abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

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

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

18 § 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.

§ 798. Disclosure of Classified Information [1]

(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 purposes; 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 processes—

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

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

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

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

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

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

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

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

§ 783. Offenses—(a) Conspiracy or attempt to establish totalitarian dictatorship

It shall be unlawful for any person knowingly to combine, conspire, or agree with any other person to perform any act which would substantially contribute to the establishment within the United States of a totalitarian dictatorship, as defined in paragraph (15) of section 782 of this title, the direction and control of which is to be vested in, or exercised by or under the domination or control of, any foreign government, foreign organization, or foreign individual: *Provided, however*, That this subsection shall not apply to the proposal of a constitutional amendment.

Communication of classified information by Government officer or employee

(b) 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.

Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information

(c) It shall be unlawful for any agent or representative of any foreign government, or any officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

Penalties for violation

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

Limitation period

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

Membership as not violation per se

(f) Neither the holding of office nor membership in any Communist organization by any person shall constitute per se a violation of subsection (a) or subsection (c) of this section or of any other criminal statute. As amended Jan. 2, 1968, Pub.L. 90-237, § 3, 81 Stat. 765.

EXECUTIVE ORDER NO. 11652

Mar. 8, 1972, 37 F.R. 5209, as amended by Ex.Ord.No.11714, Apr. 24, 1973, 38 F.R. 10243; Ex.Ord.No.11862, June 11, 1975, 40 F.R. 25197

CLASSIFICATION AND DECLASSIFICATION OF NATIONAL SECURITY INFORMATION AND MATERIAL

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act [section 552 of Title 5, Government Organization and Employees] and in the current public information policies of the executive branch.

Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b) (1) of Title 5, United States Code [section 552(b) (1) of Title 5, Government Organization and Employees]. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

To ensure that such information and material is protected, but only to the extent and for such period as is necessary, this order identifies the information to be protected, prescribes classification, downgrading, declassification and safeguarding procedures to be followed, and establishes a monitoring system to ensure its effectiveness.

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, it is hereby ordered:

Section 1. Security Classification Categories. Official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of three categories, namely "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(A) *"Top Secret."* "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(B) *"Secret."* "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

(C) *"Confidential."* "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

Sec. 2. Authority to Classify. The authority to originally classify information or material under this order shall be restricted solely to those offices within the executive branch which are concerned with matters of national security, and shall be limited to the minimum number absolutely required for efficient administration. Except as the context may otherwise indicate, the term "Department"

as used in this order shall include agency or other governmental unit.

(A) The authority to originally classify information or material under this order as "Top Secret" shall be exercised only by such officials as the President may designate in writing and by:

(1) The heads of the Departments listed below;

(2) Such of their senior principal deputies and assistants as the heads of such Departments may designate in writing; and

(3) Such heads and senior principal deputies and assistants of major elements of such Departments, as the heads of such Departments may designate in writing.

Such offices in the Executive Office of the President as the President may designate in writing
Central Intelligence Agency
Energy Research and Development Administration
Department of State
Department of the Treasury
Department of Defense
Department of the Army
Department of the Navy
Department of the Air Force
United States Arms Control and Disarmament Agency
Department of Justice
National Aeronautics and Space Administration
Agency for International Development

(B) The authority to originally classify information or material under this order as "Secret" shall be exercised only by:

(1) Officials who have "Top Secret" classification authority;

(2) Such subordinates as officials with "Top Secret" classification authority under (A) (1) and (2) above may designate in writing; and

(3) The heads of the following named Departments and such senior principal deputies or assistants as they may designate in writing.

Department of Transportation
Federal Communications Commission
Export-Import Bank of the United States
Department of Commerce
United States Civil Service Commission
United States Information Agency
General Services Administration
Department of Health, Education, and Welfare
Civil Aeronautics Board
Federal Maritime Commission
Federal Power Commission
National Science Foundation
Overseas Private Investment Corporation
Nuclear Regulatory Commission

(C) The authority to originally classify information or material under this order as "Confidential" may be exercised by officials who have "Top Secret" or "Secret" classification authority and such officials as they may designate in writing.

(D) Any Department not referred to herein and any Department or unit established hereafter shall not have authority to originally classify information or material under this order, unless specifically authorized hereafter by an Executive order.

Sec. 3. Authority to Downgrade and Declassify. The authority to downgrade and declassify national security information or material shall be exercised as follows:

(A) Information or material may be downgraded or declassified by the official authorizing the original classification, by a successor in capacity or by a supervisory official of either.

(B) Downgrading and declassification authority may also be exercised by an official specifically authorized under regulations issued by the head of the Department listed in Sections 2(A) or (B) hereof.

(C) In the case of classified information or material officially transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this order including downgrading and declassification.

(D) In the case of classified information or material not officially transferred within (C) above, but originated in a Department which has since ceased to exist, each Department in possession shall be deemed to be the originating Department for all purposes under this order. Such information or material may be downgraded and declassified by the Department in possession after consulting with any other Departments having an interest in the subject matter.

(E) Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the Departments.

(F) Classified information or material with special markings, as described in Section 8, shall be downgraded and declassified as required by law and governing regulations.

Sec. 4. Classification. Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and over-classification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order:

(A) *Documents in General.* Each classified document shall show on its face its classification and whether it is subject to or exempt from the General Declassification Schedule. It shall also show the office of origin, the date of preparation and classification and, to the extent practicable, be so marked as to indicate which portions are classified, at what level, and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

(B) *Identification of Classifying Authority.* Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case, material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification. Where the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required.

(C) *Information or Material Furnished by a Foreign Government or Internation-*

al Organization. Classified information or material furnished to the United States by a foreign government or international organization shall either retain its original classification or be assigned a United States classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(D) *Classification Responsibilities.* A holder of classified information or material shall observe and respect the classification assigned by the originator. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under this order, he shall so inform the originator who shall thereupon re-examine the classification.

Sec. 5. Declassification and Downgrading. Classified information and material, unless declassified earlier by the original classifying authority, shall be declassified and downgraded in accordance with the following rules:

(A) *General Declassification Schedule.*

(1) *"Top Secret."* Information or material originally classified "Top Secret" shall become automatically downgraded to "Secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "Confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

(2) *"Secret."* Information and material originally classified "Secret" shall become automatically downgraded to "Confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(3) *"Confidential."* Information and material originally classified "Confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(B) *Exemptions from General Declassification Schedule.* Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the General Declassification Schedule. An official authorized to originally classify information or material "Top Secret" may exempt from the General Declassification Schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

(1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

(4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

(C) *Mandatory Review of Exempted Material.* All classified information and material originated after the effective date of this order which is exempted under (B) above from the General Declassification Schedule shall be subject to a classification review by the originating Department at any time after the expiration of ten years from the date of origin provided:

(1) A Department or member of the public requests a review;

(2) The request describes the record with sufficient particularity to enable the Department to identify it; and

(3) The record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption under (B) above shall be declassified. Information or material continuing to qualify under (B) shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(D) *Applicability of the General Declassification Schedule to Previously Classified Material.* Information or material classified before the effective date of this order and which is assigned to Group 4 under Executive Order No. 10501, as amended by Executive Order No. 10964, shall be subject to the General Declassification Schedule. All other information or material classified before the effective date of this order, whether or not assigned to Groups 1, 2, or 3 of Executive Order No. 10501, as amended, shall be excluded from the General Declassification Schedule. However, at any time after the expiration of ten years from the date of origin it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to classified information and material created after the effective date of this order as set forth in (B) and (C) above.

(E) *Declassification of Classified Information or Material After Thirty Years.* All classified information or material which is thirty years old or more, whether originating before or after the effective date of this order, shall be declassified under the following conditions:

(1) All information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of thirty full calendar years after the date of its original classification except for such specifically identified information or material which the head of the originating Department personally determines in writing at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such case, the head of the Department shall also specify the period of continued classification.

(2) All information and material classified before the effective date of this order and more than thirty years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was originated. In his review, the Archivist will separate and keep protected only such information or material as is specifically identified by the head of the Department in accordance with (E)(1) above. In such case, the head of the Department shall also specify the period of continued classification.

(F) *Departments Which Do Not Have Authority For Original Classification.* The provisions of this section relating to the declassification of national security information or material shall apply to Departments which, under the terms of this order, do not have current authority to originally classify information or material, but which formerly had such authority under previous Executive orders.

Sec. 6. **Policy Directives on Access, Marking, Safekeeping, Accountability, Transmission, Disposition and Destruction of Classified Information and Material.** The President acting through the National Security Council shall issue directives which shall be binding on all Departments to protect classified information from loss or compromise. Such directives shall conform to the following policies:

(A) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.

(B) All classified information and material shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.

(C) Classified information and material shall be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons.

(D) All classified information and material disseminated outside the executive branch under Executive Order No. 10865 [set out as a note under this section] or otherwise shall be properly protected.

(E) Appropriate accountability records for classified information shall be established and maintained and such information and material shall be protected adequately during all transmissions.

(F) Classified information and material no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in Chapter 33 of Title 44 of the United States Code [sections 3301-3314 of Title 44, Public Printing and Documents] and other applicable statutes.

(G) Classified information or material shall be reviewed on a systematic basis for the purpose of accomplishing downgrading, declassification, transfer, retirement and destruction at the earliest practicable date.

Sec. 7. **Implementation and Review Responsibilities.** (A) The National Security Council shall monitor the implementation of this order. To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of a Chairman designated by the President, the Archivist of the United States, and representatives of the Departments of State, Defense and Justice, the Energy Research and Development Administration, the Central Intelligence Agency and the National Security Council Staff. Representatives of other Departments in the executive branch may be invited to meet with the Committee on matters of particular interest to those Departments. This Committee shall meet regularly and on a continuing basis shall review and take action to ensure compliance with this order, and in particular:

(1) The Committee shall oversee Department actions to ensure compliance with the provisions of this order and implementing directives issued by the President through the National Security Council.

(2) The Committee shall, subject to procedures to be established by it, receive, consider and take action on suggestions and complaints from persons within or without the government with respect to the administration of this order, and in consultation with the affected Department or Departments assure that appropriate action is taken on such suggestions and complaints.

(3) Upon request of the Committee Chairman, any Department shall furnish to the Committee any particular information or material needed by the Committee in carrying out its functions.

(B) To promote the basic purposes of this order, the head of each Department originating or handling classified information or material shall:

(1) Prior to the effective date of this order submit to the Interagency Classification Review Committee for approval a copy of the regulations it proposes to adopt pursuant to this order.

(2) Designate a senior member of his staff who shall ensure effective compliance with and implementation of this order and shall also chair a Departmental committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of this order.

(3) Undertake an initial program to familiarize the employees of his Department with the provisions of this order. He shall also establish and maintain active training and orientation programs for employees concerned with classified information or material. Such programs shall include, as a minimum, the briefing of new employees and periodic reorientation during employment to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of this order. Additionally, upon termination of employment or contemplated temporary separation for a sixty-day period or more, employees shall be debriefed and each reminded of the provisions of the Criminal Code and other applicable provisions of law relating to penalties for unauthorized disclosure.

(C) The Attorney General, upon request of the head of a Department, his duly designated representative, or the Chairman of the above described Committee, shall personally or through authorized representatives of the Department of Justice render an interpretation of this order with respect to any question arising in the course of its administration.

Sec. 8. **Material Covered by the Atomic Energy Act.** Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended [section 2011 et seq. of Title 42, The Public Health and Welfare]. "Restricted Data," and material designated as "Formerly Restricted Data," shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Energy Research and Development Administration.

Sec. 9. **Special Departmental Arrangements.** The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.

Sec. 10. **Exceptional Cases.** In an exceptional case when a person or Department not authorized to classify information originates information which is believed to require classification, such person or Department shall protect that information in the manner prescribed by

this order. Such persons or Department shall transmit the information forthwith, under appropriate safeguards, to the Department having primary interest in the subject matter with a request that a determination be made as to classification.

Sec. 11. Declassification of Presidential Papers. The Archivist of the United States shall have authority to review and declassify information and material which has been classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a Presidential Library. Such declassification shall only be undertaken in accord with: (i) the terms of the donor's deed of gift, (ii) consultations with the Departments having a primary subject-matter interest, and (iii) the provisions of Section 5.

Sec. 12. Historical Research and Access by Former Government Officials. The requirement in Section 6(A) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policy-making positions to which they were appointed by the President; *Provided*, however, that in each case the head of the originating Department shall:

(i) determine that access is clearly consistent with the interests of national security; and

(ii) take appropriate steps to assure that classified information or material is not published or otherwise compromised. Access granted a person by reason of his having previously occupied a policy-making position shall be limited to those papers which the former official originated, reviewed, signed or received while in public office.

Sec. 13. Administrative and Judicial Action. (A) Any officer or employee of the United States who unnecessarily classifies or overclassifies information or material shall be notified that his actions are in violation of the terms of this order or of a directive of the President issued through the National Security Council. Repeated abuse of the classification process shall be grounds for an administrative reprimand. In any case where the Departmental committee or the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred, it shall make a report to the head of the Department concerned in order that corrective steps may be taken.

(B) The head of each Department is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, Departments will refer any such case promptly to the Department of Justice.

Sec. 14. Revocation of Executive Order No. 10501. Executive Order No. 10501 of November 5, 1953, as amended by Executive Orders No. 10816 of May 8, 1959, No. 10901 of January 11, 1961, No. 10964 of September 20, 1961, No. 10985 of January 15, 1962, No. 11097 of March 6, 1963 and by Section 1(a) of No. 11382 of November 28, 1967, is superseded as of the effective date of this order.

Sec. 15. Effective date. This order shall become effective on June 1, 1972.

RICHARD NIXON

NATIONAL SECURITY COUNCIL, DIRECTIVE OF MAY 17, 1972

May 17, 1972, 37 F.R. 10053

CLASSIFICATION, DOWNGRADING, DECLASSIFICATION AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION

The President has directed that Executive Order 11652, "Classification and Declassification of National Security Information and Material," approved March 8, 1972 (37 F.R. 5209, March 10, 1972) [set out as a note under this section] be implemented in accordance with the following:

I AUTHORITY TO CLASSIFY

A. Personal and Non-delegable. Classification authority may be exercised only by those officials who are designated by, or in writing pursuant to, Section 2 of Executive Order 11652 (hereinafter the "Order") [set out as a note under this section]. Such officials may classify information or material only at the level authorized or below. This authority vests only to the official designated under the Order, and may not be delegated.

B. Observance of Classification. Whenever information or material classified by an official designated under A above is incorporated in another document or other material by any person other than the classifier, the previously assigned security classification category shall be reflected thereon together with the identity of the classifier.

C. Identification of Classifier. The person at the highest level authorizing the classification must be identified on the face of the information or material classified, unless the identity of such person might disclose sensitive intelligence information. In the latter instance the Department shall establish some other record by which the classifier can readily be identified.

D. Record Requirement. Each Department listed in Section 2(A) of the Order shall maintain a listing by name of the officials who have been designated in writing to have Top Secret classification authority. Each Department listed in Section 2(A) and (B) of the Order shall also maintain separate listings by name of the persons designated in writing to have Secret authority and persons designated in writing to have Confidential authority. In cases where listing of the names of officials having classification authority might disclose sensitive intelligence information, the Department shall establish some other record by which such officials can readily be identified. The foregoing listings and records shall be compiled beginning July 1, 1972 and updated at least on a quarterly basis.

E. Resolution of Doubts. If the classifier has any substantial doubt as to which security classification category is appropriate, or as to whether the material should be classified at all, he should designate the less restrictive treatment.

II DOWNGRADING AND DECLASSIFICATION

A. General Declassification Schedule and Exemptions. Classified information

and material shall be classified as soon as there are no longer any grounds for continued classification within the classification category definitions set forth in Section 1 of the Order. At the time of origination the classifier shall, whenever possible, clearly mark on the information or material a specific date or event upon which downgrading or declassification shall occur. Such dates or events shall be as early as is permissible without causing damage to the national security as defined in Section 1 of the Order. Whenever earlier dates or events cannot be determined, the General Declassification Schedule set forth in Section 5(A) of the Order shall apply. If the information or material is exempted under Section 5(B) of the Order from the General Declassification Schedule, the classifier shall clearly mark the material to show that it is exempt and indicate the applicable exemption category. Unless impossible, the exempted information or material shall be assigned and clearly marked by the classifier with a specific date or event upon which declassification shall occur. Downgrading and declassification dates or events established in accordance with the foregoing, whether scheduled or non-scheduled, shall to the extent possible be carried forward and applied whenever the classified information or material is incorporated in other documents or material.

B. Extracts and Compilations. When classified information or material from more than one source is incorporated into a new document or other material, the document or other material shall be classified, downgraded or declassified in accordance with the provisions of the Order and Directives thereunder applicable to the information requiring the greatest protection.

C. Material Not Officially Transferred. When a Department holding classified information or material under the circumstances described in Section 3(D) of the Order notifies another Department of its intention to downgrade or declassify, it shall allow the notified Department 30 days in which to express its objections before taking action.

D. Declassification of Material 30 Years Old. The head of each Department shall assign experienced personnel to assist the Archivist of the United States in the exercise of his responsibility under Section 5(E) of the Order to systematically review for declassification all materials classified before June 1, 1972 and more than 30 years old. Such personnel will: (1) provide guidance and assistance to archival employees in identifying and separating those materials originated in their Departments which are deemed to require continued classification; and (2) develop a list for submission to the head of the Department which identifies the materials so separated, with recommendations concerning continued classification. The head of the originating Department will then make the determination required under Section 5(E) of the Order and cause a list to be created which identifies the documentation included in the determination, indicates the reason for continued classification and specifies the date on which such material shall be declassified.

E. Notification of Expedited Downgrading or Declassification. When classified information or material is downgraded or declassified in a manner other than originally specified, whether scheduled or exempted, the classifier shall, to the extent practicable, promptly notify all addressees to whom the information or material was originally officially transmitted. In turn, the addressees shall notify any other known recipient of the classified information or material.

III REVIEW OF CLASSIFIED MATERIAL FOR DECLASSIFICATION PURPOSES

A. Systematic Reviews. All information and material classified after the effective date of the Order and determined in accordance with Chapter 21, 44 U.S.C (52 Stat. 1281) [section 2101 et seq. of Title 44, Public Printing and Documents] to be of sufficient historical or other value to warrant preservation shall be systematically reviewed on a timely basis by each Department for the purpose of making such information and material publicly available in accordance with the determination regarding declassification made by the classifier under Section 5 of the Order. During each calendar year each Department shall segregate to the maximum extent possible all such information and material warranting preservation and becoming declassified at or prior to the end of such year. Promptly after the end of such year the Department responsible, or the Archives of the United States if transferred thereto, shall make the declassified information and material available to the public to the extent permitted by law.

B. Review for Declassification of Classified Material Over 10 Years Old. Each Department shall designate in its implementing regulations an office to which members of the public or Departments may direct requests for mandatory review for declassification under Section 5(C) and (D) of the Order. This office shall in turn assign the request to the appropriate office for action. In addition, this office or the office which has been assigned action shall immediately acknowledge receipt of the request in writing. If the request requires the rendering of services for which fair and equitable fees should be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 1952, 65 Stat. 290, 31 U.S.C. 483a [section 483a of Title 31, Money and Finance] the requester shall be so notified. The office which has been assigned action shall thereafter make a determination within 30 days of receipt or shall explain the reasons why further time is necessary. If at the end of 60 days from receipt of the request for review no determination has been made, the requester may apply to the Departmental Committee established by Section 7(B) of the Order for a determination. Should the office assigned action on a request for review determine that under the criteria set forth in Section 5(B) of the Order continued classification is required, the requester shall promptly be notified, and whenever possible, provided with a brief statement as to why the requested information or material cannot be declassified. The requester may appeal any such determination to the Departmental Committee and the notice of determination shall advise him of this right.

C. Departmental Committee Review for Declassification. The Departmental Committee shall establish procedures to review and act within 30 days upon all applications and appeals regarding requests for declassification. The Department head, acting through the Departmental Committee shall be authorized to overrule previous determinations in whole or in part when, in its judgment, continued protection is no longer required. If the Departmental Committee determines that continued classification is required under the criteria of Section 5(B) of the Order it shall promptly so notify the requester and advise him that he may appeal the

denial to the Interagency Classification Review Committee.

D. Review of Classified Material Over 30 Years Old. A request by a member of the public or by a Department under Section 5(C) or (D) of the Order to review for declassification documents more than 30 years old shall be referred directly to the Archivist of the United States, and he shall have the requested documents reviewed for declassification in accordance with Part II.D. hereof. If the information or material requested has not been transferred to the General Services Administration for accession into the Archives, the Archivist shall, together with the head of the Department having custody, have the requested documents reviewed for declassification. Classification shall be continued in either case only where the head of the Department concerned makes at that time the personal determination required by Section 5(E)(1) of the Order. The Archivist shall promptly notify the requester of such determination and of his right to appeal the denial to the Interagency Classification Review Committee.

E. Burden of Proof for Administrative Determinations. For purposes of administrative determinations under B., C., or D. above, the burden of proof is on the originating Department to show that continued classification is warranted within the terms of the Order.

F. Availability of Declassified Material. Upon a determination under B., C., or D. above that the requested material no longer warrants classification it shall be declassified and made promptly available to the requester, if not otherwise exempt from disclosure under Section 552(b) of Title 5 U.S.C. [section 552(b) of Title 5, Government Organization and Employees] (Freedom of Information Act) or other provision of law.

G. Classification Review Requests. As required by Section 5(C) of the Order, a request for classification review must describe the document with sufficient particularity to enable the Department to identify it and obtain it with a reasonable amount of effort. Whenever a request is deficient in its description of the record sought, the requester should be asked to provide additional identifying information whenever possible. Before denying a request on the ground that it is unduly burdensome, the requester should be asked to limit his request to records that are reasonably obtainable. If, none-the-less the requester does not describe the records sought with sufficient particularity, or the record requested cannot be obtained with a reasonable amount of effort, the requester shall be notified of the reasons why no action will be taken and of his right to appeal such decision.

IV MARKING REQUIREMENTS

A. When Document or Other Material is Prepared. At the time of origination, each document or other material containing classified information shall be marked with its assigned security classification and whether it is subject to or exempt from the General Declassification Schedule.

(1) For marking documents which are subject to the General Declassification Schedule, the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED BY

SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS AND DECLASSIFIED ON DEC. 31 (insert year)

(2) For marking documents which are to be automatically declassified on a given event or date earlier than the General Declassification Schedule the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED BY

AUTOMATICALLY DECLASSIFIED ON (effective date or event)

(3) For marking documents which are exempt from the General Declassification Schedule the following stamp shall be used:

(TOP SECRET, SECRET OR CONFIDENTIAL) CLASSIFIED BY

EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 EXEMPTION CATEGORY (§ 5B(1), (2), (3), OR (4)) AUTOMATICALLY DECLASSIFIED ON (effective date or event, if any)

Should the classifier inadvertently fail to mark a document with one of the foregoing stamps the document shall be deemed to be subject to the General Declassification Schedule. The person who signs or finally approves a document or other material containing classified information shall be deemed to be the classifier. If the classifier is other than such person he shall be identified on the stamp as indicated.

The "Restricted Data" and "Formerly Restricted Data" stamps (H. below) are, in themselves, evidence of exemption from the General Declassification Schedule.

B. Overall and Page Marking of Documents. The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, on the back page and on the outside of the back cover (if any). To the extent practicable each interior page of a document which is not permanently bound shall be conspicuously marked or stamped at the top and bottom according to its own content, including the designation "Unclassified" when appropriate.

C. Paragraph Marking. Whenever a classified document contains either more than one security classification category or unclassified information, each section, part or paragraph should be marked to the extent practicable to show its classification category or that it is unclassified.

D. Material Other Than Documents. If classified material cannot be marked, written notification of the information otherwise required in markings shall accompany such material.

E. Transmittal Documents. A transmittal document shall carry on it a prominent notation as to the highest classification of the information which is carried with it, and a legend showing the classification, if any, of the transmittal document standing alone.

F. Wholly Unclassified Material Not Usually Marked. Normally, unclassified material shall not be marked or stamped

"Unclassified" unless the purpose of the marking is to indicate that a decision has been made not to classify it.

G. Downgrading, Declassification and Upgrading Markings. Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information or material it shall be promptly and conspicuously marked to indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. In addition, all earlier classification markings shall be cancelled, if practicable, but in any event on the first page.

(1) Limited Use of Posted Notice for Large Quantities of Material. When the volume of information or material is such that prompt remarking of each classified item could not be accomplished without unduly interfering with operations, the custodian may attach downgrading, declassification or upgrading notices to the storage unit in lieu of the remarking otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, the identity of the person taking the action and the storage units to which it applies. When individual documents or other materials are withdrawn from such storage units they shall be promptly remarked in accordance with the change, or if the documents have been declassified, the old markings shall be cancelled.

(2) Transfer of Stored Quantities Covered by Posted Notice. When information or material subject to a posted downgrading, upgrading or declassification notice are withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or other materials is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

H. Additional Warning Notices. In addition to the foregoing marking requirements, warning notices shall be prominently displayed on classified documents or materials as prescribed below. When display of these warning notices on the documents or other materials is not feasible, the warnings shall be included in the written notification of the assigned classification.

(1) Restricted Data. For classified information or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended [section 2011 et seq. of Title 42, The Public Health and Welfare]:

"RESTRICTED DATA"

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Its dissemination or disclosure to any unauthorized person is prohibited.

(2) Formerly Restricted Data. For classified information or material containing solely Formerly Restricted Data, as defined in Section 142.d., Atomic Energy Act of 1954, as amended [section 2162(d), of Title 42, The Public Health and Welfare]:

"FORMERLY RESTRICTED DATA"

Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act, 1954.

(3) Information Other Than Restricted Data or Formerly Restricted Data. For classified information or material furnished to persons outside the Executive Branch of Government other than as described in (1) and (2) above:

"NATIONAL SECURITY INFORMATION"

Unauthorized Disclosure Subject to Criminal Sanctions.

(4) Sensitive Intelligence Information. For classified information or material relating to sensitive intelligence sources and methods, the following warning notice shall be used, in addition to and in conjunction with those prescribed in (1), (2), or (3), above, as appropriate:

"WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED"

V PROTECTION AND TRANSMISSION OF CLASSIFIED INFORMATION

A. General. Classified information or material may be used, held, or stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. Whenever such information or material is not under the personal supervision of an authorized person, the methods set forth in Appendix A hereto shall be used to protect it. Whenever such information or material is transmitted outside the originating Department the requirements of Appendix B hereto shall be observed.

B. Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to a designated official of his Department or organization. In turn, the originating Department and any other interested Department shall be notified about the loss or possible compromise in order that a damage assessment may be conducted. An immediate inquiry shall be initiated by the Department in which the loss or compromise occurred for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action.

VI ACCESS AND ACCOUNTABILITY

A. General Access Requirements. Except as provided in B. and C. below, access to classified information shall be granted in accordance with the following:

(1) Determination of Trustworthiness. No person shall be given access to classified information or material unless a favorable determination has been made as to his trustworthiness. The determination of eligibility, referred to as a security clearance, shall be based on such investigations as the Department may require in accordance with the standards and criteria of E.O. 10450 [set out as a note under section 7311 of Title 5, Government Organization and Employees] and E.O. 10865 [set out as a note under this section] as appropriate.

(2) Determination of Need-to-Know. 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 official duties or contractual obligations. The determination of that need shall be made by officials having responsibility for the classified information or material.

(3) Administrative Withdrawal of Security Clearance. Each Department shall make provision for administratively withdrawing the security clearance of any person who no longer requires access to classified information or material in connection with the performance of his official duties or contractural obligations. Likewise, when a person no longer needs

access to a particular security classification category, the security clearance shall be adjusted to the classification category still required for the performance of his duties and obligations. In both instances, such action shall be without prejudice to the person's eligibility for a security clearance should the need again arise.

B. Access by Historical Researchers. Persons outside the Executive Branch engaged in historical research projects may be authorized access to classified information or material provided that the head of the originating Department determines that:

(1) The project and access sought conform to the requirements of Section 12 of the Order.

(2) The information or material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort.

(3) The historical researcher agrees to safeguard the information or material in a manner consistent with the Order and Directives thereunder.

(4) The historical researcher agrees to authorize a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein.

An authorization for access shall be valid for the period required but no longer than two years from the date of issuance unless renewed under regulations of the originating Department.

C. Access by Former Presidential Appointees. Persons who previously occupied policy making positions to which they were appointed by the President, other than those referred to in Section 11 of the Order, may be authorized access to classified information or material which they originated, reviewed, signed or received while in public office. Upon the request of any such former official, such information and material as he may identify shall be reviewed for declassification in accordance with the provisions of Section 5 of the Order.

D. Consent of Originating Department to Dissemination by Recipient. Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403 [section 403 of this title], classified information or material originating in one Department shall not be disseminated outside any other Department to which it has been made available without the consent of the originating Department.

E. Dissemination of Sensitive Intelligence Information. Information or material bearing the notation "WARNING NOTICE—SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating Department and an assessment by the senior intelligence official in the disseminating Department as to the potential risk to the national security and to the intelligence sources and methods involved.

F. Restraint on Special Access Requirements. The establishment of special rules limiting access to, distribution and protection of classified information and material under Section 9 of the Order requires the specific prior approval of the head of a Department or his designee.

G. Accountability Procedures. Each Department shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified information or material. Particularly stringent controls shall be placed on information and material classified Top Secret.

(1) Top Secret Control Officers. Top Secret Control Officers shall be designated, as required, to receive, maintain current accountability records of, and dispatch Top Secret material.

(2) Physical Inventory. A physical inventory of all Top Secret material shall be made at least annually. As an exception, repositories storing large volumes of classified material, shall develop inventory lists or other finding aids.

(3) Current Accountability. Top Secret and Secret information and material shall be subject to such controls including current accountability records as the head of the Department may prescribe.

(4) Restraint on Reproduction. Documents or portions of documents containing Top Secret information shall not be reproduced without the consent of the originating office. All other classified material shall be reproduced sparingly and any stated prohibition against reproduction shall be strictly adhered to.

(5) Restraint on Number of Copies. The number of copies of documents containing classified information shall be kept to a minimum to decrease the risk of compromise and reduce storage costs.

VII Data Index System

Each Department originating classified information or material shall undertake to establish a data index system for Top Secret, Secret and Confidential information in selected categories approved by the Interagency Classification Review Committee as having sufficient historical or other value appropriate for preservation. The index system shall contain the following data for each document indexed: (a) Identity of classifier, (b) Department of origin, (c) Addressees, (d) Date of classification, (e) Subject/Area, (f) Classification category and whether subject to or exempt from the General Declassification Schedule, (g) If exempt, which exemption category is applicable, (h) Date or event set for declassification, and (i) File designation. Information and material shall be indexed into the system at the earliest practicable date during the course of the calendar year in which it is produced and classified, or in any event no later than March 31st of the succeeding year. Each Department shall undertake to establish such a data index system no later than July 1, 1973, which shall index the selected categories of information and material produced and classified after December 31, 1972.

VIII Combat Operations

The provisions of the Order and this Directive with regard to dissemination, transmission, or safekeeping of classified information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

IX Interagency Classification Review Committee

A. Composition of Interagency Committee. In accordance with Section 7 of the Order, an Interagency Classification Review Committee is established to assist the National Security Council in monitoring implementation of the Order. Its membership is comprised of senior representatives of the Departments of State, Defense, and Justice, the Atomic Energy Commission, the Central Intelligence Agency, the National Security Council staff, and a Chairman designated by the President.

B. Meetings and Staff. The Interagency Committee shall meet regularly, but

no less frequently than on a monthly basis, and take such actions as are deemed necessary to insure uniform compliance with the Order and this Directive. The Chairman is authorized to appoint an Executive Director, and to maintain a permanent administrative staff.

C. Interagency Committee's Functions. The Interagency Committee shall carry out the duties assigned it by Section 7(A) of the Order. It shall place particular emphasis on overseeing compliance with and implementation of the Order and programs established thereunder by each Department. It shall seek to develop means to (a) prevent overclassification, (b) ensure prompt declassification in accord with the provision of the Order, (c) facilitate access to declassified material and (d) eliminate unauthorized disclosure of classified information.

D. Classification Complaints. Under such procedures as the Interagency Committee may prescribe, it shall consider and take action on complaints from persons within or without the government with respect to the general administration of the Order including appeals from denials by Departmental Committees or the Archivist of declassification requests.

X DEPARTMENTAL IMPLEMENTATION AND ENFORCEMENT

A. Action Programs. Those Departments listed in Section 2(A) and (B) of the Order shall insure that adequate personnel and funding are provided for the purpose of carrying out the Order and Directives thereunder.

B. Departmental Committee. All suggestions and complaints, including those regarding overclassification, failure to declassify, or delay in declassifying not otherwise resolved, shall be referred to the Departmental Committee for resolution. In addition, the Departmental Committee shall review all appeals of requests for records under Section 522 of Title 5 U.S.C. (Freedom of Information Act) [probably means section 552 of Title 5, Government Organization and Employees] when the proposed denial is based on their continued classification under the Order.

C. Regulations and Reports. Each Department shall submit its proposed implementing regulations of the Order and Directives thereunder to the Chairman of the Interagency Classification Review Committee for approval by the Committee. Upon approval such regulations shall be published in the FEDERAL REGISTER to the extent they affect the general public. Each Department shall also submit to the said Chairman (1) copies of the record lists required under Part I.D. hereof by July 1, 1972 and thereafter quarterly, (2) quarterly reports of Departmental Committee actions on classification review requests, classification abuses and unauthorized disclosures, and (3) provide progress reports on information accumulated in the data index system established under Part VII hereof and such other reports as said Chairman may find necessary for the Interagency Classification Review Committee to carry out its responsibilities.

D. Administrative Enforcement. The Departmental Committees shall have responsibility for recommending to the head of the respective Departments appropriate administrative action to correct abuse or violation of any provision of the Order or Directives thereunder, including notifications by warning letter, formal reprimand, and to the extent permitted by law, suspension without pay and removal. Upon receipt of such a recommendation the head of the Department concerned shall act promptly and advise the Departmental Committee of his action.

Publication and Effective Date: This Directive shall be published in the FEDERAL REGISTER and become effective June 1, 1972.

HENRY A. KISSINGER,
Assistant to the President for National Security Affairs.
May 17, 1972.

APPENDIX A
PROTECTION OF CLASSIFIED INFORMATION

A. Storage of Top Secret. Top Secret information and material shall be stored in a safe or safe-type steel file container having a built in three-position dial-type combination lock, vault, or vault-type room, or other storage facility which meets the standards for Top Secret established under the provisions of (C) below, and which minimizes the possibility of unauthorized access to, or the physical theft of, such information or material.

B. Storage of Secret or Confidential. Secret and Confidential material may be stored in a manner authorized for Top Secret information and material, or in a container or vault which meets the standards for Secret or Confidential, as the case may be, established under the provisions of (C) below.

C. Standards for Security Equipment. The General Services Administration shall, in coordination with Departments originating classified information or material, establish and publish uniform standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of all categories of classified information and material. Any Department may establish for use within such Department more stringent standards. Whenever new security equipment is procured, it shall be in conformance with the foregoing standards and specifications and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration.

D. Exception to Standards for Security Equipment. As an exception to (C) above, Secret and Confidential material may also be stored in a steel filing cabinet having a built in, three-position, dial-type combination lock; or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA approved changeable combination padlock.

E. Combinations. Combinations to security equipment and devices shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination is transferred from the office to which the equipment is assigned, whenever a combination has been subjected to possible compromise, and at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest category of classified information or material authorized for storage in the security equipment concerned.

F. Telecommunications Conversations. Classified information shall not be revealed in telecommunications conversations, except as may be authorized under Appendix B with respect to the transmission of classified information over approved communications circuits or systems.

G. Responsibilities of Custodians. Custodians of classified material shall be

responsible for providing protection and accountability for such material at all times and particularly for locking classified material in approved security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

APPENDIX B

TRANSMISSION OF CLASSIFIED INFORMATION

A. **Preparation and Receipting.** Classified information and material shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and address. The outer cover shall be sealed and addressed with no indication of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential material shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

B. **Transmission of Top Secret.** The transmission of Top Secret information and material shall be effected preferably by oral discussions in person between the officials concerned. Otherwise the transmission of Top Secret information and material shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, over authorized communications circuits in encrypted form or by other means authorized by the National Security Council; except that in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are approved by the Director, Federal Bureau of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating Department.

C. **Transmission of Secret.** The transmission of Secret material shall be effected in the following manner.

(1) **The Fifty States, District of Columbia, Puerto Rico.** Secret information and material may be transmitted within and between the forty-eight contiguous states and District of Columbia, or wholly within the State of Hawaii, the State of Alaska, or the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information and material, the United States Postal Service registered mail and protective services provided by the United States air or surface commercial carriers under such conditions as may be prescribed by the head of the Department concerned.

(2) **Other Areas, Vessels, Military Postal Services, Aircraft.** Secret information and material may be transmitted from or to or within areas other than those specified in (1) above, by one of the means established for Top Secret information and material, captains or masters of vessels of United States registry under contract to a Department of the Executive Branch, United States registered mail through Army, Navy or Air Force Postal Service facilities provided that material does not at any time pass out of United States citizen control and does not pass through a foreign postal system, and commercial aircraft under charter to the United States and military or other government aircraft.

(3) **Canadian Government Installations.** Secret information and material may be transmitted between United States Government or Canadian Government installations, or both, in the forty-eight contiguous states, Alaska, the District of Columbia and Canada by United States and Canadian registered mail with registered mail receipt.

(4) **Special Cases.** Each Department may authorize the use of the United States Postal Service registered mail outside the forty-eight contiguous states, the District of Columbia, the State of Hawaii, the State of Alaska, and the Commonwealth of Puerto Rico if warranted by security conditions and essential operational requirements provided that the material does not at any time pass out of United States Government and United States citizen control and does not pass through a foreign postal system.

D. **Transmittal of Confidential.** Confidential information and material shall be transmitted within the forty-eight contiguous states and the District of Columbia, or wholly within Alaska, Hawaii, the Commonwealth of Puerto Rico, or a United States possession, by one of the means established for higher classifications, or by certified or first class mail. Outside these areas, Confidential information and material shall be transmitted in the same manner as authorized for higher classifications.

E. **Alternative Transmission of Confidential.** Each Department having authority to classify information or material as "Confidential" may issue regulations authorizing alternative or additional methods for the transmission of material classified "Confidential" outside of the Department. In the case of material originated by another agency, the method of transmission must be at least as secure as the transmission procedures imposed by the originator.

F. **Transmission Within a Department.** Department regulations governing the preparation and transmission of classified information within a Department shall ensure a degree of security equivalent to that prescribed above for transmission outside the Department.