is referred to an outside agency, that agency may impose sanctions.

k. Security Education and Awareness. The SAA House Security Division is responsible for the administration of a security education and awareness program for House employees. Participation in the program is mandatory for staff holding security clearances. The Security Awareness Program consists of the following:

- i. **Initial Security Briefings.** Before being allowed access to classified information, all House staff granted a security clearance will be given an initial security briefing by SAA staff. 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 they have read and understand the Security Policy Manual and agree to comply with the provisions thereof. In addition, House staff must comply with *Clause 13 of Rule XXIII of the Rules of the U.S. House of Representatives* and must sign the "Oath to Access Classified Information" which will be kept on file with the SAA. **All House staff must attend the initial security briefing before their security clearance is activated. This includes periodic reinvestigations and transfers.**
- ii. **Refresher Briefings.** Refresher briefings are required both annually and when House staff is granted access to classified information of

significantly greater sensitivity than their previous investigation permitted, or when security violations are serious or continuing.

- iii. **Topical Briefings.** Briefings on various security-related issues will be scheduled periodically. All House staff holding the necessary level of clearance will be informed in advance. Subjects to be covered in topical briefings include: counterintelligence, communications security, hostile intelligence activities on Capitol Hill, computer security, and technical security countermeasures.
 - iv. **Foreign Travel Briefings.** During foreign travel, House staff are more vulnerable to common street crime, social unrest, and acts of terrorism. To minimize the threat to the individual, the SAA 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 Members and House staff contemplating travel.
 - v. **Termination Briefings.** House staff will be given a security termination briefing and will sign a termination statement upon termination of employment, withdrawal of clearance, beginning of terminal leave (60 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 will be the responsibility of the employing Member to ensure that employees attend termination briefings.
 - vi. **Counterintelligence Briefings.** The Federal Bureau of Investigation (FBI) frequently conducts counterintelligence briefs. The SAA strongly encourages House Members and staff comply with their requests.
 - vii. **Security Awareness Bulletins.** The SAA will periodically distribute current articles and reports on security related topics to all office security managers. Office security managers are responsible for circulating the bulletins to all staff within their respective offices.
- i. **Termination of Security Clearances or Employment, and Extended Leave.** House staff whose security clearances have been withdrawn, whose employment has been terminated, who are reassigned to a position not requiring access to classified information, or who are taking terminal leave for a period of 60 days or more, should surrender all classified documents or materials in their possession before departure and will receive a security termination briefing.
- m. **Contact Reports.** The conduct of official House business sometimes involves the interaction of House staff with representatives of nations considered adversaries of the United States.
- i. All House staff, regardless of whether they hold a security clearance, should immediately report to the SAA 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 obtain classified information
2. The House staffer is concerned that they may be the target of an attempted exploitation by a foreign entity
- ii. In addition to the requirements of *Section II(a)*, all House staff having access to classified information should immediately report to the SAA:
 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 House duties
 2. Any actual or suspected attempt by an official or representative of a designated country to establish social relationships, cultivate friendships, or to place one under obligation
 3. Any attempt by officials or representatives of any country to:
 - a. Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.
 - b. Coerce staff by blackmail or threat.
- n. **National Security Threat List.** Dramatic changes in Eastern Europe and the former Soviet Union in the late 1980s and early 1990s, as well as increased economic, scientific and technological espionage activities by foreign intelligence services, have resulted in new guidelines governing the FBI's counterintelligence program. The new guidelines 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:
 1. **Critical Technology:** Foreign intelligence activities directed at U.S. critical technologies as identified by the National Critical Technologies Panel
 2. **Proprietary Economic Information:** Foreign intelligence activities directed at the ultimate collection of U.S. industrial activities or proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial base
 3. **Clandestine Activity:** Covert foreign intelligence activity in the United States; espionage
 4. **Defense Information:** Foreign intelligence activities directed at the 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 and foreign affairs information and U.S. Government officials, including House employees

7. Active Measures: Foreign intelligence activities involving perception management and active measures activities

Any House staff having knowledge or suspicion of such activities should immediately report such knowledge or suspicion to the Director of House Security Division.