

## INFORMATION SECURITY BRIEFING

## A. OVERVIEW

1. Executive Order 12356 (E.O. 12356), "National Security Information," Information Security Oversight Office (ISOO) Directive No. 1, National Security Decision Directives 84 and 197 (NSDD-84 and NSDD-197), and Department security regulations prescribe and implement procedures for classifying, declassifying, downgrading, and safeguarding classified information, to include security awareness briefings, reporting attempts to obtain illegal or unauthorized access to classified or otherwise sensitive information, and reporting employee contacts with nationals of certain foreign countries or political entities, to include hostile intelligence services.
2. E.O. 12356 further recognizes that it is essential that the public be informed concerning activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be safeguarded from unauthorized disclosure.
3. E.O. 12356 also requires each agency that handles national security information to establish a security education program. The program shall be sufficient to familiarize all necessary employees with the provisions of E.O. 12356, ISOO Directive No. 1, NSDD-84, NSDD-197, and Department security regulations and to impress upon them their individual security responsibilities. The program shall also provide refresher and termination briefings.

## B. PURPOSE OF BRIEFING

1. Under the provisions of E.O. 12356 and Department security regulations, each employee has a continuing obligation to safeguard information vital to the national security of the United States. This briefing is designed to help you obtain a better understanding of your obligations regarding information security matters which will help you to discharge your security responsibilities as a HUD employee.
  2. Basically, the responsibility for security rests with the employee who has access to any form of information, classified or unclassified. Physical controls over information, facilities, and storage areas are not totally sufficient for good security. Rather, we must be security conscious and aware of the importance of our Department security regulations. While seemingly complex and restrictive, our security regulations are based upon sound judgment, and are designed to provide the utmost protection for classified and otherwise sensitive information in the possession of this Department.
-

---

1750.1 REV-4 CHG-2

Appendix 6

---

3. This briefing will assist you in developing good security habits and acquiring a better understanding of Department security regulations. However, the contents of this briefing shall not be used as a substitute for Department security regulations, as outlined in HUD Handbook 1750.1 Rev-4, "National Security Information," which provide more specific information and detailed procedures for handling and safeguarding classified information. Additionally, any questions you may have about security matters can be resolved by directing the questions, oral or written, to the Assistant Director for Security, Headquarters Operations Division, Office of Investigation, Office of Inspector General, Room 8270, 451 Seventh Street, S.W., Washington, D.C. 20410, telephone number FTS 755-6387.
- C. TERMS AND DEFINITIONS - The following is a brief description of some information security program terms and their definitions that may be helpful:
1. Access - The ability and opportunity to obtain knowledge of classified information.
  2. Communications Security (COMSEC) - Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such information.
  3. Classification Guide - A document issued by an original classification authority that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively.
  4. Compromise - The intentional or unintentional disclosure of classified information to unauthorized persons.
  5. Confidential Source - For the purposes of this briefing, any individual or organization that has provided, or may provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information and/or relationship, be held in confidence.
  6. Controlled Area - Any area that is restricted or controlled for security reasons.
  7. Custodian - An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified documents.
-

---

1750.1 REV-4 CHG-2

---

Appendix 6

---

8. Damage Assessment - An analysis of the damage that has occurred to the national security as a result of an unauthorized disclosure of classified information.
9. Declassification - A determination made by an original classification authority that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation. The identification of an original classification authority is contained on the cover or first page of a classified document.
10. Derivative Classification - The act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classified marking of the source material. The source of information ordinarily consists of classified documents, usually correspondence or publications generated by an original classification authority, or a classification guide issued by an original classification authority.
11. Downgrade - A determination made by an original classification authority that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.
12. Executive Order (E.O.), 12356, "National Security Information" - Prescribes a uniform system for classifying, declassifying, and safeguarding national security information.
13. Forced Entry - Unauthorized entry into a controlled area or security storage container in a manner that is easily recognizable.
14. Foreign Government Information - This type of information includes:
  - a. Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence.
  - b. Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or

governments or an international organization of governments, or any element thereof, requiring that information, the arrangement, or both, are to be held in confidence.

---

1750.1 REV-4 CHG-2

Appendix 6

---

15. Hostile Contacts - Within the meaning of NSDD-197, when an individual of any nationality, either within or outside the scope of the employee's official activities, attempts to obtain illegal or unauthorized access to proprietary, sensitive, or classified information, to include targetting an employee for exploitation. Such contacts must be reported immediately to the Assistant Director for Security, Office of Investigation, Office of Inspector General, at FTS 755-6387.
16. Information Security Program - A program consisting of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is required by executive order or statute.
17. Information Security Oversight Office (ISOO) Directive No. 1 - Implements the provisions of E.O. 12356 and further sets forth guidance relating to original and derivative classification, downgrading, declassification, and safeguarding of national security information.
18. Logging Control Officer - An employee responsible for the proper maintenance of records relating to the safeguarding, storage, accountability, transmission, and destruction of national security information.
19. Logging Control Point - A place designated within an organization/office where all classified information is received, recorded, stored or transmitted. Each Logging Control Point has a Logging Control Officer who maintains the required accountability and control over the classified information received.
20. Multiple Sources - The term used to indicate that a document is derivatively classified when it contains classified information derived from two or more sources.
21. National Security Decision Directive 84 (NSDD-84), "Safeguarding National Security Information" - Establishes procedures to safeguard against the unauthorized disclosure of national security information.
22. National Security Decision Directive 197 (NSDD-197), "Reporting Hostile Contacts and Security Awareness " - Establishes procedures for reporting hostile contacts and for providing security awareness briefings.

23. National Security - The national defense or foreign relations of the United States.
24. National Security Information - Information that has been determined pursuant to E.O. 12356 or any predecessor E.O. to require protection against unauthorized disclosure. National security information is also referred to as classified information. Such information shall be appropriately marked TOP SECRET, SECRET, or CONFIDENTIAL, according to contents.

---

4/86

4

---

1750.1 REV-4 CHG-2  
Appendix 6

- 
25. Normal Use - Opening a combination lock. releasing the locking mechanism, gaining entry to the container, removing and replacing material, and relocking the container.
26. Original Classification - An initial determination, made by an original classification authority, that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.
27. Original Classification Authority - The authority vested in a designated Executive Branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. No HUD official has been granted original classification authority under E.O. 12356.
28. Security Classification Levels - Information which requires protection against unauthorized disclosure in the interest of national security is classified by an official exercising original classification authority, at one of the following levels:
- a. TOP SECRET is applied only to information, the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security.
  - b. SECRET is applied only to information, the unauthorized disclosure of which could be expected to cause serious damage to the national security.
  - c. CONFIDENTIAL is applied only to information, the unauthorized disclosure of which could cause damage to the national security.
29. Security Clearance, the Need-to-know, and Access :
- a. A security clearance is a personnel security determination that an employee is currently trustworthy and authorized to have access to a specific level of classified information. This determination is made by the Department's Assistant Director for Security, subsequent to the favorable completion

and adjudication of a personnel security investigation. Formal access to classified information is completed when the employee receives this Information Security Briefing, and signs Standard Form 189, Classified Information Nondisclosure Agreement.

- b. Need-to-know - A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of, the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge or possession of, or access to

---

5

4/86

---

1750.1 REV-4 CHG-2

#### Appendix 6

---

classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

- c. Before any Department employee releases classified information in any form, he/she shall require positive identification, determine level of security clearance, and establish the need-to-know of the recipient. Verification of any employee's need-to-know shall be established by contacting the employee's supervisor. Verification of an employee's personnel security clearance shall be made by contacting the Assistant Director for Security. These procedures are considered essential prerequisites to the release of any level of classified information.
- 30. Sensitive Compartmented Information (SCI) - Highly sensitive intelligence information, the disclosure of which may result in the compromise of intelligence sources or methods.
  - 31. Sensitive Position - Any position in this Department the occupant of which could bring about, because of the nature or conditions of employment, a materially adverse effect on the national security.
  - 32. Special Access Program - Any program imposing "need-to-know" or access controls beyond those normally provided for access to TOP SECRET, SECRET or CONFIDENTIAL information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials to determine "need-to-know," or special lists of persons determined to have a "need-to-know."
  - 33. Surreptitious Entry - The unauthorized entry into a controlled area or security storage container in a manner in which evidence of such entry is not readily recognizable.

34. Unauthorized Disclosure - A communication or physical transfer of classified information to an unauthorized person or place.
35. Upgrade - A determination that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification level. This determination may only be made by the official exercising original classification authority over the upgraded information.

D. GENERAL SECURITY REQUIREMENTS

1. Accountability of Classified Information - The establishment of certain administrative procedures for regulation the accountability of all classified

---

4/86

6

---

1750.1 REV-4 CHG-2  
Appendix 6

- 
- documents in a Department office or organization. Such procedures must provide for tracing the movement of classified information, limited dissemination, prompt retrieval of documents, detection of the loss of information, and prevention of excessive production and reproduction of documents.
  2. Destruction of Classified Information - Classified documents will be destroyed when no longer needed in a manner to preclude recognition or reconstruction of the classified information. Classified documents will only be destroyed by the methods prescribed by Department security regulations.
  3. Marking Derivatively Classified Documents - A uniform system for marking derivatively classified documents is contained in Department security regulations. The basic purpose for applying markings to documents containing or revealing classified information is to communicate to a recipient the degree of protection required and to facilitate extracting, paraphrasing, upgrading, downgrading, and declassification actions. It is important that all employees who derivatively classify information utilize the uniform system, otherwise this basic purpose will not be realized.
  4. Storage of Classified Information :
    - a. Classified information will be stored under conditions that will provide adequate protection and prevent access by unauthorized persons. Whenever classified information is not under the personal control and observation of an authorized person, it will be guarded by cleared personnel having a need-to-know or stored in a locked security container. Only the security containers prescribed in Department security regulations will be used for the storage of classified information.

- b. Combinations used for storage of classified information will be changed upon request to the Assistant Director for Security. Under no circumstances may these combinations be changed by a commercial locksmith without prior approval of the Assistant Director for Security. Combinations will be changed:

- (1) When a container is placed in use;
- (2) When an individual knowing the combination no longer requires access to the container;
- (3) When the combination has been subjected to possible compromise;
- (4) At least once every 12 months; or
- (5) When a container is taken out of service. Built in combination locks will be reset to the standard combination 50-25-50 (10-20-30 for padlocks) prior to removal from the office space.

---

1750.1 REV-4 CHG-2  
Appendix 6

- 
- c. The combination of a lock used for the storage of classified information will be afforded protection equal to that given the highest level of the classified information stored therein. Combinations will be memorized or recorded and stored in an approved security container; not on calendars, in desk drawers, in wallets, etc.
- d. Access to the combinations will be given only to those employees who are appropriately cleared and authorized access to the classified information stored in the container and must have it for the efficient performance of their duties.
5. Transmission of Classified Documents - This refers to any movement of classified information from one place to another. The classified information has to be in the custody of a cleared individual or an approved system. Approved methods for the transmission of TOP SECRET, SECRET and CONFIDENTIAL information are contained in Department security regulations. The regulations also prescribe procedures for the proper packaging and receipting of classified information for transmission. Classified documents will not, under any circumstances, be removed from the Department for reasons of personal convenience.
6. Production and Reproduction of Classified Information  
- Production means the initial typing or writing of letters, memoranda, and other documents containing classified information. Reproduction means the duplication of any classified information, in whole or in part.



- a. The Assistant Director for Security will be responsible for the reproduction of all classified documents in the Department and will obtain approval from the original classification authority prior to the reproduction of such classified information
  - b. Reproduced copies of classified documents will be subject to the same accountability and controls as the original documents.
- E. RESPONSIBILITIES - To further provide for the protection and safeguarding of classified information, the following responsibilities have been assigned:
- 1. Office Managers and Supervisors. The responsibility for safeguarding national security information rests upon each office manager and supervisor to the same degree that the office manager and supervisor are charged with functional responsibility for their office. While certain employees may be assigned specific security responsibilities, it is nevertheless the basic responsibility of the office manager and supervisor to ensure that national security information entrusted to their offices is handled and safeguarded according to the policies and procedures contained in Department security regulations. Any office manager and supervisor who handles or stores national security

---

4/86

8

---

1750.1 REV-4 CHG-2  
Appendix 6

- 
- information will appoint a custodian of classified files for their respective offices. They will also establish a system of security checks at the close of each working day to ensure that:
- a. All classified information has been returned, removed from desks and file trays, and stored in an approved security container.
  - b. All typewriter ribbons, floppy disks, carbon papers, handwritten notes and working papers which may contain classified information are stored, until destruction, in an approved security container.
  - c. Wastebaskets do not contain any classified information.
  - d. Security containers are checked to be sure they are locked. Form HUD 1443, Classified Container Locking Record, will be used to record information relating to the unlocking, locking, and checking of security containers.
  - e. All windows and doors, where appropriate, are locked.
- 2. Logging Control Officer (LCO). As a minimum, each LCO, in addition to his/her regularly assigned duties, will accomplish the following tasks:

- a. Verify the security clearance status of custodians of classified files and other recipients authorized to receive classified information.
- b. Receive unopened, all incoming accountable communications, including First Class mail containing classified information.
- c. Inspect sealed envelopes or similar wrappings containing classified information for any evidence of tampering or damage.
- d. Match the actual contents of an incoming package of classified material with the enclosed receipt.
- e. Sign and return to the sender, receipts enclosed in classified transmittals.
- f. Locate classified documents for return to the originating office when required.
- g. Maintain appropriate Departmental security accountability records.
- h. Take prompt action on any downgrading and/or declassification notices received.
- i. Assure that the appropriate secure method of transmission is selected, and that the material is properly prepared for transmission.

---

1750.1 REV-4 CHG-2

#### Appendix 6

- 
- j. Arrange for the destruction of any unneeded classified documents.
  - k. Insure that offices who merely coordinate, sign, or route classified documents that are prepared and controlled by another office, do not keep copies of the document for the sole purpose of control or a possible later need.
3. Custodians of Classified Files. Where it is considered an absolute necessity that classified documents be stored in offices other than the LCP, custodians of classified files will be appointed to carry out the required duties. Employees appointed as custodians of classified files will, as a minimum, in addition to his/her regular assigned duties, be responsible for the following duties:
- a. Provide protection for all classified information entrusted to his/her care.
  - b. Lock classified information in approved security containers

whenever it is not in use or under direct supervision of an authorized person.

- c. Verify the clearance status and need-to-know of office personnel or other recipients authorized to review classified information.
  - d. Return all classified material marked for destruction to the LCP.
4. Employees. Each employee who may have access to national security information is responsible for the protection of that information, no matter how it was received. Each employee who handles national security information will be familiar with and adhere to the provisions of Department security regulations. Employees are also responsible for reporting the loss, or temporary loss, or control or possession of national security information to their supervisor.

#### F. SECURITY TIPS

- 1. Account for all classified information that may be furnished to you.
- 2. Protect proprietary, sensitive, or classified information from loss or compromise, regardless of the manner in which you received it, and report immediately any act that has or might result in such loss or compromise. This responsibility is yours whether the act or omission is your own or that of another person.
- 3. Classified information should not be hand carried to an outlying HUD office or non-HUD organization unless time limitations do not permit the use of U. S. Registered Mail. When this need does exist, the classified material must be processed through the LCP, and approval to act as a courier must be obtained from the appropriate manager or supervisor.
- 4. Remember not to take classified information home.

- 
- 5. Do not discuss classified information within an office or conference room if your conversation may be overheard by unauthorized persons such as uncleared visitors or employees without a need-to-know.
  - 6. Never discuss classified information with unauthorized persons, including your family or friends.
  - 7. Do not discuss classified information over an unsecured telephone

at anytime, anywhere.

8. Never put classified material in wastebaskets.
9. Do not comment on published news articles concerning information that you know to be classified. Publication by a news media does not constitute proper authority for declassification and is often the product of astute guessing. You should not lend credence to such reports by agreeing or disagreeing with them until they have been evaluated officially.
10. Whenever leaving your office, even for a short time, lock up classified information in an approved security container unless the information is under the physical control of a cleared person with an authorized need-to-know.
11. Do not keep a written record of safe combinations on desk blotters, calendar pads, etc., as they must be committed to memory.
12. Lock up in approved security containers all shorthand notes, preliminary drafts, carbon paper, typewriter ribbons, and other material of a similar nature which was used for the generation of classified information in the course of a work day.
13. Double check and test all drawers of each container used for the storage of classified material at the close of business each day to assure that they are properly secured. REMEMBER to turn the dial of each combination lock at least four times to the right after the container has been secured.

#### G. ADMINISTRATIVE AND CRIMINAL SANCTIONS

1. HUD employees may be subject to administrative sanctions which could include reprimand, termination of security access authorization, suspension from or termination of employment, as appropriate, if they:
  - a. Refuse to cooperate in the conduct of a preliminary inquiry or formal investigation.
  - b. Knowingly, willfully, or negligently cause or have knowledge of an unauthorized disclosure of proprietary, sensitive, or classified information.

#### Appendix 6

- 
2. In addition to the administrative sanctions stated above, criminal sanctions may also be imposed. HUD employees may be subject to criminal sanctions as described under Section 641, 793, 794, 798, and 952 of Title 18, U.S.C., Section 783(b) of Title 50 U.S.C., or other appropriate statutes for being adjudged responsible for the unauthorized disclosure of national security

information. Such sanctions may include penalties of up to \$10,000 fine or imprisonment for ten years, or both. Also, penalties for engaging in espionage activities could include imprisonment for any term of years, or for life.

H. EXCERPTS FROM TITLE 18, UNITED STATES CODE

1. Section 641 - Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Who receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted :

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of \$100, he shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

2. Section 793 - Gathering, transmitting, or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal, station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or otherwise on behalf of the United States, or any department or agency thereof, or with any person on

designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

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

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

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

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

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

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

(h) If two or ore persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

3. Section 794 - Gathering or delivering defense information to aid foreign government

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

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

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

4. Section 798 - Disclosure of classified information

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

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

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

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

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

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

(b) as used in subsection (a) of this section :

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

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



meaning any person or persons acting or purporting to act for or on behalf of any factions, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States,

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

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

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

5. Section 952 - Diplomatic codes and correspondence

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

6. Excerpt from Title 50, United States Code, Section 783(b)  
- Communication of classified information by Government officer or employee

a. It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of Section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such

---

department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

---