BASIC DOCUMENTS ON SECURITY CLASSIFICATION OF INFORMATION FOR NATIONAL SECURITY PURPOSES

WESTON BURNETT
Research Assistant
Foreign Affairs Division

July 15, 1971

TABLE OF CONTENTS

EXECUTIVE ORDER 10501 - SAFEGUARDING OFFICIAL INFORMATION

EXECUTIVE ORDER NO. 10501

Nov. 9, 1953, 18 F.R. 7049, as amended by Ex.Ord.No.10816, May 8, 1959, 24 F.R. 3777; Ex.Ord.No.10901, Jan. 11, 1961, 26 F.R. 217; Ex.Ord.No.10964, Sept. 20, 1961, 26 F.R. 8932; Ex.Ord.No.10985, Jan. 15, 1962, 27 F.R. 439; Ex.Ord.No.11097, Mar. 6, 1963, 28 F.R. 2225; Ex.Ord.No.11382, Nov. 28, 1967, 32 F.R. 16247

SAFEGUARDING OFFICIAL INFORMATION

Section 1. Classification Categories. Official information which requires protection in the interests of national defense shall be limited to three categories of classification, which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential. No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute. These categories are defined as follows:

(a) **Top Secret.** Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The Top Secret Classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence opera-

35

SOURCE:
U.S. Laws, Statutes, etc., United States Code Annotated. St. Paul, Minnesota; West Publishing Company, 1927 -- (Title 50, War and National Defense, Section 401, pages 35-45).

tions, or scientific or technological developments vital to the national defense.

(b) Secret. Except as may be expressly provided by statute, the use of the classification Secret shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

(c) Confidential. Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

Sec. 2. Limitation of authority to classify. The authority to classify defense information or material under this order shall be limited in the departments, agencies, and other units of the executive branch as hereinafter specified.

(a) In the following departments, agencies, and Governmental units, having primary responsibility for matters pertaining to national defense, the authority for original classification of information or material under this order may be exercised by the head of the department, agency, or Governmental unit concerned or by such responsible officers or employees as he, or his representative, may designate for that purpose. The delegation of such authority to classify shall be limited as severely as is consistent with the orderly and expeditious transaction of Government business.

The White House Office
President's Science Advisory Committee
Bureau of the Budget
Council of Economic Advisers
National Security Council
Central Intelligence Agency
Department of State
Department of the Treasury
Department of Defense
Department of the Army
Department of the Navy
Department of the Air Force
Department of Justice
Department of Commerce
Department of Labor
Department of Transportation
Atomic Energy Commission
Canal Zone Government
Federal Communications Commission
Federal Radiation Council
General Services Administration
Interstate Commerce Commission
National Aeronautics and Space Administration
National Aeronautics and Space Council
United States Civil Service Commission
United States Information Agency
Agency for International Development
Office of Emergency Planning
Peace Corps
President's Foreign Intelligence Advisory Board
United States Arms Control and Disarmament Agency
Export-Import Bank of Washington
Office of Science and Technology
The Special Representative for Trade Negotiations

(b) In the following departments, agencies, and Governmental units, having partial but not primary responsibility for matters pertaining to national defense, the authority for original classification of information or material under this order shall be exercised only by the head of the department, agency, or Governmental unit without delegation:

Post Office Department
Department of the Interior
Department of Agriculture
Department of Health, Education, and Welfare
Civil Aeronautics Board
Federal Power Commission
National Science Foundation
Panama Canal Company
Renegotiation Board
Small Business Administration
Subversive Activities Control Board
Tennessee Valley Authority
Federal Maritime Commission
Subversive Activities Control Board

(c) Any agency or unit of the executive branch not named herein, and any such agency or unit which may be established hereafter, shall be deemed not to have authority for original classification of information or material under this order, except as such authority may be specifically conferred upon any such agency or unit hereafter.

Sec. 3. Classification. Persons designated to have authority for original classification of information or material which requires protection in the interests of national defense under this order shall be held responsible for its proper classification in accordance with the definitions of the three categories in section 1, hereof. Unnecessary classification and over-classification shall be scrupulously avoided. The following special rules shall be observed in classification of defense information or material:

(a) Documents in General. Documents shall be classified according to their own content and not necessarily according to their relationship to other documents. References to classified material which do not reveal classified defense information shall not be classified.

(b) Physically Connected Documents. The classification of a file or group of physically connected documents shall be at least as high as that of the most highly classified document therein. Documents separated from the file or group shall be handled in accordance with their individual defense classification.

(c) Multiple Classification. A document, product, or substance shall bear a classification at least as high as that of its highest classified component. The document, product, or substance shall bear only one over-all classification, notwithstanding that pages, paragraphs, sections, or components thereof bear different classifications.

(d) Transmittal Letters. A letter transmitting defense information shall be classified at least as high as its highest classified enclosure.

(e) Information Originated by a Foreign Government or Organization. Defense information of a classified nature furnished to the United States by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information.

Sec. 4. Declassification, Downgrading, or Upgrading. When classified information or material no longer requires its present level of protection in the defense interest, it shall be downgraded or declassified in order to preserve the ef-

fectiveness and integrity of the classification system and to eliminate classifications of information or material which no longer require classification protection. Heads of departments or agencies originating classified information or material shall designate persons to be responsible for continuing review of such classified information or material on a document-by-document, category, project, program, or other systematic basis, for the purpose of declassifying or downgrading whenever national defense considerations permit, and for receiving requests for such review from all sources. However, Restricted Data and material formerly designated as Restricted Data shall be handled only in accordance with subparagraphs 4(a) (1) below and section 13 of this order. The following special rules shall be observed with respect to changes of classification of defense information or material, including information or material heretofore classified:

(a) Automatic Changes. In order to insure uniform procedures for automatic changes, heads of departments and agencies having authority for original classification of information or material, as set forth in section 2, shall categorize such classified information or material into the following groups:

(1) Group 1. Information or material originated by foreign governments or international organizations and over which the United States Government has no jurisdiction, information or material provided for by statutes such as the Atomic Energy Act [section 2011 et seq. of Title 42, The Public Health and Welfare], and information or material requiring special handling, such as intelligence and cryptography. This information and material is excluded from automatic downgrading or declassification.

(2) Group 2. Extremely sensitive information or material which the head of the agency or his designees exempt, on an individual basis, from automatic downgrading and declassification.

(3) Group 3. Information or material which warrants some degree of classification for an indefinite period. Such information or material shall become automatically downgraded at 12-year intervals until the lowest classification is reached, but shall not become automatically declassified.

(4) Group 4. Information or material which does not qualify for, or is not assigned to, one of the first three groups. Such information or material shall become automatically downgraded at three-year intervals until the lowest classification is reached, and shall be automatically declassified twelve years after date of issuance.

To the fullest extent practicable, the classifying authority shall indicate on the information or material at the time of original classification if it can be downgraded or declassified at an earlier date, or if it can be downgraded or declassified after a specified event, or upon the removal of classified attachments or enclosures. The heads, or their designees, of departments and agencies in possession of defense information or material classified pursuant to this order, but not bearing markings for automatic downgrading or declassification, are hereby authorized to mark or designate for automatic downgrading or declassification such information or material in accordance with the rules or regulations established by the department or agency that originally classified such information or material.

(b) Non-Automatic Changes. The persons designated to receive requests for review of classified material may downgrade or declassify such material when circumstances no longer warrant its retention in its original classification provided the consent of the appropriate classifying authority has been obtained. The downgrading or declassification of extracts from or paraphrases of classified documents shall also require the consent of the appropriate classifying authority unless the agency making such extracts knows positively that they warrant a classification lower than that of the document from which extracted, or that they are not classified.

(c) Material Officially Transferred. In the case of material transferred by or pursuant to statute or Executive order from one department or agency to another for the latter's use and as part of its official files or property, as distinguished from transfers merely for purposes of storage, the receiving department or agency shall be deemed to be the classifying authority for all purposes under this order, including declassification and downgrading.

(d) Material Not Officially Transferred. When any department or agency has in its possession any classified material which has become five years old, and it appears (1) that such material originated in an agency which has since become defunct and whose files and other property have not been officially transferred to another department or agency within the meaning of subsection (c), above, or (2) that it is impossible for the possessing department or agency to identify the originating agency, and (3) a review of the material indicates that it should be downgraded or declassified, the said possessing department or agency shall have power to declassify or downgrade such material. If it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the possessing department or agency shall not exercise the power conferred upon it by this subsection, except with the consent of the other department or agency, until thirty days after it has notified such other department or agency of the nature of the material and of its intention to declassify or downgrade the same. During such thirty-day period the other department or agency may, if it so desires, express its objections to declassifying or downgrading the particular material, but the power to make the ultimate decision shall reside in the possessing department or agency.

(e) Information or Material Transmitted by Electrical Means. The downgrading or declassification of classified information or material transmitted by electrical means shall be accomplished in accordance with the procedures described above unless specifically prohibited by the originating department or agency. Unclassified information or material which is transmitted in encrypted form shall be safeguarded and handled in accordance with the regulations of the originating department or agency.

(f) Downgrading. If the recipient of classified material believes that it has been classified too highly, he may make a request to the reviewing official who may downgrade or declassify the material after obtaining the consent of the appropriate classifying authority.

(g) Upgrading. If the recipient of unclassified information or material believes that it should be classified, or if the recipient of classified information or material believes that its classification is not sufficiently protective, it shall be safeguarded in accordance with the classifica-

tion deemed appropriate and a request made to the reviewing official, who may classify the information or material or upgrade the classification after obtaining the consent of the appropriate classifying authority. The date of this action shall constitute a new date of origin insofar as the downgrading or declassification schedule (paragraph (a) above) is concerned.

(h) Departments and Agencies Which Do Not Have Authority for Original Classification. The provisions of this section relating to the declassification of defense information or material shall apply to departments or agencies which do not, under the terms of this order, have authority for original classification of information or material, but which have formerly classified information or material pursuant to Executive Order No. 10290 of September 24, 1951.

(i) Notification of Change in Classification. In all cases in which action is taken by the reviewing official to downgrade or declassify earlier than called for by the automatic downgrading-declassification stamp, the reviewing official shall promptly notify all addressees to whom the information or material was originally transmitted. Recipients of original information or material, upon receipt of notification of change in classification, shall notify addressees to whom they have transmitted the classified information or material.

Sec. 5. Marking of Classified Material. After a determination of the proper defense classification to be assigned has been made in accordance with the provisions of this order the classified material shall be marked as follows:

(a) Downgrading-Declassification Markings. At the time of origination, all classified information or material shall be marked to indicate the downgrading-declassification schedule to be followed in accordance with paragraph (a) of section 4 of this order.

(b) Bound Documents. The assigned defense classification on bound documents, such as books or pamphlets, the pages of which are permanently and securely fastened together, shall be conspicuously marked or stamped on the outside of the front cover, on the title page, on the first page, on the back page and on the outside of the back cover. In each case the markings shall be applied to the top and bottom of the page or cover.

(c) Unbound Documents. The assigned defense classification on unbound documents, such as letters, memoranda, reports, telegrams, and other similar documents, the pages of which are not permanently and securely fastened together, shall be conspicuously marked or stamped at the top and bottom of each page, in such manner that the marking will be clearly visible when the pages are clipped or stapled together.

(d) Charts, Maps, and Drawings. Classified charts, maps, and drawings shall carry the defense classification marking under the legend, title block, or scale in such manner that it will be reproduced on all copies made therefrom. Such classification shall also be marked at the top and bottom in each instance.

(e) Photographs, Films and Recordings. Classified photographs, films, and recordings, and their containers, shall be conspicuously and appropriately marked with the assigned defense classification.

(f) Products or Substances. The assigned defense classification shall be conspicuously marked on classified products or substances, if possible, and on their containers, if possible, or, if the article or container cannot be marked, written notification of such classification shall be furnished to recipients of such products or substances.

(g) Reproductions. All copies or reproductions of classified material shall be appropriately marked or stamped in the same manner as the original thereof.

(h) Unclassified Material. Normally, unclassified material shall not be marked or stamped Unclassified unless it is essential to convey to a recipient of such material that it has been examined specifically with a view to imposing a defense classification and has been determined not to require such classification.

(i) Change or Removal of Classification. Whenever classified material is declassified, downgraded, or upgraded, the material shall be marked or stamped in a prominent place to reflect the change in classification, the authority for the action, the date of action, and the identity of the person or unit taking the action. In addition, the old classification marking shall be cancelled and the new classification (if any) substituted therefor. Automatic change in classification shall be indicated by the appropriate classifying authority through marking or stamping in a prominent place to reflect information specified in subsection 4 (a) hereof.

(j) Material Furnished Persons not in the Executive Branch of the Government. When classified material affecting the national defense is furnished authorized persons, in or out of Federal service, other than those in the executive branch, the following notation, in addition to the assigned classification marking, shall whenever practicable be placed on the material, on its container, or on the written notification of its assigned classification:

This material contains information affecting the national defense of the United States within the meaning of the espionage laws, Title 18, U.S.C., Secs. 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law

Use of alternative marking concerning "Restricted Data" as defined by the Atomic Energy Act [sections 1801-1819 of Title 42] is authorized when appropriate.

Sec. 6. Custody and Safekeeping. The possession or use of classified defense information or material shall be limited to locations where facilities for secure storage or protection thereof are available by means of which unauthorized persons are prevented from gaining access thereto. Whenever such information or material is not under the personal supervision of its custodian, whether during or outside of working hours, the following means shall be taken to protect it:

(a) Storage of Top Secret Information and Material. As a minimum, Top Secret defense information and material shall be stored in a safe or safe-type steel file container having a three-position dial-type combination lock, and being of such weight, size, construction, or installation as to minimize the possibility of unauthorized access to, or the physical theft of, such information and material. The head of a department or agency may approve other storage facilities which afford equal protection, such as an alarmed area, a vault, a vault-type room, or an area under continuous surveillance.

(b) Storage of Secret and Confidential Information and Material. As a minimum, Secret and Confidential defense in-

formation and material may be stored in a manner authorized for Top Secret information and material, or in steel file cabinets equipped with steel lockbar and a changeable three-combination dial-type padlock or in other storage facilities which afford equal protection and which are authorized by the head of the department or agency.

(c) **Storage or Protection Equipment.** Whenever new security storage equipment is procured, it should, to the maximum extent practicable, be of the type designated as security filing cabinets on the Federal Supply Schedule of the General Services Administration.

(d) **Other Classified Material.** Heads of departments and agencies shall prescribe such protective facilities as may be necessary in their departments or agencies for material originating under statutory provisions requiring protection of certain information.

(e) **Changes of Lock Combinations.** Combinations on locks of safekeeping equipment shall be changed, only by persons having appropriate security clearance, whenever such equipment is placed in use after procurement from the manufacturer or other sources, whenever a person knowing the combination is transferred from the office to which the equipment is assigned, or whenever the combination has been subjected to 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 defense material authorized for storage in the safekeeping equipment concerned.

(f) **Custodian's Responsibilities.** Custodians of classified defense material shall be responsible for providing the best possible protection and accountability for such material at all times and particularly for securely locking classified material in approved safekeeping equipment whenever it is not in use or under direct supervision of authorized employees. Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified defense information or material by sight or sound, and classified information shall not be discussed with or in the presence of unauthorized persons.

(g) **Telephone Conversations.** Defense information classified in the three categories under the provisions of this order shall not be revealed in telephone conversations, except as may be authorized under section 8 hereof with respect to the transmission of Secret and Confidential material over certain military communications circuits.

(h) **Loss or Subjection to Compromise.** Any person in the executive branch who has knowledge of the loss or possible subjection to compromise of classified defense information shall promptly report the circumstances to a designated official of his agency, and the latter shall take appropriate action forthwith, including advice to the originating department or agency.

Sec. 7. Accountability and Dissemination. Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and only if they have been determined to be trustworthy. Proper control of dissemination of classified defense information shall be maintained at all times, including good accountability records of classified defense information documents, and severe limitation on the number of such documents originated as well as the number of copies thereof reproduced. The number of copies of classified defense information documents shall be kept to a minimum to decrease the risk of compromise of the information contained in such documents and the financial burden on the Government in protecting such documents. The following special rules shall be observed in connection with accountability for and dissemination of defense information or material:

(a) **Accountability Procedures.** Heads of departments and agencies shall prescribe such accountability procedures as are necessary to control effectively the dissemination of classified defense information, with particularly severe control on material classified Top Secret under this order. Top Secret Control Officers shall be designated, as required, to receive, maintain accountability registers of, and dispatch Top Secret material.

(b) **Dissemination Outside the Executive Branch.** Classified defense information shall not be disseminated outside the executive branch except under conditions and through channels authorized by the head of the disseminating department or agency, even though the person or agency to which dissemination of such information is proposed to be made may have been solely or partly responsible for its production.

(c) **Information Originating in Another Department or Agency.** Except as otherwise provided by section 102 of the National Security Act of July 26, 1947, c. 343, 61 Stat. 498, as amended, [section 403 of this title], classified defense information originating in another department or agency shall not be disseminated outside the receiving department or agency without the consent of the originating department or agency. Documents and material containing defense information which are classified Top Secret or Secret shall not be reproduced without the consent of the originating department or agency.

Sec. 8. Transmission. For transmission outside of a department or agency, classified defense material of the three categories originated under the provisions of this order shall be prepared and transmitted as follows:

(a) **Preparation for Transmission.** Such material shall be enclosed in opaque inner and outer covers. 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 form 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 form shall identify the addresser, addressee, and the document, but shall contain no classified information. It shall be signed by the proper recipient and returned to the sender.

(b) **Transmitting Top Secret Material.** The transmission of Top Secret material shall be effected preferably by direct contact of officials concerned, or, alternatively, by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, or by electric means in encrypted form; or, in the case of information transmitted by the Federal Bureau of Investigation, such means of transmission may be used as are currently approved by the Director, Federal Bureau

of Investigation, unless express reservation to the contrary is made in exceptional cases by the originating agency.

(c) **Transmitting Secret Information and Material.** Secret information and material shall be transmitted within and between 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 Top Secret information and material, by authorized courier, by United States registered mail, or by the use of protective services provided by commercial carriers, air or surface, under such conditions as may be prescribed by the head of the department or agency concerned. Secret information and material may be transmitted outside those areas by one of the means established for Top Secret information and material, by commanders or masters of vessels of United States registry, or by the United States registered mail through Army, Navy, Air Force, or United States civil postal facilities: provided that the information or material does not at any time pass out of United States Government control and does not pass through a foreign postal system. For the purposes of this section registered mail in the custody of a transporting agency of the United States Post Office is considered within United States Government control unless the transporting agent is foreign controlled or operated. Secret information and material may, however, be transmitted between United States Government or Canadian Government installations, or both, in the forty-eight contiguous States, the District of Columbia, Alaska, and Canada by United States and Canadian registered mail with registered mail receipt. Secret information and material may also be transmitted over communications circuits in accordance with regulations promulgated for such purpose by the Secretary of Defense.

(d) **Transmitting Confidential Information and Material.** 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 those areas Confidential information and material shall be transmitted in the same manner as authorized for higher classifications.

(e) **Within an Agency.** Preparation of classified defense material for transmission, and transmission of it, within a department or agency shall be governed by regulations, issued by the head of the department or agency, insuring a degree of security equivalent to that outlined above for transmission outside a department or agency.

Sec. 9. Disposal and Destruction. Documentary record material made or received by a department or agency in connection with transaction of public business and preserved as evidence of the organization, functions, policies, operations, decisions, procedures or other activities of any department or agency of the Government, or because of the informational value of the data contained therein, may be destroyed only in accordance with the act of July 7, 1945, c. 192, 57 Stat. 380, as amended [sections 366-380 of Title 44]. Nonrecord classified material, consisting of extra copies and duplicates including shorthand notes, preliminary drafts, used carbon paper, and other material of similar temporary nature, may be destroyed, under procedures established by the head of the department or agency which meet the following requirements, as soon as it has served its purpose:

(a) **Methods of Destruction.** Classified defense material shall be destroyed by burning in the presence of an appropriate official or by other methods authorized by the head of an agency provided the resulting destruction is equally complete.

(b) **Records of Destruction.** Appropriate accountability records maintained in the department or agency shall reflect the destruction of classified defense material.

Sec. 10. Orientation and Inspection. To promote the basic purposes of this order, heads of those departments and agencies originating or handling classified defense information shall designate experienced persons to coordinate and supervise the activities applicable to their departments or agencies under this order. Persons so designated shall maintain active training and orientation programs for employees concerned with classified defense information to impress each such employee with his individual responsibility for exercising vigilance and care in complying with the provisions of this order. Such persons shall be authorized on behalf of the heads of the departments and agencies to establish adequate and active inspection programs to the end that the provisions of this order are administered effectively.

Sec. 11. Interpretation of Regulations by the Attorney General. The Attorney General, upon request of the head of a department or agency or his duly designated representative, shall personally or through authorized representatives of the Department of Justice render an interpretation of these regulations in connection with any problems arising out of their administration.

Sec. 12. Statutory Requirements. Nothing in this order shall be construed to authorize the dissemination, handling or transmission of classified information contrary to the provisions of any statute.

Sec. 13. "Restricted Data." Material Formerly Designated as "Restricted Data." Communications Intelligence and Cryptography. (a) 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 formerly designated as "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 Atomic Energy Commission.

(b) Nothing in this order shall prohibit any special requirements that the originating agency or other appropriate authority may impose as to communications intelligence, cryptography, and matters related thereto.

Sec. 14. Combat Operations. The provisions of this order with regard to dissemination, transmission, or safekeeping of classified defense information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

Sec. 15. Exceptional Cases. When, in an exceptional case, a person or agency not authorized to classify defense information originates information which is believed to require classification, such person or agency shall protect that information in the manner prescribed by this order for that category of classified defense information into which it is believed to fall, and shall transmit the information forth-

with, under appropriate safeguards, to the department, agency, or person having both the authority to classify information and a direct official interest in the information (preferably, that department, agency, or person to which the information would be transmitted in the ordinary course of business), with a request that such department, agency, or person classify the information.

Historical Research. As an exception to the standard for access prescribed in the first sentence of section 7, but subject to all other provisions of this order, the head of an agency may permit persons outside the executive branch performing functions in connection with historical research projects to have access to classified defense information originated within his agency if he determines that: (a) access to the information will be clearly consistent with the interests of national defense, and (b) the person to be granted access is trustworthy: Provided, that the head of the agency shall take appropriate steps to assure that classified information is not published or otherwise compromised.

Sec. 16. Review to Insure That Information Is Not Improperly Withheld Hereunder. The President shall designate a member of his staff who shall receive, consider, and take action upon, suggestions or complaints from non-Governmental sources relating to the operation of this order.

Sec. 17. Review to Insure Safeguarding of Classified Defense Information. The National Security Council shall conduct a continuing review of the implementation of this order to insure that classified defense information is properly safeguarded, in conformity herewith.

Sec. 18. Review Within Departments and Agencies. The head of each department and agency shall designate a member or members of his staff who shall conduct a continuing review of the implementation of this order within the department or agency concerned to insure that no information is withheld hereunder which the people of the United States have a right to know, and to insure that classified defense information is properly safeguarded in conformity herewith.

Sec. 19. Unauthorized Disclosure by Government Personnel. The head of each department and agency 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 knowingly responsible for any release or disclosure of classified defense information or material except in the manner authorized by this order, and where a violation of criminal statutes may be involved, to refer promptly to the Department of Justice any such case.

Sec. 20. Revocation of Executive Order No. 10290. Executive Order No. 10290 of September 24, 1951 [set out as a note under this section] is revoked as of the effective date of this order.

Sec. 21. Effective Date. This order shall become effective on December 15, 1953.

EXECUTIVE ORDER NO. 10865

Feb. 23, 1960, 25 F.R. 1583, as amended by Ex.Ord.No.10909, Jan. 18, 1961, 26 F.R. 508; Ex.Ord.No.11382, Nov. 28, 1967, 32 F.R. 16247

SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that these provisions and procedures recognize the interest of individuals affected thereby and provide maximum possible safeguards to protect such interests:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the armed forces of the United States, it is hereby ordered as follows:

Section 1. (a) The Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, and the Secretary of Transportation, respectively, shall, by regulation, prescribe such specific requirements, restrictions, and other safeguards as they consider necessary to protect (1) releases of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with their respective agencies, and (2) other releases of classified information to or within industry that such agencies have responsibility for safeguarding. So far as possible, regulations prescribed by them under this order shall be uniform and provide for full cooperation among the agencies concerned.

(b) Under agreement between the Department of Defense and any other department or agency of the United States, including, but not limited to, those referred to in subsection (c) of this section, regulations prescribed by the Secretary of Defense under subsection (a) of this section may be extended to apply to protect releases (1) of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with such other department or agency, and (2) other releases of classified information to or within industry which such other department or agency has responsibility for safeguarding.

(c) When used in this order, the term "head of a department" means the Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, the head of any other department or agency of the United States with which the Department of Defense makes an agreement under subsection (b) of this section, and, in sections 4 and 8, includes the Attorney General. The term "department" means the Department of State, the Department of Defense, the Atomic Energy Commission, the National Aeronautics and Space Administration, the Department of Transportation, any other department or agency of the United States with which the Department of

Defense makes an agreement under subsection (c) of this section, and, in sections 4 and 8, includes the Department of Justice.

Sec. 2. An authorization for access to classified information may be granted by the head of a department or his designee, including but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an "applicant", for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

Sec. 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee, including, but not limited to, those officials named in section 8 of this order, for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

Sec. 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the department to be good and sufficient.

(b) Whenever procedures under paragraphs (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

Sec. 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

Sec. 6. The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section 1(b), or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Stand-

ardized Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the executive branch of the Government or members of the armed forces of the United States not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An officer or employee of the executive branch of the Government or a member of the armed forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other department or agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination.

Sec. 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

Sec. 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a department by this order may be delegated to the

(1) Under Secretary of State or a Deputy Under Secretary of State, in the case of authority vested in the Secretary of State;

(2) Deputy Secretary of Defense or an Assistant Secretary of Defense, in the case of authority vested in the Secretary of Defense;

(3) General Manager of the Atomic Energy Commission, in the case of authority vested in the Commissioners of the Atomic Energy Commission;

(4) Deputy Administrator of the National Aeronautics and Space Administration, in the case of authority vested in the Administrator of the National Aeronautics and Space Administration;

(5) Under Secretary of Transportation, in the case of authority vested in the Secretary of Transportation;

(6) Deputy Attorney General or an Assistant Attorney General, in the case of authority vested in the Attorney General; or

(7) the deputy of that department, or the principal assistant to the head of that department, as the case may be, in the case of authority vested in the head of a department or agency of the United States with which the Department of Defense makes an agreement under section 1(b).

Sec. 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

DWIGHT D. EISENHOWER

EXECUTIVE ORDER NO. 10985

Jan. 15, 1962, 27 F.R. 439

AMENDMENT OF EXECUTIVE ORDER NO. 10501, RELATING TO SAFEGUARDING OFFICIAL INFORMATION

By virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, and deeming such action necessary in the best interest of the national security, it is ordered that section 2 of Executive Order No. 10501 of November 5, 1953, as amended by Executive Order No. 10901 of January 9, 1961 [set out as a note under this section], be, and it is hereby, further amended as follows:

Section 1. Subsection (a) of section 2 is amended (1) by deleting from the list of departments and agencies thereunder the Operations Coordinating Board, the Office of Civil and Defense Mobilization, the International Cooperation Administration, the Council on Foreign Economic Policy, the Development Loan Fund, and the President's Board of Consultants on Foreign Intelligence Activities, and (2) by adding thereto the following-named agencies:

Agency for International Development
Office of Emergency Planning
Peace Corps
President's Foreign Intelligence Advisory Board
United States Arms Control and Disarmament Agency

Sec. 2. Subsection (b) of section 2 is amended by deleting from the list of departments and agencies thereunder the Government Patent Board, and by adding thereto the following-named agency:

Federal Maritime Commission

Sec. 3. The agencies which have been added by this order to the lists of departments and agencies under subsections (a) and (b) of section 2 of Executive Order No. 10501, as amended [set out as a note under this section], shall be deemed to have had authority for classification of information or material from the respective dates on which such agencies were established.

JOHN F. KENNEDY

EXECUTIVE ORDER NO. 11097

Mar. 6, 1963, 28 F.R. 2225

AMENDMENT OF EXECUTIVE ORDER NO. 10501, RELATING TO SAFEGUARDING OFFICIAL INFORMATION

By virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, and deeming such action necessary in the best interest of the national security, it is hereby ordered as follows:

Section 1. Section 2 of Executive Order No. 10501 of November 5, 1953, as amended by Executive Order No. 10901 of January 9, 1961, and by Executive Order No. 10985 of January 12, 1962 [set out as a note under this section], is hereby further amended (A) by adding at the

end of Subsection (a) thereof "Export-Import Bank of Washington", "Office of Science and Technology", and "The Special Representative for Trade Negotiations"; and (B) by deleting from Subsection (b) thereof "Subversive Activities Control Board."

Sec. 2. The Export-Import Bank of Washington, the Office of Science and Technology, and The Special Representative for Trade Negotiations shall be deemed to have had authority for the original classification of information and material from the respective dates on which such agencies were established.

JOHN F. KENNEDY

Notes of Decisions

Library references
War and National Defense ⟸10.
C.J.S. War and National Defense § 48.

1. Classification of material

"Classification" in security sense simply means decision made by proper authority in Department of Defense to put piece of defense information or material into specific category that then makes it subject to current regulations regarding safekeeping and dissemination. Dubin v. U. S., 1966, 363 F.2d 938, 176 Ct.Cl. 702, certiorari denied 87 S.Ct. 1019, 386 U.S. 956, 18 L.Ed.2d 103.

Purposes of classification system of Department of Defense is to safeguard information from becoming known to potential enemies of United States in interest of national defense. Id.

Under section 783 of this title, prohibiting communication of classified information by United States officers or employees to an agent or representative of a foreign government, the classification of documents is not required to be made personally by President of United States or Secretary of State; an Ambassador of United States Embassy had authority to classify foreign service dispatches, and dispatches as classified and certified by the Ambassador were within scope of section 783 of this title. Scarbeck v. U. S., C.A.D.C.1962, 317 F.2d 546, certiorari denied 83 S.Ct. 1897, 374 U.S. 856, 10 L.Ed.2d 1077.

Foreign service dispatches classified as "secret" or "confidential" pursuant to presidential executive order and foreign service manual were "classified as affecting the security of the United States" within meaning of section 783 of this title prohibiting a United States officer or employee from communicating classified information to representatives of a foreign government. Id.

2. Suspension of security clearance

Defense department order providing that willful failure or refusal of employee, needing security clearance, to furnish information might prevent finding required for security clearance in which event security clearance would be suspended and further processing of case discontinued, was not authorized by any executive order or Congressional act. Shoultz v. McNamara, D.C.Cal.1968, 282 F.Supp. 315.

Where, under defense department order, employee whose security clearance was once suspended had no further administrative or judicial remedy to challenge suspension, and further processing of case was discontinued, and where employer would no longer employ employee until clearance, suspension was equivalent of final revocation and was deprivation of employment and professional rights within liberty and property concepts of U.S.C.A.Const. Amend. 5. Id.

3. Procedure for redress

That employee whose security clearance and employment had been suspended could obtain resumption of processing of his case by answering questions under procedures which he believed to be unauthorized and unconstitutional and which did raise serious constitutional questions did not negate deprivation of employment and property rights within liberty and property concepts of U.S.C.A.Const. Amend. 5. Shoultz v. McNamara, D.C. Cal.1968, 282 F.Supp. 315.

4. Access to secret information

Where court found that board followed improper procedure in determining that employee of government contractor was not entitled to clearance for access to secret information and in determining that, pending final disposition of case, employee was not authorized for clearance at any level, trial court should have remanded the case for further proceedings but should not have ordered that pending such proceedings employee be given clearance for access to secret information. McNamara v. Remenyl, C.A.Cal. 1968, 391 F.2d 128.

ESPIONAGE ACT

Chapter 37.—ESPIONAGE AND CENSORSHIP

AMENDMENTS

1961—Pub. L. 87-369, § 2, Oct. 4, 1961, 75 Stat. 795, deleted item 791.

1958—Pub. L. 85-568, title III, § 304 (c) (2), July 29, 1958, 72 Stat. 434, added item 799.

1953—Act June 30, 1953, ch. 175, § 3, 67 Stat. 133, added second item 798.

1951—Act Oct. 31, 1951, ch. 655, § 23, 65 Stat. 719, added item 798.

§ 791. Repealed. Pub. L. 87-369, § 1, Oct. 4, 1961, 75 Stat. 795.

Section, act June 25, 1948, ch. 645, 62 Stat. 736, related to the application of the chapter within the admiralty and maritime jurisdiction of the United States, on the high seas, and within the United States.

§ 792. Harboring or concealing persons.

Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offense under sections 793 or 794 of this title, shall be fined not more than $10,000 or imprisoned not more than ten years, or both. (June 25, 1948, ch. 645, 62 Stat. 736.)

LEGISLATIVE HISTORY

Revisor's Note.—Based on section 35 of title 50, U. S. C., 1940 ed., War and National Defense (June 15, 1917, ch. 30, title I, § 6, 40 Stat. 219; Mar. 28, 1940, ch. 72, § 2, 54 Stat. 79).

Similar harboring and concealing language was added to section 2388 of this title.

Mandatory punishment provision was rephrased in the alternative.

INDICTMENT FOR VIOLATING THIS SECTION AND SECTIONS 793, 794; LIMITATION PERIOD

Act Sept. 23, 1950, ch. 1024, § 19, 64 Stat. 1005, provides that an indictment for any violation of this section and sections 793 and 794 of this title, other than a violation constituting a capital offense, may be found at any time within ten years next after such violation shall have been

[1] So enacted.

SOURCE:
U.S. Laws, Statutes, etc. United States Code. 1969 ed., containing the general and permanent laws of the United States, in force on January 3, 1965. Prepared and published . . .by the Committee on the Judiciary of the House of Representatives. Washington, U.S. Govt. Print. Off., 1965 - (v. 4, title 18, Crimes and Criminal Procedure, chapter 37, pages 3574-9).

committed, but that such section 19 shall not authorize prosecution, trial, or punishment for any offense "now" barred by the provisions of existing law.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

CROSS REFERENCES

Federal retirement benefits, forfeiture upon conviction of offenses described under this section, see section 2282 of Title 5, Executive Departments and Government Officers and Employees.

Forfeiture of veterans' benefits upon conviction under this section, see section 3505 of Title 38, Veterans' Benefits.

Harboring and concealing, generally, see section 1071 et seq. of this title.

Jurisdiction of offenses, see section 3241 of this title.

Misprision of felony, see section 4 of this title.

§ 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 any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to 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, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

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

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

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

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

LEGISLATIVE HISTORY

Revisor's Note.—Based on sections 31 and 36 of title 50, U. S. C., 1940 ed., War and National Defense (June 15, 1917, ch. 30, title I, §§ 1, 6, 40 Stat. 217, 219; Mar. 28, 1940, ch. 72, § 1, 54 Stat. 79).

Section consolidated sections 31 and 36 of title 50, U. S. C., 1940 ed., War and National Defense.

Words "departments or agencies" were inserted twice in conformity with definitive section 6 of this title to eliminate any possible ambiguity as to scope of section.

The words "or induces or aids another" were omitted wherever occurring as unnecessary in view of definition of "principal" in section 2 of this title.

Mandatory punishment provision was rephrased in the alternative.

Minor changes were made in phraseology.

AMENDMENTS

1950—Act Sept. 23, 1950, divided section into subdivisions, added laboratories and stations, and places where material or instruments for use in time of war are the subject of research or development to the list of facilities and places to which subsection (a) applies, made subsection (d) applicable only in cases in which possession, access, or control is lawful, added subsection (e) to take care of cases in which possession, access, or control, is unlawful, made subsection (f) applicable to instruments and appliances, as well as to documents, records, etc., and provided by subsection (g) a separate penalty for conspiracy to violate any provisions of this section.

INDICTMENT FOR VIOLATING THIS SECTION; LIMITATION PERIOD

Limitation period in connection with indictments for violating this section, see note under section 792 of this title.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

CROSS REFERENCES

Activities affecting armed forces—

Generally, see section 2387 of this title.

During war, see section 2388 of this title.

Classified information, disclosure by Government official, or other person, penalty for, see section 783 (b), (d) of Title 50, War and National Defense and section 798 of this title.

Federal retirement benefits, forfeiture upon conviction of offenses described under this section, see section 2282 of Title 5, Executive Departments and Government Officers and Employees.

Forfeiture of veterans' benefits upon conviction under this section, see section 3505 of Title 38, Veterans' Benefits.

Jurisdiction of offenses, see section 3241 of this title.

Letters, writings, etc., in violation of this section as nonmailable, see section 1717 of this title.

Nonmailable letters and writings, see section 1717 of this title.

§ 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. (June 25, 1948, ch. 645, 62 Stat. 737; Sept. 3, 1954, ch. 1261, title II, § 201, 68 Stat. 1219.)

LEGISLATIVE HISTORY

Revisor's Note.—Based on sections 32 and 34 of title 50, U. S. C., 1940 ed., War and National Defense (June 15, 1917, ch. 30, title I, §§ 2, 4, 40 Stat. 218, 219).

Section consolidates sections 32 and 34 of title 50, U. S. C., 1940 ed., War and National Defense.

The words "or induces or aids another" were omitted as unnecessary in view of definition of "principal" in section 2 of this title.

The conspiracy provision of said section 34 was also incorporated in section 2388 of this title.

Minor changes were made in phraseology.

AMENDMENTS

1954—Act Sept. 3, 1954, increased the penalty for peacetime espionage and corrected a deficiency on the sentencing authority by increasing penalty to death or imprisonment for any term of years.

TEMPORARY EXTENSION OF WAR PERIOD

Temporary extension of war period, see section 798 of this title.

Section 7 of act June 30, 1953, ch. 175, 67 Stat. 133, repealed Joint Res. July 3, 1952, ch. 570, § 1 (a) (29), 66 Stat. 333; Joint Res. Mar. 31, 1953, ch. 13, § 1, 67 Stat. 18, which had provided that this section should continue in force until six months after the termination of the National emergency proclaimed by 1950 Proc. No. 2914 which is set out as a note preceding section 1 of Appendix to Title 50, War and National Defense.

Section 6 of Joint Res. July 3, 1952, repealed Joint Res. Apr. 14, 1952, ch. 204, 66 Stat. 54, as amended by Joint Res. May 28, 1952, ch. 339, 66 Stat. 96. Intermediate extensions by Joint Res. June 14, 1952, ch. 437, 66 Stat. 137, and Joint Res. June 30, 1952, ch. 526, 66 Stat. 296, which continued provisions until July 3, 1952, expired by their own terms.

INDICTMENT FOR VIOLATING THIS SECTION; LIMITATION PERIOD

Limitation period in connection with indictments for violating this section, see note under section 792 of this title.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

CROSS REFERENCES

Classified information, disclosure by Government official or other person, penalty for, see section 783 (b), (d) of Title 50, War and National Defense and section 798 of this title.

Conspiracy to commit offense generally, see section 371 of this title.

Federal retirement benefits, forfeiture upon conviction of offenses described under this section, see section 2282 of Title 5, Executive Departments and Government Officers and Employees.

Forfeiture of veterans' benefits upon conviction under this section, see section 3505 of Title 38, Veterans' Benefits.

Jurisdiction of offenses, see section 3241 of this title.

Letters, writings, etc., in violation of this section as nonmailable, see section 1717 of this title.

Nonmailable letters and writings, see section 1717 of this title.

§ 795. Photographing and sketching defense installations.

(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 737.)

Legislative History

Reviser's Note.—Based on sections 45 and 45c of title 50, U. S. C., 1940 ed., War and National Defense (Jan. 12, 1938, ch. 2, §§ 1, 4, 52 Stat. 3, 4).

Section consolidated sections 45 and 45c of title 50, U. S. C., 1940 ed., War and National Defense.

Minor changes were made in phraseology.

Canal Zone

Applicability of section to Canal Zone, see section 14 of this title.

Ex. Ord. No. 10104. Definitions of Vital Military and Naval Installations and Equipment

Ex. Ord. No. 10104, Feb. 1, 1950, 15 F. R. 597, provided:

Now, therefore, by virtue of the authority vested in me by the foregoing statutory provisions, and in the interests of national defense, I hereby define the following as vital military and naval installations or equipment requiring protection against the general dissemination of information relative thereto:

1. All military, naval, or air-force installations and equipment which are now classified, designated, or marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", "confidential", or "restricted", and all military, naval, or air-force installations and equipment which may hereafter be so classified, designated, or marked with the approval or at the direction of the President, and located within:

(a) Any military, naval, or air-force reservation, post, arsenal, proving ground, range, mine field, camp, base, airfield, fort, yard, station, district, or area.

(b) Any defensive sea area heretofore established by Executive order and not subsequently discontinued by Executive order, and any defensive sea area hereafter established under authority of section 2152 of title 18 of the United States Code.

(c) Any airspace reservation heretofore or hereafter established under authority of section 4 of the Air Commerce Act of 1926 (44 Stat. 570; 49 U. S. C. 174) except the airspace reservation established by Executive Order No. 10092 of December 17, 1949.

(d) Any naval harbor closed to foreign vessels.

(e) Any area required for fleet purposes.

(f) Any commercial establishment engaged in the development or manufacture of classified military or naval arms, munitions, equipment, designs, ships, aircraft, or vessels for the United States Army, Navy, or Air Force.

2. All military, naval, or air-force aircraft, weapons, ammunition, vehicles, ships, vessels, instruments, engines, manufacturing machinery, tools, devices, or any other equipment whatsoever, in the possession of the Army, Navy, or Air Force or in the course of experimentation, development, manufacture, or delivery for the Army, Navy, or Air Force which are now classified, designated, or marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", "confidential", or "restricted", and all such articles, materials, or equipment which may hereafter be so classified, designated, or marked with the approval or at the direction of the President.

3. All official military, naval, or air-force books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications which are now marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", "confidential", or "restricted", and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.

This order supersedes Executive Order No. 8381 of March 22, 1940, entitled "Defining Certain Vital Military and Naval Installations and Equipment."

Cross References

Publication and sale of photographs of defense installations, see section 797 of this title.

§ 796. Use of aircraft for photographing defense installations.

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 738.)

Legislative History

Reviser's Note.—Based on sections 45, 45a, and 45c of title 50, U. S. C., 1940 ed., War and National Defense (Jan. 12, 1938, ch. 2, §§ 1, 2, 4, 52 Stat. 3, 4).

Reference to persons causing or procuring was omitted as unnecessary in view of definition of "principal" in section 2 of this title.

Punishment provided by section 795 of this title is repeated, and is from said section 45 of title 50, U. S. C., 1940 ed.

Minor changes were made in phraseology.

Canal Zone

Applicability of section to Canal Zone, see section 14 of this title.

§ 797. Publication and sale of photographs of defense installations.

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both. (June 25, 1948, ch. 645, 62 Stat. 738.)

LEGISLATIVE HISTORY

Revisor's Note.—Based on sections 45 and 45b, of title 50, U. S. C., 1940 ed., War and National Defense (Jan. 12, 1938, ch. 2, §§ 1, 3, 52 Stat. 3).

Punishment provision of section 45 of title 50, U. S. C., 1940 ed., War and National Defense, is repeated. Words "upon conviction" were deleted as surplusage since punishment cannot be imposed until a conviction is secured.

Minor changes were made in phraseology.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

§ 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 process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

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

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

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

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

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

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

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

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

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

CROSS REFERENCES

Disclosure of classified information by Government officer or employee, see section 783 (b), (d) of Title 50, War and National Defense.

Federal retirement benefits, forfeiture upon conviction of offenses described under this section, see section 2282 of Title 5, Executive Departments and Government Officers and Employees.

Forfeiture of veterans' benefits upon conviction under this section, see section 3505 of Title 38, Veterans' Benefits.

§ 798. Temporary extension of section 794.[1]

The provisions of section 794 of this title, as amended and extended by section 1 (a) (29) of the Emergency Powers Continuation Act (66 Stat. 333), as further amended by Public Law 12, Eighty-third Congress, in addition to coming into full force and effect in time of war shall remain in full force and effect until six months after the termination of the national emergency proclaimed by the President on December 16, 1950 (Proc. 2912, 3 C. F. R., 1950 Supp., p. 71), or such earlier date as may be prescribed by concurrent resolution of the Congress, and acts which would give rise to legal consequences and penalties under section 794 when performed during a state of war shall give rise to the same legal consequences and penalties when they are performed during the period above provided for. (Added June 30, 1953, ch. 175, § 4, 67 Stat. 133.)

REFERENCES IN TEXT

Section 1 (a) (29) of the Emergency Powers Continuation Act (66 Stat. 333) as further amended by Public Law 12, Eighty-third Congress, referred to in the text, was formerly set out as a note under section 791 of this title and was repealed by section 7 of act June 30, 1953.

Proc. 2912, 3 C. F. R., 1950 Supp., p. 71, referred to in the text, is an erroneous citation. It should refer to Proc. 2914 which is set out as a note preceding section 1 of Appendix to Title 50, War and National Defense.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

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

Whoever willfully shall violate, attempt to violate, or conspire to violate any regulation or order promulgated by the Administrator of the National Aeronautics and Space Administration for the protection or security of any laboratory, station, base or other facility, or part thereof, or any aircraft,

[1] So enacted. See second section 798 enacted on June 30, 1953, set out below.

[1] So enacted. See first section 798 enacted on Oct. 31, 1951, set out above.

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

CODIFICATION

Section was added by subsec. (c) of section 304 of Pub. L. 85-568. Subsecs. (a) and (b) of section 304 are classified to section 2455 of Title 42, The Public Health and Welfare. Subsec. (d) of section 304 is classified to section 1114 of this title. Subsec. (e) of section 304 is classified to section 2456 of Title 42.

CANAL ZONE

Applicability of section to Canal Zone, see section 14 of this title.

CLASSIFYING, DECLASSIFYING OF PAPERS

Affidavit of George MacClain, *presented in open session in U.S. District Court. Most of the government's affidavits were presented in closed session.*

I, George MacClain, Director of the Security Classification Management Division, Office of the Deputy Assistant Secretary of Defense (Security Policy) (Administration), being duly sworn, depose and say:

1. That I have held my present position since 1953. I have been employed in the Department of Defense continuously since 1955.

2. That under the general direction of the Assistant Secretary of Defense (Administration), my Division is responsible for the development, promulgation, and administrative oversight of the rules and regulations of downgrading, and declassification of official information over which the Department of Defense (DoD) has original classification jurisdiction vested in the Secretary of Defense by Executive Order (EO) 10501 Safeguarding Official Information in the Interests of the Defense of the United States, December 15, 1953, as amended, or over which the DoD has derivative classification authority by reason of having been placed in custody thereof by some other United States Government agency, foreign nation, or international organization exercising original classifying jurisdiction. A copy of EO 10501, as amended to date, is attached hereto.

3. That the principal regulations of the DoD for security classification, downgrading and declassification consist of DoD Instruction 5210.47, Security Classification of Official Information, December 31, 1964, and DoD Directive 5200.10, Downgrading and Declassification of Classified Defense Information, July 26, 1962. These regulations specifically implement those portions of EO 10501, as amended, which pertain to security classification, downgrading and declassification of official information. Copies of these regulations, as amended to date, are attached hereto.

4. That as originally issued in 1953, EO 10501 provided guidance for security classification at three levels, TOP SECRET, SECRET, and CONFIDENTIAL, and further provided for the downgrading and declassification of information when the same level or no level of classification was no longer required. Under the original EO 10501, downgrading and declassification were to be accomplished upon the basis of the results of review and reevaluation from time to time more or less on continuous basis. On September 1961, EO 10501 was amended by EO 10964 for the purpose of providing for a system of time-phased automatic downgrading and declassification to supplement the on-going review and reevaluation process. This automatic system was derived from a similar system earlier created by the DoD for its own use. DoD Directive 5200.10 implements EO 10501 as amended by EO 10964.

purpose of providing for a system of time-phased automatic downgrading and declassification to supplement the on-going review and reevaluation process. This automatic system was derived from a similar system earits own use DoD Directive 20, 1961, EO 10501 was amended, as implemented by DoD Instruction 5210.47 and DoD Directive 5200.10, the following are some of the basic concepts of the system.

Source: Classifying, Declassifying of Papers. Affidavit of George Mclain, presented in open session in U.S. District Court. Washington Post, June 22, 1971: A 11.

a. The basis for original security classification is that the unauthorized disclosure of the information involved could or would be harmful to the national defense interests of the United States. The judgment whether to impose an original classification is derived from considerations of the immediate present and future. The considerations include, without limitation, the following: The international posture of the United States as related to other nations in those respects which affect, directly or indirectly, United States national defense interests. The technological state of the art in respect to those systems and equipments by which the United States is enabled to preserve its security including, without limitation, systems and equipment for gathering intelligence; weapon systems; systems and equipments for supply, maintenance and operation of military forces; systems and equipments for military forces; systems and equipments for the exercise of effective diplomatic relationships with other nations. The extent to which the information involved is already publicly known either domestically or in foreign countries. The extent to which a United States lead time advantage is deemed absolutely necessary in the interests of United States national defense, and whether in order to achieve and maintain this lead time, security classification is indispensable. The extent to which a United States national defense, and whether in order to achieve and maintain this lead time, security classificationis indispensable. The extent to which a United States lead time advantage can be forgone in the interests of net overall advantage to the United States from unclassified use of the information. The extent to which the information can in fact be safeguarded against unauthorized disclosure. The extent to which the costs of effective safeguarding would or could defeat the purposes of the program to which security classification would be applied.

b. The question as to whether the level of classification should be TOP SECRET, SECRET or CONFIDENTIAL is determined by the extent of possible damage to the current and future United States national defense interests if the information were disclosed without authority. If the damage could or would be exceptionally grave, TOP SECRET (TS) would be the required level. If the damage could or would be serious, SECRET (S); if prejudicial, CONFIDENTIAL (C). The safeguarding measures for the information subsequently applied would vary according to the level of classification.

c. Downgrading means to reduce the level of classification. Downgrading is appropriate when, on the basis of a current judgment of the present and future United States national defense interests, the degree of possible harm to those interests would change foom exceptionally grave to serious or prejudicial, or from serious to prejudicial.

d. Declassification means to terminate the classification. Downgrading is appropriate when, on the basis of a current judgment of the present and future United States national defense interests, the degree of possible harm to those interests is less than prejudicial.

e. The factors applied to command and control of cation are the same as those used for classification in the first instance. With the passage od time, changes in the state of the art, and other changes in the circumstances which justified the original classification or a later reduced level of classification, a new curerent judgment is made in the light of the now current situation, all relevant things considered.

f. The passage or time, in and of itself, is not in any case a completely sufficient reason for downgrading or declassification. On the other hand, the passage of time is always important because of the inevitable connotation that during the passage of time the circumstances and conditions originally justifying classification, or reduced classification, have themselves changed.

g. It has always been a policy that at the time of original classification, the original classifier would endeavor to visualize a future situation in which downgrading or declassification could and should occur. The purpose would be to try to bring about downgrading or declassification at the earliest reasonable and feasible time, and to achieve this result if per chance the action did not earlier result from review and reevaluation. In other words, if a specific event, or date, or period of time can be identified, the downgrading or declassification process can be made to occur automatically upon the occurrence of the selected factor or factors.

h. Unless the original classifier establishes the conditions for automatic downgrading and declassification and signifies those conditions by markings intended to put the future custodian immediately on notice, the level of classification as originally determined, or as reduced, will continue without change until the process of review and reevaluation occurs and the appropriate downgrading or declassification action is determined and ordered.

i. A determination to classify must be accompanied by a classification designation directly and immediately associated with the information involved. On documents, this designation is achieved by the marking "Top Secret," "Secret," or "Confidential." These markings are not authorized to be changed or removed except as an incident of downgrading or declassification.

j. An essential part of a completed downgrading or declassification action is a change in, or cancellation of, the current designation. Even if a judgment to downgrade or declassify has been made, the judgment cannot be made effective without the appropriate change, or cancellation of, the current designation.

k. Downgrading or declassification can occur at any time. Review and reevaluation can occur at any time. The system contains requirements for continuous review and reevaluation, and also for review and reevaluation on a systematic and orderly basis. It is difficult administratively to achieve the officially desired frequency of review and reevaluation.

l. In connection with making a response to a request for information which currently is classified, a review and reevaluation of the information would be needed if the requester was not eligible, by personal security clearance and by officially determined need to have the information, to be given access to that information at its current level of classification.

6. That the time-phased system of automatic downgrading and declassification established by EO 10501 as amended by EO 10964 and as implemented in DoD by DoD directive 5200.10, provides for four categories or groups numbered from one through four. For groups 1, 3, and 4, there is no necessary relationship between a level of classification, TS, S or C, and the particular group. Thus, TOP SECRET, as well as SECRET or CONFIDENTIAL information can be placed in either group 1, 3, or 4. Group 2 information, however, is used for only very sensitive information, and may be applied only on a unit basis, such as, document by document. The classification level of group 2 information must always be either TS or S.

a. Group 1 information is excluded from the automatic system. Information which is not completely within the exclusive original security classification jurisdiciton made of the DoD must be placed in group 1. Thus, classified information made available to the DoD by another agency of the United States Government, such as the Department of State or The Central Intelligence Agency, or by a foreign nation or international organization, must be placed in group 1 regardless of its level of classification. Some group 1 information is within the exclusive jurisdiction of DoD. Group 1 information is never automatically downgraded or declassified. If not within exclusive DoD jurisdiction, it can be downgraded or declassified only with the combined action of the original classifier and the DoD.

b. Group 3 information is subject to automatic downgrading on a 12-year, time-phased basis. TS becomes S in 12 years, and S becomes C in 12 years. There is no automatic declassification.

c. Group 4 information is subject to automatic downgrading and declassification on the prescribed time basis of reducing one level in 3 years and becoming automatically declassified after 12 years from date of origin. Thus, TS would become S in three years, S would become C in three more years, and declassification would occur in 6 more years, a total of 12. Information starting at S or C would become declassified only after the passage of a total of 12 years from date of origin.

7. That original classification is very different from derivative classification. Original classification is determined by the original classifier in relation to his judgment of the current interests of United States national defense. After the original classification, all custodians are bound by the classification originally imposed, until and unless changed by the original classifier or by those duly authorized to act for him. Within the DoD, the authority for original classification, downgrading and declassification is exercised within a vertical channel of command or supervision. Any higher official in a vertical channel of command or supervision may change a classification imposed at a lower level, or act in lieu of a classifier at a lower level. The exercise of original classification is controlled by the Secretary of Defense or his designee, the Assistant Secretary of Defense (Administration). At the TS level, the number of officials vested with original classification authority is relatively few and is precisely specified on the basis of official positions. Many more officials have original classifying authority at the S and C levels, generally determined by the necessities of the particular positions and responsibilities held as veri-

fied by appropriate authority.

8. That the original classifying authority not only determines the level of classification, as TS, S or C. He also is required to establish the group for automatic downgrading and declassification purposes. A custodian holding only derivative classification authority with respect to the information in question is authorized, however, if a group marking has not been made, to establish the correct group and put the appropriate group marking on the document in accordance with the rules under which the original classifier exercised his authority.

9. That the classification of documents is required to be determined on the basis of the content of the particular document. Within any document there may be classified as well as unclassified portions, and there may be portions classified at different levels from other portions. The document as an entirety, however, carries only one overall classification, and that classification must be the same as that portion of the document bearing the highest level of classification. When two or more documents are combined together to make a single package, the overall classification of the total package would depend upon not only the highest level of classification of any portion of material in either of the parts of the package, but also upon the question whether putting the two or more parts together into a single package gives rise to information which in itself merits a higher classification than any part within the total package. On this principle, it is sometimes necessary to classify a document in which no single piece or part is itself classified.

10. That when a new document is prepared from two or more source documents, it is sometimes very difficult, if not impossible, to sort out the individual portions of the new document in relation to specific sources for the purpose of endeavoring to identify specific portions of the new document which can be determined to be unclassified. For example, if source documents were supplied to the DoD by the Department of State or the Central Intelligence Agency, or by a foreign nation, and from those several sources a new document was prepared as an original composition, it is absolutely certain that the new original composition would have to carry the classification level of the highest classified portion of any source document which had been carried into the final new composition.

11. That under the foregoing system, certain necessary conclusions follow. Within DoD, an original TS classification determination must be made by an official specifically vested with that authority, and subsequent downgrading and declassification of TS information must be determined by that same authority unless another official has been duly designated to take that action. Further, when classified information at any level is entrusted by another agency of the United States Government to the DoD, no official in the DoD may reduce or cancel that classification except in concert with and by authority of the other agency exercising the original classifying authority.

12. That it is appropriate to repeat with emphasis that classification, downgrading and declassification determinations under EO 10501 as amended as implemented by the DoD must be made in terms of the current and future national defense interests of the United States, whether those interests are related in one case to the international posture of the United States in relation to other nations, or in another case to a particular weapons system or intelligence gathering or collection system or to intelligence sources and methods, or to plans for current or future military operations. Further, classification, downgrading and declassification always depend upon a judgment currently made as to the immediate and future national defense interests of the United States.

13. That, based upon information and belief and my understanding, and pursuant to EO 10501, as amended, DoD Instruction 5210.47, and DoD Directive 5200.10, the required classification of the study entitled "United States—Vietnam Relations 1945-1967," as a single package document consisting of 47 volumes, based upon and derived from miscellaneous source materials some of which were prepared and classified Top Secret by original classifying authorities outside of the DoD and some of which were prepared and classified Top Secret by original classifying authorities within the DoD, at the time of completion of the study was, and now is, Top Secret.

DEPARTMENTAL REGULATIONS; SEC. 301 TITLE 5 U.S.C.

§ 301. Departmental regulations.

The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. This section does not authorize withholding information from the public or limiting the availability of records to the public. (Pub. L. 89-554, Sept. 6, 1966, 80 Stat. 379.)

HISTORICAL AND REVISION NOTES

Derivation	*U.S. Code*	*Revised Statutes and Statutes at Large*
----	5 U.S.C. 22	R.S. § 161. Aug. 12, 1958, Pub. L. 85-619, 72 Stat. 547.

The words "Executive department" are substituted for "department" as the definition of "department" applicable to this section is coextensive with the definition of "Executive department" in section 101. The words "not inconsistent with law" are omitted as surplusage as a regulation which is inconsistent with law is invalid.

The words "or military department" are inserted to preserve the application of the source law. Before enactment of the National Security Act Amendments of 1949 (63 Stat. 578), the Department of the Army, the Department of the Navy, and the Department of the Air Force were Executive departments. The National Security Act Amendments of 1949 established the Department of Defense as an Executive Department including the Department of the Army, the Department of the Navy, and the Department of the Air Force as military departments, not as Executive departments. However, the source law for this section, which was in effect in 1949, remained applicable to the Secretaries of the military departments by virtue of section 12(g) of the National Security Act Amendments of 1949 (63 Stat. 591), which provided:

SOURCE:
U.S. Laws, Statutes, etc. United States Code. 1964 ed., supplement V, containing the general and permanent laws of the United States enacted during the 89th and 90th Congresses and 91st Congress, first session, January 4, 1965, to January 18, 1970. Prepared and published . . . by the Committee on the Judiciary of the House of Representatives. Washington, U.S. Govt. Print. Off., 1965. (Title 5, government organization and employees, chapter 3, pp. 70-71).

"All laws, orders, regulations, and other actions relating to the National Military Establishment, the Departments of the Army, the Navy, or the Air Force, or to any officer or activity of such establishment or such departments, shall, except to the extent inconsistent with the provisions of this Act, have the same effect as if this Act had not been enacted; but, after the effective date of this Act, any such law, order, regulation, or other action which vested functions in or otherwise related to any officer, department, or establishment, shall be deemed to have vested such function in or relate to the officer or department, executive or military, succeeding the officer, department, or establishment in which such function was vested. For purposes of this subsection the Department of Defense shall be deemed the department succeeding the National Military Establishment, and the military departments of Army, Navy, and Air Force shall be deemed the departments succeeding the Executive Departments of Army, Navy, and Air Force."

This section was part of title IV of the Revised Statutes. The Act of July 26, 1947, ch. 343, § 201(d), as added Aug. 10, 1949, ch. 412, § 4, 63 Stat. 579 (former 5 U.S.C. 171-1), which provides "Except to the extent inconsistent with the provisions of this Act [National Security Act of 1947], the provisions of title IV of the Revised Statutes as now or hereafter amended shall be applicable to the Department of Defense" is omitted from this title but is not repealed.

Standard changes are made to conform with the definitions applicable and the style of this title as outlined in the preface to the report.

FREEDOM OF INFORMATION ACT; P.L. 89-487

SOURCE:
U.S. Laws, Statutes, etc. An act to amend section 3 of the Administrative Procedure Act, chapter 324 of the act of June 11, 1946 (60 stat. 238), to clarify and protect the right of the public to information, and for other purposes [Freedom of Information Act]. Approved July 4, 1966. [Washington, U.S. Govt. Print. Off., 1966], [2] p. (Public law 487, 89th Congress, 80 stat. 250).

Public Law 89-487

July 4, 1966
[S. 1160]

AN ACT

To amend section 3 of the Administrative Procedure Act, chapter 324, of the Act of June 11, 1946 (60 Stat. 238), to clarify and protect the right of the public to information, and for other purposes.

Public information, availability, 5 USC 1002.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 3, chapter 324, of the Act of June 11, 1946 (60 Stat. 238), is amended to read as follows:

"SEC. 3. Every agency shall make available to the public the following information:

"(a) PUBLICATION IN THE FEDERAL REGISTER.—Every agency shall separately state and currently publish in the Federal Register for the guidance of the public (A) descriptions of its central and field organization and the established places at which, the officers from whom, and the methods whereby, the public may secure information, make submittals or requests, or obtain decisions; (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available; (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations; (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and (E) every amendment, revision, or repeal of the foregoing. Except to the extent that a person has actual and timely notice of the terms thereof, no person shall in any manner be required to resort to, or be adversely affected by any matter required to be published in the Federal Register and not so published. For purposes of this subsection, matter which is reasonably available to the class of persons affected thereby shall be deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

"(b) AGENCY OPINIONS AND ORDERS.—Every agency shall, in accordance with published rules, make available for public inspection and copying (A) all final opinions (including concurring and dissenting opinions) and all orders made in the adjudication of cases, (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register, and (C) administrative staff manuals and instructions to staff that affect any member of the public, unless such materials are promptly published and copies offered for sale. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction: *Provided*, That in every case the justification for the deletion must be fully explained in writing. Every agency also shall maintain and make available for public inspection and copying a current index providing identifying information for the public as to any matter which is issued, adopted, or promulgated after the effective date of this Act and which is required by this subsection to be made available or published. No final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects any member of the public may be relied upon, used or cited as precedent by an agency against any private party unless it has been indexed and either

made available or published as provided by this subsection or unless that private party shall have actual and timely notice of the terms thereof.

"(c) AGENCY RECORDS.—Except with respect to the records made available pursuant to subsections (a) and (b), every agency shall, upon request for identifiable records made in accordance with published rules stating the time, place, fees to the extent authorized by statute and procedure to be followed, make such records promptly available to any person. Upon complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated shall have jurisdiction to enjoin the agency from the withholding of agency records and to order the production of any agency records improperly withheld from the complainant. In such cases the court shall determine the matter de novo and the burden shall be upon the agency to sustain its action. In the event of noncompliance with the court's order, the district court may punish the responsible officers for contempt. Except as to those causes which the court deems of greater importance, proceedings before the district court as authorized by this subsection shall take precedence on the docket over all other causes and shall be assigned for hearing and trial at the earliest practicable date and expedited in every way.

"(d) AGENCY PROCEEDINGS.—Every agency having more than one member shall keep a record of the final votes of each member in every agency proceeding and such record shall be available for public inspection.

"(e) EXEMPTIONS.—The provisions of this section shall not be applicable to matters that are (1) specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy; (2) related solely to the internal personnel rules and practices of any agency; (3) specifically exempted from disclosure by statute; (4) trade secrets and commercial or financial information obtained from any person and privileged or confidential; (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a private party in litigation with the agency; (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; (7) investigatory files compiled for law enforcement purposes except to the extent available by law to a private party; (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions; and (9) geological and geophysical information and data (including maps) concerning wells.

"(f) LIMITATION OF EXEMPTIONS.—Nothing in this section authorizes withholding of information or limiting the availability of records to the public except as specifically stated in this section, nor shall this section be authority to withhold information from Congress.

"(g) PRIVATE PARTY.—As used in this section, 'private party' means any party other than an agency.

"(h) EFFECTIVE DATE.—This amendment shall become effective one year following the date of the enactment of this Act."

Approved July 4, 1966.

CONTROL OF INFORMATION (AEC); SECS. 2161-2-66 TITLE 42 U.S.C.

SUBCHAPTER XI.—CONTROL OF INFORMATION

PRIOR PROVISIONS

Provisions similar to those comprising this subchapter were contained in section 10 of act Aug. 1, 1946, ch. 724, 60 Stat. 755 (formerly classified to section 1810 of this title), prior to the complete amendment and renumbering of act Aug. 1, 1946 by act Aug. 30, 1954, 9:44 a. m., E. D. T., ch. 1073, 68 Stat. 921.

§ 2161. Policy of Commission.

It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. Consistent with such policy, the Commission shall be guided by the following principles:

(a) Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 2164 of this title; and

(b) The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information. (Aug. 1, 1946, ch. 724, § 141, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 940.)

SOURCE:

U.S. Laws, statutes, etc. United States code. 1964 ed., containing the general and permanent law of the United States, in force on January 3, 1965. Prepared and published . . .by the Committee on the Judiciary of the House of Representatives. Washington, U.S. Govt. Print. Off., 1965. (v. 9, title 42 public health and welfare, subchapter 11, pages 8070-8073).

§ 2162. Classification and declassification of Restricted Data.

(a) Periodic determination.

The Commission shall from time to time determine the data, within the definition of Restricted Data, which can be published without undue risk to the common defense and security and shall thereupon cause such data to be declassified and removed from the category of Restricted Data.

(b) Continuous review.

The Commission shall maintain a continuous review of Restricted Data and of any Classification Guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data which have been declassified in order to determine which information may be declassified and removed from the category of Restricted Data without undue risk to the common defense and security.

(c) Joint determination on atomic weapons; Presidential determination on disagreement.

In the case of Restricted Data which the Commission and the Department of Defense jointly determine to relate primarily to the military utilization of atomic weapons, the determination that such data may be published without constituting an unreasonable risk to the common defense and security shall be made by the Commission and the Department of Defense jointly, and if the Commission and the Department of Defense do not agree, the determination shall be made by the President.

(d) Same; removal from Restricted Data category.

The Commission shall remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and Department of Defense jointly determine can be adequately safeguarded as defense information: *Provided, however,* That no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with section 2164 (b) of this title.

(e) Joint determination on atomic energy programs.

The Commission shall remove from the Restricted Data category such information concerning the

atomic energy programs of other nations as the Commission and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 403 (d) of Title 50 and can be adequately safeguarded as defense information. (Aug. 1, 1946, ch. 724, § 142, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 941.)

EX. ORD. NO. 10899. COMMUNICATION OF RESTRICTED DATA BY CENTRAL INTELLIGENCE AGENCY

Ex. Ord. No. 10899, Dec. 9, 1960, 25 F.R. 12729, provided:

By virtue of the authority vested in me by the Atomic Energy Act of 1954, as amended (hereinafter referred to as the Act; 42 U.S.C. 2011 *et seq.*) [this chapter], and as President of the United States, it is ordered as follows:

The Central Intelligence Agency is hereby authorized to communicate for intelligence purposes, in accordance with the terms and conditions of any agreement for cooperation arranged pursuant to subsections 144 a, b, or c of the act (42 U.S.C. 2162 (a), (b), or (c)), such restricted data and data removed from the restricted data category under subsection 142d of the Act (42 U.S.C. 2162(d)) [subsection (d) of this section] as is determined

(i) by the President, pursuant to the provisions of the Act, or

(ii) by the Atomic Energy Commission and the Department of Defense, jointly pursuant to the provisions of Executive Order No. 10841 [set out as a note under section 2153 of this title], to be transmissible under the agreement for cooperation involved. Such communications shall be effected through mechanisms established by the Central Intelligence Agency in accordance with the terms and conditions of the agreement for cooperation involved: *Provided*, that no such communication shall be made by the Central Intelligence Agency until the proposed communication has been authorized either in accordance with procedures adopted by the Atomic Energy Commission and the Department of Defense and applicable to conduct of programs for cooperation by those agencies, or in accordance with procedures approved by the Atomic Energy Commission and the Department of Defense and applicable to conduct of programs for cooperation by the Central Intelligence Agency.

DWIGHT D. EISENHOWER

EX. ORD. NO. 11057. COMMUNICATION OF RESTRICTED DATA BY DEPARTMENT OF STATE

Ex. Ord. No. 11057, Oct. 18, 1962, 27 F.R. 10289, provided:

By virtue of the authority vested in me by the Atomic Energy Act of 1954, as amended (hereinafter referred to as the Act; 42 U.S.C. 2011 et seq.) [this chapter], and as President of the United States, it is ordered as follows:

The Department of State is hereby authorized to communicate, in accordance with the terms and conditions of any agreement for cooperation arranged pursuant to subsection 144b of the act (42 U.S.C. 2164(b)), such restricted data and data removed from the restricted data category under subsection 142d of the act (42 U.S.C. 2162(d)) [subsec. (d) of this section] as is determined

(i) by the President, pursuant to the provisions of the Act, or

(ii) by the Atomic Energy Commission and the Department of Defense, jointly pursuant to the provisions of Executive Order No. 10841, as amended [set out as a note under section 2153 of this title], to be transmissible under the agreement for cooperation involved. Such communications shall be effected through mechanisms established by the Department of State in accordance with the terms and conditions of the agreement for cooperation involved: *Provided*, that no such communication shall be made by the Department of State until the proposed communication has been authorized either in accordance with procedures adopted by the Atomic Energy Commission and the Department of Defense and applicable to conduct of programs for cooperation by those agencies, or in accordance with procedures approved by the Atomic Energy Commission and the Department of Defense and applicable to conduct of programs for cooperation by the Department of State.

JOHN F. KENNEDY

§ 2163. Access to Restricted Data.

The Commission may authorize any of its employees, or employees of any contractor, prospective contractor, licensee or prospective licensee of the Commission or any other person authorized access to Restricted Data by the Commission under section 2165 (b) and (c) of this title to permit any employee of an agency of the Department of Defense or of its contractors, or any member of the Armed Forces to have access to Restricted Data required in the performance of his duties and so certified by the head of the appropriate agency of the Department of Defense or his designee: *Provided, however*, That, the head of the appropriate agency of the Department of Defense or his designee has determined, in accordance with the established personnel security procedures and standards of such agency, that permitting the member or employee to have access to such Restricted Data will not endanger the common defense and security: *And provided further*, That the Secretary of Defense finds that the established personnel and other security procedures and standards of such agency are adequate and in reasonable conformity to the standards established by the Commission under section 2165 of this title. (Aug. 1, 1946, ch. 724, § 143, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 941, and amended Aug. 6, 1956, ch. 1015, § 14, 70 Stat. 1071; Sept. 6, 1961, Pub. L. 87-206, § 5, 75 Stat. 476.)

AMENDMENTS

1961—Pub. L. 87-206 inserted the reference to subsection (c) of section 2165 of this title.

1956—Act Aug. 6, 1956, inserted between the words "licensee of the Commission" and the words "to permit any employee" the words "or any other person authorized access to Restricted Data by the Commission under section 2165(b) of this title".

§ 2164. International cooperation.

(a) By Commission.

The President may authorize the Commission to cooperate with another nation and to communicate to that nation Restricted Data on—

(1) refining, purification, and subsequent treatment of source material;

(2) civilian reactor development;

(3) production of special nuclear material;

(4) health and safety;

(5) industrial and other applications of atomic energy for peaceful purposes; and

(6) research and development relating to the foregoing:

Provided, however, That no such cooperation shall involve the communication of Restricted Data relating to the design or fabrication of atomic weapons: *And provided further*, That the cooperation is undertaken pursuant to an agreement for cooperation entered into in accordance with section 2153 of this title, or is undertaken pursuant to an agreement existing on August 30, 1954.

(b) By Department of Defense.

The President may authorize the Department of Defense, with the assistance of the Commission, to cooperate with another nation or with a regional defense organization to which the United States is a

party, and to communicate to that nation or organization such Restricted Data (including design information) as is necessary to—

(1) the development of defense plans;

(2) the training of personnel in the employment of and defense against atomic weapons and other military applications of atomic energy;

(3) the evaluation of the capabilities of potential enemies in the employment of atomic weapons and other military applications of atomic energy; and

(4) the development of compatible delivery systems for atomic weapons;

whenever the President determines that the proposed cooperation and the proposed communication of the Restricted Data will promote and will not constitute an unreasonable risk to the common defense and security, while such other nation or organization is participating with the United States pursuant to an international arrangement by substantial and material contributions to the mutual defense and security: *Provided, however,* That the cooperation is undertaken pursuant to an agreement entered into in accordance with section 2153 of this title.

(c) Exchange of information concerning atomic weapons; research, development, or design, of military reactors.

In addition to the cooperation authorized in subsections (a) and (b) of this section, the President may authorize the Commission, with the assistance of the Department of Defense, to cooperate with another nation and—

(1) to exchange with that nation Restricted Data concerning atomic weapons: *Provided,* That communication of such Restricted Data to that nation is necessary to improve its atomic weapon design, development, or fabrication capability and provided that nation has made substantial progress in the development of atomic weapons; and

(2) to communicate or exchange with that nation Restricted Data concerning research, development, or design, of military reactors,

whenever the President determines that the proposed cooperation and the communication of the proposed Restricted Data will promote and will not constitute an unreasonable risk to the common defense and security, while such other nation is participating with the United States pursuant to an international arrangement by substantial and material contributions to the mutual defense and security: *Provided, however,* That the cooperation is undertaken pursuant to an agreement entered into in accordance with section 2153 of this title.

(d) Communication of data by other Governmental agencies.

The President may authorize any agency of the United States to communicate in accordance with the terms and conditions of an agreement for cooperation arranged pursuant to subsection (a), (b), or (c) of this section, such Restricted Data as is determined to be transmissible under the agreement for cooperation involved. (Aug. 1, 1946, ch. 724, § 144, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 942, and amended July 2, 1958, Pub. L. 85–479, §§ 5–7, 72 Stat. 278.)

AMENDMENTS

1958—Subsec. (a). Pub. L. 85–479, § 5, substituted "civilian reactor development" for "reactor development" in cl. (2).

Subsec. (b). Pub. L. 85–479, § 6, authorized communication of design information, of data concerning other military applications of atomic energy necessary for the training of personnel or for the evaluation of the capabilities of potential enemies, and of data necessary to the development of compatible delivery systems for atomic weapons, and eliminated provisions which prohibited communication of data which would reveal important information concerning the design or fabrication of the nuclear components of atomic weapons.

Subsecs. (c) and (d). Pub. L. 85–479, § 7, added subsecs. (c) and (d).

§ 2165. Security restrictions.

(a) On contractors and licensees.

No arrangement shall be made under section 2051 of this title, no contract shall be made or continued in effect under section 2061 of this title, and no license shall be issued under section 2133 or 2134 of this title, unless the person with whom such arrangement is made, the contractor or prospective contractor, or the prospective licensee agrees in writing not to permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(b) Employment of personnel; access to Restricted Data.

Except as authorized by the Commission or the General Manager upon a determination by the Commission or General Manager that such action is clearly consistent with the national interest, no individual shall be employed by the Commission nor shall the Commission permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(c) Acceptance of investigation and clearance granted by other Government agencies.

In lieu of the investigation and report to be made by the Civil Service Commission pursuant to subsection (b) of this section, the Commission may accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individual by another Government agency based on such investigation and report.

(d) Investigations by FBI.

In the event an investigation made pursuant to subsections (a) and (b) of this section develops any data reflecting that the individual who is the subject of the investigation is of questionable loyalty, the Civil Service Commission shall refer the matter to the Federal Bureau of Investigation for the conduct of a full field investigation, the results

of which shall be furnished to the Civil Service Commission for its information and appropriate action.

(e) Same; Presidential investigation.

If the President deems it to be in the national interest, he may from time to time determine investigations of any group or class which are required by subsections (a), (b), and (c) of this section to be made by the Federal Bureau of Investigation.

(f) Certification of specific positions for investigation by FBI.

Notwithstanding the provisions of subsections (a), (b), and (c) of this section, a majority of the members of the Commission shall certify those specific positions which are of a high degree of importance or sensitivity and upon such certification the investigation and reports required by such provisions shall be made by the Federal Bureau of Investigation.

(g) Investigation standards.

The Commission shall establish standards and specifications in writing as to the scope and extent of investigations, the reports of which will be utilized by the Commission in making the determination pursuant to subsections (a), (b), and (c) of this section, that permitting a person access to restricted data will not endanger the common defense and security. Such standards and specifications shall be based on the location and class or kind of work to be done, and shall, among other considerations, take into account the degree of importance to the common defense and security of the restricted data to which access will be permitted.

(h) War time clearance.

Whenever the Congress declares that a state of war exists, or in the event of a national disaster due to enemy attack, the Commission is authorized during the state of war or period of national disaster due to enemy attack to employ individuals and to permit individuals access to Restricted Data pending the investigation report, and determination required by subsection (b) of this section to the extent that and so long as the Commission finds that such action is required to prevent impairment of its activities in furtherance of the common defense and security. (Aug. 1, 1946, ch. 724, § 145, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 942, and amended Aug. 19, 1958, Pub. L. 85-681, § 5, 72 Stat. 633; Sept. 6, 1961, Pub. L. 87-206, § 6, 75 Stat. 476; Aug. 29, 1962, Pub. L. 87-615, § 10, 76 Stat. 411.)

AMENDMENTS

1962—Subsec. (f). Pub. L. 87-615 deleted the comma following "investigation".

1961—Subsec. (c). Pub. L. 87-206 added subsec. (c) Former subsec. (c) redesignated (d).

Subsec. (d). Pub. L. 87-206 redesignated former subsec (c) as (d). Former subsec. (d) redesignated (e).

Subsec. (e). Pub. L. 87-206 redesignated former subsec (d) as (e) and amended the provisions by substituting "determine that" for "cause investigations", inserting reference to subsection (c) of this section and eliminating "instead of by the Civil Service Commission" following "Federal Bureau of Investigation." Former subsec. (e) redesignated (f).

Subsec. (f). Pub. L. 87-206 redesignated former subsec (e) as (f) and amended the provisions by inserting reference to subsection (c) of this section and eliminating "instead of by the Civil Service Commission" following "Federal Bureau of Investigation." Former subsec. (f) redesignated (g).

Subsec. (g). Pub. L. 87-206 redesignated former subsec. (f) as (g) and amended the provisions by substituting ", the reports of which will be utilized by the Commission in making the determination, pursuant to subsections (a), (b), and (c) of this section, that permitting a person access to restricted data will not endanger the common defense and security" for "to be made by the Civil Service Commission pursuant to subsections (a) and (b) of this section." Former subsec. (g) redesignated (h).

Subsec. (h). Pub. L. 87-206 redesignated former subsec. (g) as (h).

1958—Subsec. (g). Pub. L. 85-681 added subsec. (g).

CROSS REFERENCE

Arms control and disarmament security restrictions, see section 2585 of Title 22, Foreign Relations and Intercourse.

§ 2166. Applicability of other laws.

(a) Sections 2161—2165 of this title shall not exclude the applicable provisions of any other laws, except that no Government agency shall take any action under such other laws inconsistent with the provisions of those sections.

(b) The Commission shall have no power to control or restrict the dissemination of information other than as granted by this or any other law. (Aug. 1, 1946, ch. 724, § 146, as added Aug. 30, 1954, ch. 1073, § 1, 68 Stat. 943.)

SECURITY REGULATIONS: PHYSICAL AND PROCEDURAL
(State Department/AID/USIA); Selected excerpts

UNIFORM STATE/AID/USIA REGULATIONS

900 - Physical and Procedural Security

901 Policy

901.1 Interests of National Defense

The interests of national defense require the preservation of the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action. Therefore, certain official information *including that in the field of foreign relations* affecting the national defense must be protected against unauthorized disclosure. *(See section 911.2.)*

901.2 Safeguarding Official Information

Executive Order No. 10501 of November 5, 1953 (18 F.R. 7047), as amended (note following 50 U.S.C. 401), provides for the safeguarding of official information which requires protection in the interests of national defense. *For the types of foreign policy information which may fall within the criteria of national defense, see sections 911.2 and 911.4.*

**901.3 Safeguarding Other Official Information

The Freedom of Information Act (5 U.S.C. 552) recognizes the necessity for the Government to withhold from public disclosure certain categories of records in addition to those containing information specified in Executive Order 10501 and other Executive Orders. These include, but are not limited to, records the disclosure of which would be a clearly unwarranted invasion of personal privacy or would violate a privileged relationship.

The absence of a security classification or an administrative control designation on a record should not be regarded as authorizing the public disclosure of information contained therein without independent consideration of the appropriateness of the disclosure. In this regard, Department and Agency policy with respect to disclosure of information under the Freedom of Information Act, or otherwise, does not alter the individual's responsibility arising from his employment relationship with the Department or Agency.**

SOURCE: U.S. Department of State. Uniform State/AID/USIA security regulations, physical and procedural. [Washington, U.S. Govt. Print. Off.] 1969. 1 v. (various pagings)

901.4 Limitation

The requirement to safeguard information in the national defense interest and in order to protect sources of privileged information in no way implies an indiscriminate license to restrict information from the public. It is important that the citizens of the United States have the fullest possible access, consistent with security and integrity, to information concerning the policies and programs of their Government.

901.5 Scope

These regulations prescribe the security rules for classifying, marking, reproducing, handling, transmitting, disseminating, storing, regrading, declassifying, decontrolling, and destroying official material in accordance with its relative importance. They are intended to ensure accurate and uniform classification of such information and to establish standards for its protection, as required by Executive Order 10501.

901.6 Responsibility

a. Primary

The specific responsibility for the maintenance of the security of classified or controlled information rests with each person having knowledge or physical custody thereof, no matter how obtained.

b. Individual

Each employee is responsible for familiarizing himself with and adhering to all security regulations.

c. Supervisory

The ultimate responsibility for safeguarding classified and administratively controlled information as prescribed in these regulations rests upon each supervisor to the same degree that he is charged with functional responsibility for his organizational unit. Supervisors may, however, delegate the performance of any or all of these functions relating to the safeguarding of material.

d. Organizational

The Offices of Security in State, USIA, and A.I.D. are responsible for physical and personnel security in their respective agencies. The Office of Communications in the Department of State is responsible for cryptographic security. For administration and enforcement, see section 990.

**e. Limitation

Responsibility for safeguarding classified and controlled information and records shall not be construed as authority to determine whether records may be withheld from the public when requests for their disclosure are made under the Freedom of Information Act (5 U.S.C. 552). Such requests must be referred in the manner described in section 943.2 for processing in accordance with applicable agency regulations. (State, 5 FAM 480; A.I.D., M.O. 820.1; USIA, 22 CFR 503.5-503.7.)**

910 CLASSIFICATION AND CONTROL OF INFORMATION AND MATERIAL

911 Authorized Classifications

911.1 Classification Categories

Classification of official information requiring protection in the interests of national defense shall be limited to one of the three authorized categories of classification, which in descending order of importance are: Top Secret, Secret, and Confidential. No other classification shall be used to identify defense information, including military information, requiring protection in the interests of national defense, except as expressly provided by statute.

911.2 Defense *and Foreign Policy * Information

The Attorney General of the United States on April 17, 1954, advised that defense classifications may be interpreted, in proper instances, to include the safeguarding of information and material developed in the course of conduct of foreign relations of the United States whenever it appears that the effect of the unauthorized disclosure of such information or material upon international relations or upon policies being pursued through diplomatic channels could result in serious damage to the Nation. The Attorney General further noted that it is a fact that there exists an interrelation between the foreign relations of the United States and the national defense of the United States, which fact is recognized in section 1 of Executive Order 10501. Illustrative examples of such information which may require classification include but are not confined to:

a. Information and material relating to cryptographic devices and systems.

b. Information pertaining to vital defense or diplomatic programs or operations.

c. Intelligence or information relating to intelligence operations which will assist the United States to be better prepared to defend itself against attack or to conduct foreign relations.

d. Information pertaining to national stockpiles, requirements for strategic materials, critical products, technological development, or testing activities vital to national defense.

e. Investigative reports which contain information relating to subversive activities affecting the internal security of the United States.

f. Political and economic reports containing information, the unauthorized disclosure of which may jeopardize the international relations of the United States or may otherwise affect the national defense.

g. Information received in confidence from officials of a foreign government whenever it appears that the breach of such confidence might have serious consequences affecting the national defense or foreign relations.

911.3 Classification of Defense Information

911.3-1 Top Secret

Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized by an appropriate official only for defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense or diplomatic aspect of which is paramount and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation, such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military defense plans, intelligence operations, or scientific or technological developments vital to the national defense.

911.3-2 Secret

Except as may be expressly provided by statute, the use of the classification Secret shall be authorized by an appropriate official only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as jeopardizing the international relations of the United States or its allies, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important diplomatic or intelligence operations.

911.3-3 Confidential

Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by an appropriate official, only for defense information or material the unauthorized disclosure of which could be prejudicial to the conduct of United States foreign relations or the defense interests of the Nation.

911.3-4 Unclassified

Normally, unclassified material should not be marked or stamped "Unclassified" unless it is essential to convey to its recipient that it has been examined specifically for the need of a defense classification or control designation and has been determined not to require such classification or control. However, preprinted forms such as telegrams, which make provision for an assigned classification, shall include the term "Unclassified" if the information contained the text is neither classified nor administratively controlled.
Envelopes containing unclassified information to be sent by diplomatic pouch must be marked or stamped "UNCLASSIFIED" on both sides. (See section 956.5b.)

911.4 Authorized Administrative Control Designation

911.4-1 Limited Official Use

The administrative control designation Limited Official Use is authorized to identify *non-classified information which requires physical protection comparable to that given "Confidential" material in order to safeguard it* from unauthorized access. Matters which should be administratively controlled include information received through privileged sources certain personnel, medical, investigative *commercial, and financial* records; specific references to contents of diplomatic pouches; and other similar material.

Documents which routinely would be made available to the public upon request pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552) should not be administratively controlled. See State, 5 FAM 480; A.I.D., M.O. 820.1; USIA, M.O.A. III 526.

911.5 Restricted Data

a. "Restricted Data" is a term used in connection with atomic energy matters. Section 11r of the Atomic Energy Act of 1954 defines Restricted Data as follows:

> "The term 'Restricted Data' means all data concerning:
>
> "(1) Design, manufacture, or utilization of atomic weapons;
>
> "(2) The production of special nuclear material; or
>
> "(3) The use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data Category."

b. Restricted Data shall be classified Top Secret, Secret, or Confidential. Before any person may be permitted to have access to Restricted Data, he must have a "Q" clearance from, or the special permission of, the Atomic Energy Commission. Nothing in these regulations shall be construed as superseding any requirements of the Atomic Energy Act of 1954. Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954 and the regulations of the Atomic Energy Commission.

c. A cover sheet, JF-42, Restricted Data, bearing the appropriate defense classification top and bottom, shall be used to cover each copy of each document marked "Restricted Data." (See Appendix V (p. 18.)

911.6 Limitations

No other security classification or administrative control designation shall be used on documents originating in the Department, USIA, and A.I.D. without the specific approval of the appropriate Office of Security.

912 Principles of Classification and Control

912.1 Assigning a Classification or Control Designation

a. The originator of a document is responsible for the original assignment of its classification or control designation. Documents or materials shall be classified or controlled according to their own content and not necessarily according to their relationship to other documents. Each document or item of material shall be assigned the lowest classification or control designation consistent with the proper protection of the information in it. *Documents or material containing references to classified material which do not themselves reveal classified information are not to be classified. (See sections 912.2 and 912.3.)*

b. The practice of assigning to a document a classification or control designation exceeding the degree of protection required may appear to be a simple, innocuous means of providing extra protection in the interests of security. To the contrary, overclassification and unnecessary control of documents result in the establishment of cumbersome administrative procedures and seriously hamper operations, especially abroad, even to the extent of defeating the purposes for which the documents are intended. Overclassification and unnecessary control cause delays in handling and may preclude the accessibility of documents to personnel who should be working with them.

912.2 Physically Connected Documents

The classification or administrative control designation assigned to a file or group of physically connected documents must be at least as high as that of the most highly classified or controlled document in it. Documents separated from the file are handled in accordance with their individual classification or control designation. A cover sheet, JF-18, Classified or Controlled File, may be placed on the front of each file or group of physically connected documents, marked to indicate the highest classification or control designation it covers, or the front and back of the folder must be stamped or marked according to the highest classification or designation of the combined information contained in it.

912.3 Transmitting Communication

A transmitting communication shall bear a classification or control designation at least as high as the most highly classified or controlled document it covers. The transmitting communication also must be marked with its appropriate group marking. (See section 966.1.)

912.4 Foreign Government Classified Information

Information furnished by a foreign government or by an international organization with restrictions on its dissemination must be protected according to the instructions specified by the foreign government or international organization furnishing the information.

912.5 Multiple Classifications or Control Designations

A document must bear a classification or administrative control designation at least as high as that of its most highly classified or controlled component. Pages, paragraphs, sections, or components may bear different classifications or a control designation, but the document shall bear only one over-all classification or control designation. When separate portions of a document are marked with different classifications or control designations, each portion bearing a single classification or control designation (including "Unclassified") shall be set off with the phrases:

"Begin_____" (Insert classification or designation.)	"End_____" (Insert classification or designation.)

940 SAFEGUARDING AND DISSEMINATION OF CLASSIFIED AND ADMINISTRATIVELY CONTROLLED INFORMATION

941 Principles Governing the Safeguarding of Classified and Controlled Information

941.1 Authorization for Access and Use

Classified or administratively controlled information must be given only to those persons who require and are authorized to receive the information in the course of the performance of their official duties; who have an appropriate and current security clearance; and who have adequate facilities for protection of documents or other tangible matters.

Special and specifically authorized clearances are required for access to information identified as Restricted Data, Cosmic, SEATO, CENTO, Cryptographic, Intelligence, Office of Security, and other information given special protection by law or regulation.

941.2 Need-to-Know Doctrine

A person is not entitled to receive classified or administratively controlled information solely by virtue of his official position or by virtue of having been granted security clearance. The "need-to-know" doctrine shall be enforced at all times in the interest of good security.

941.3 In Conversation

The discussion of classified or administratively controlled information must not be held in the presence or hearing of persons who are not authorized to have knowledge thereof.

Classified or administratively controlled information must not be discussed in telephone conversations.

941.4 Control on Dissemination

The dissemination of classified or administratively controlled information must be carefully controlled at all times. This includes maintenance of adequate records of transmission and receipt and the imposition of strict limitations on the number of copies prepared or reproduced.

941.5 Restriction on Personal Use

Classified or administratively controlled information must not be used for personal interests of any employee and must not be entered in personal diaries or other nonofficial records.

941.6 Access by Foreign National Employees

Classified information must not be dictated to, typed, or otherwise prepared by local employees. This restriction must not be circumvented by the assignment or classifications after a local employee has prepared a particular document. However, when warranted, information collected by local employees and prepared in report form by such employees may receive classification protection by appending such reports to classified transmittal reports prepared by U.S. employees.

Except as noted in sections 941.6-1, 941.6-2, and 941.6-3, classified or administratively controlled information must not be made available to, or left in the custody of, Foreign Service local employees or alien employees resident in the United States; nor will such employees be permitted to attend meetings where classified or administratively controlled information is discussed.

941.6-1 When local employees obtain information from privileged sources or otherwise develop information warranting an administrative control designation or must be given access to administratively controlled information or material originated elsewhere in order to perform their official duties, they may be authorized limited access to such information provided that:

(a) The local employee's U.S. citizen supervisor requests authority to permit access to administratively controlled material in writing, specifying the reasons the employee must have access in order to perform his official duties and describing the type of material, reports, etc., contemplated for access.

(b) The regional security officer concurs in the request, issues a memorandum of limited access, and recommends approval to the principal officer of the post concerned.

(c) The principal officer must authorize the limited access in writing. Such authority shall be reviewed by each succeeding principal officer, and he shall affirm or discontinue such authority as he deems appropriate.

(d) The employee's access is not construed to mean blanket authority to receive administratively controlled information or material. Select local employees authorized to have access to administratively controlled material shall be permitted access only to that type of material specified in paragraph (a) of this section on a strict "need-to-know" basis.

941.6-2 When it is essential that information contained in classified documents (excluding Top Secret) be disseminated to the broadcasting service alien personnel resident in the United States, in order for them to perform their duties, such information must be given verbally. They are prohibited access to Top Secret information and are not authorized visual access to classified documents or material.

**941.6-3 Foreign Service local employees in very limited cases, may be permitted access to Confidential information coming from or to be delivered to the government of the host country. The internal procedures for granting access are the same as those provided in the foregoing parts of section 941.6 with regard to local employee access to administratively controlled material. Almost all instances of use of this authority will involve necessary translations. Access to such material should be allowed only after consideration of the host government's reaction to the particular Foreign Service local employee's having such access. When and where feasible, the local employee should be given such access only after a responsible agency of the host country has indicated it has no objection to the specific local employee's access to the information. **

941.7 Access by Binational Center Grantees

Since appointments of Binational Center grantees are made only upon completion of a full field investigation, classified information that applies to their assignments and is necessary in the performance of their duties may be made available to them. Under no circumstances will classified documents be given to them for retention at a Binational Center. (This authority does not apply to those U.S. citizens appointed locally whose salaries are paid from Binational Center operating funds.)

942 Report of Missing or Comprised Documents

Any employee who discovers that a classified or administratively controlled document is missing must make a prompt report to the Office of Security or regional security officer via his unit or post security officer. In the case of a known or suspected compromise of a Top Secret document or cryptographic material, the report must be made immediately. Telegraphic or oral reports must be followed by a prompt submission ** of a memorandum addressed to the Office of Security or regional security officer, which includes the following information:

a. Complete identification of the material, including, when possible, the date, subject, originator, address, serial or legend markings, classification, and type of material (i.e., telegram, memorandum, airgram, etc.).

b. Where compromise is belived to have occurred, a narrative statement detailing the circumstance which gave rise to the compromise, the unauthorized person who had or may have had access to the material, the steps taken to determine whether compromise in fact occurred and the office or post evaluation of the importance of the material compromised.

c. Where a document is lost or missing, the narrative statement should detail the movements of the material from the time it was received by the post or office, including to whom it was initially delivered; later routings; the persons having access to the material; the time, date, and circumstances under which loss was realized; and the steps taken to locate the material.**

**d. When material is either compromised or missing, identify if possible the person responsible and state the action taken with regard to the person and/or procedures to prevent a recurrence.

Where cryptographic material is involved, a report is also to be made to the Office of Communications (OC/S) using FS-507, Report of Violation of Communications Security. **

943 Official Dissemination

943.1 Distribution to Other Agencies

Classified or administratively controlled material may be sent to other Federal departments or agencies or to officials and committees of Congress or to individuals therein only through established liaison or distribution channels. An exception is permitted when a post transmits classified or administratively controlled material to an office of another U. S. Government agency within the executive branch located outside the United States.

Classified or administratively controlled material originated in another U. S. department or agency must not be communicated to a third department or agency without the consent of the originating department or agency, including material originated in State, USIA, and A. I. D. Such approval must be obtained in writing, and a record of the approval and communication must be maintained by the communicator.

943.2 Referral of Public Requests

**Requests from the public for classified records, whether made to a Department or Agency office within the United States, or to a post abroad, must be referred to the Chief, Records Services Division (State); Director, Information Staff (A. I. D.); or Assistant Director, Office of Public Information (USIA), as appropriate.

Administratively controlled and unclassified records may be released upon approval by chiefs of mission at Foreign Service posts in accordance with 5 FAM 482.2. Administratively controlled and unclassified records abroad of A. I. D. and of USIA may also be released by the A. I. D. country mission director and by the USIA country public affairs officer respectively. See M. O. 820.1 and M. O. A. III 526.

Requests for classified or for administratively controlled records which the chief of mission (for A. I. D., the mission director, or for USIA, the public affairs officer) has declined to make available on his own authority, should be submitted to the appropriate agency, by operations memorandum for State and USIA and by airgram for A. I. D., containing sufficient information to permit consideration of the request..

Classified or administratively controlled records to be made available to the public by the above-identified authorized officers in the United States and abroad must first be declassified or decontrolled in accordance with the provisions of 5 FAM 966.4.

For more detailed procedures on releasing records to the public, see the appropriate Department or Agency regulations. (State, 5 FAM 480, A. I. D., M. O. 820.1; USIA, M. O. A. III 526.)**

943.3 Clearance for Publication

Any employeee writing for publication, either in an official or private capacity, must submit his manuscript for agency clearance if the content may reasonably be interpreted as related to the current responsibilities, programs, or operations of the employee's agency or to current U.S. foreign policy, or may reasonably be expected to affect U.S. foreign relations. For detailed clearance procedures, see 3 FAM 628 and 1865, M.O. 831.1 and MOA II 120.

943.4 Use of Official Records

The regulations governing access to official records are set forth in 5 FAM 480, M.O. 820.1, and MOA III 526. They include procedures to be followed for access to official records for purposes of historical research.

943.5 Release of Material to U.S. Citizen Personnel Outside the Executive Branch

Classified and administratively controlled material must not be released to persons who are not security cleared U.S. citizen employees of the executive branch of the U.S. Government until appropriate security checks and briefings have been completed. Release of such material or information shall be made only when consistent with security and administrative requirements. Responsibility for authorizing release is vested as follows:

Top Secret, Secret, Confidential, and Limited Official Use Material--The concurrence of both the director of the originating or action office and the director of the Office of Security must be obtained prior to the release of any classified or administratively controlled information. Either the originating or action office concerned with the substance of the information may decide whether it can be declassified or decontrolled and released or whether it can be released without such action. If the information to be released remains classified or administratively controlled, the Office of Security must specify the manner in which the release is to be effected including special markings, receipts, and such other safeguards as are deemed necessary to ensure that the information receives appropriate protection.

943.6 Dissemination Ordered or Requested by a Court of Law or Other Official Body

a. Except as provided in section 943.2, any subpena, demand, or request for classified or controlled information or records from a court of law or other official body shall be handled in accordance with the regulations of the agency concerned which prescribe procedures for responding to subpenas (State, 5 FAM 485; USIA, MOA III 527 and 625.6)

b. Testimony involving classified or administratively controlled information must not be given before a court or other official body without the approval of the head of the Department or Agency concerned. An employee called upon to give such testimony without prior authorization shall state that he is not authorized to disclose the information desired and that a written request for the specific information should be transmitted to the head of the Department or Agency concerned. Such testimony, when so approved, shall be given only under such conditions as the head of the department or agency may prescribe.

c. Reports rendered by the Federal Bureau of Investigation and other investigative agencies of the executive branch are to be regarded as confidential. All reports, records, and files relative to the loyalty of employees or prospective employees (including reports of such investigative agencies) shall be maintained in confidence, and shall not be transmitted or disclosed except as required in the efficient conduct of business, and then, only in accordance with the provisions *of the President's directive of March 13, 1948. (See Appendix II.)*

944 Dissemination to Foreign Governments

944.1 Dissemination of Classified Defense Information to Foreign Governments and International Organizations

For detailed instructions governing the release of classified information to foreign governments and international organizations, see 11 FAM 600.

d. In the domestic service specific approval to remove classified or administratively controlled material for overnight custody must be obtained from an office director or higher authority. At posts, specific approval must be obtained from the principal officer or officers designated by him to approve such removals.

964.3 Transporting Classified and Administratively Controlled Material Across International Borders

Classified and administratively controlled material is carried across international borders by professional diplomatic couriers. Nonprofessional diplomatic couriers are given such material for international transmission only in emergencies when the professional service will not cover the area into which the pouch must be carried or the post to which the pouch is addressed within the time that official business must be conducted. In such isolated cases, the nonprofessional diplomatic courier must be in possession of a diplomatic passport and courier letter, and his material must be enclosed in sealed diplomatic pouches until delivered to its official destination. Special procedures are in effect for U.S.--Mexican border posts.

964.4 Personal Responsibilities

The safeguarding of classified or administratively controlled material removed from official premises remains the personal responsibility of the removing officer even though all conditions of section 964 have been met.

964.5 Office Working or Reference Files

Information and working files accumulated in the course of Government employment are not personal files as defined in section 432, M.O. 520.1, and MOA III Exhibit 610A. The transfer or removal of such working or reference files shall be in accordance with the provisions of sections 417 and 443.2, M.O. 520.1, and MOA III 512.6.

965 STORAGE AND ACCESS OF CLASSIFIED AND ADMINISTRATIVELY CONTROLLED MATERIAL BY PERSONS NOT REGULARLY EMPLOYED

965.1 Storage

Authorized consultants and contractors engaged in work involving classified or administratively controlled material may not store classified or administratively controlled material overnight on their premises unless the Office of Security has granted approval for such storage. No classified or administratively controlled material may be made available to consultants or contractors off the official premises or transmitted to such persons off the premises except with the approval of the Office of Security.

965.2 Access

Contractors or consultants may not have access to classified administratively controlled materials until a personnel security clearance has been given or confirmed by the Office of Security. Employees are personally responsible for obtaining clearance from the Office of Security prior to release or transmitting of classified or administratively controlled material to a consultant or contractor addressee off the premises. Normally, such material is sent through the Office of Security.

966 DOWNGRADING, DECLASSIFICATION, AND DECONTROL

966.1 Automatic Changes

Classified and administratively controlled material should be kept under review and be downgraded, declassified, or decontrolled as soon as conditions permit. When material is assigned a classification or control designation, it must also be assigned a group marking and/or identifying notation to effect its automatic downgrading, declassification, or decontrol when the material no longer requires its original degree of protection. There are five standard group markings and identifying notations associated with the automatic downgrading and declassification of classified material and two identifying notations associated with the automatic decontrol of administratively controlled material. In atypical situations where the standard group markings and notations do not adequately describe the method or time-phase intended to accomplish the automatic downgrading procedure, the notations may be enlarged upon or amended. Group markings and identifying notations should be placed, whenever possible, two spaces above the defense classification or control designation appearing at the bottom of page one on all copies.

966.2 Classified Documents

966.2-1 Group 5 documents are those which do not require a classification protection for any regulatory period of time specified for the protection of documents assigned to Groups 4 through 1. To the greatest extent possible, classified documents that can be assigned to Group 5 should be so assigned and be marked:

> Group 5
> Declassified following _____
> (Date or conclusion of specific event, or removal of classified enclosures or attachments)

966.2-2 Group 4 documents are those requiring protection for a minimum number of years, at the conclusion of which they may be declassified. Group 4 documents are automatically downgraded one step each 3 years and are automatically declassified 12 years after date of origin. Such documents should be marked:

> Group 4
> Downgraded at 3-year intervals.
> Declassified 12 years after date of origin.

966.2-3 Group 3 documents are those which may be automatically downgraded but not automatically declassified. Such documents should be marked:

> Group 3
> Downgraded at 12-year intervals, not automatically declassified.

966.2-4 Group 2 documents are Top Secret and Secret documents which are so extremely sensitive that in the interests of national defense they must retain their classification for an indefinite period of time. Only an official empowered to exercise original Top Secret classification authority may assign a document to Group 2. Such documents must be signed by the exempting official when his identity is not apparent from the document itself and must be marked:

> Group 2
> Exempted from automatic downgrading
> By _____
> (Signature and Title of Exempting Official)

966.2-5 Group 1 documents are those classified documents excluded from the automatic downgrading and declassification provisions because they contain information or material as follows:

a. Originated by foreign governments or international organizations not subject to the classification jurisdiction of the U.S. Government.

b. Provided for by statutes, such as the Atomic Energy Act.

c. Specifically excluded from these provisions by the head of the Department or Agency.

d. Requiring special handling, such as intelligence and cryptography.

Group 1 documents should be marked:

> Group 1
> Excluded from automatic downgrading and declassification.

966.2-6 Administratively Controlled Documents

Limited Official Use documents will be processed in one of two categories: (1) exempted from automatic decontrol or (2) decontrolled upon the conclusion of a specific event, removal of controlled attachments, or the passage of a logical period of time. Such documents must bear an appropriate notation but no group marking and shall be identified as follows:

> Exempted from automatic decontrol.

or

> Decontrolled following _____
> (Date or conclusion of specific event, or removal of administratively controlled enclosures or attachments.)

966.3 Classified and Administratively Controlled Telegrams

Information contained in Top Secret, Secret, Confidential, and Limited Official Use telegrams is subject to automatic downgrading, declassification, and decontrol procedures to the same extent as the substantive contents of nontelegraphic documents. In order to eliminate costly transmissions, code symbols have been substituted for group markings and identifying notations which shall appear at the end of the message text as the final paragraph as follows:

GP 4 for Group 4
GP 3 for Group 3
GP 2 for Group 2
GP 1 for Group 1

Instructions for downgrading or declassifying information should be appended as the final unnumbered paragraph of the message text, when such instructions do not coincide with one of the four GP code symbols.

Since there is no GP code sumbol for administratively controlled documents, the appropriate notation must be added as the final unnumbered paragraph of the message text.

363-563 O - 69 - 4

SECURITY CLASSIFICATION OF OFFICIAL INFORMATION,
DOD 5210.47
(Department of Defense); Selected excerpts

SECURITY CLASSIFICATION OF OFFICIAL INFORMATION

5210.47
Dec. 31, 64#

Refs.: (a) DoD Directive 5120.33, "Classification Management Program," January 8, 1963
(b) DoD Instruction 5120.34, "Implementation of the Classification Management Program," January 8, 1963
(c) DoD Directive 5122.5, "Assistant Secretary of Defense (Public Affairs)," July 10, 1961
(d) DoD Directive 5200.1, "Safeguarding Official Information in the Interests of the Defense of the United States," July 8, 1957
* (e) DoD Directive 5400.7, "Availability to the Public of DoD * Information," June 23, 1967 *
(f) DoD Directive 5200.10, "Downgrading and Declassification of Classified Defense Information," July 26, 1962
(g) DoD Directive 5230.9, "Clearance of Department of * Defense Public Information," December 24, 1966 *
(h) OASD(M) multi-DoD memo., "DoD Instruction 5210.47, Security Classification of Official Information," January 27, 1965 (hereby cancelled)

I. PURPOSE AND APPLICABILITY

In accordance with references (a) and (b), this Instruction provides guidance, policies, standards, criteria and procedures for the security classification of official information under the provisions of Executive Order 10501, as amended, for uniform application throughout the Department of Defense, the components of which, in turn, through their implementation of this Instruction, shall accomplish its application to defense contractors, sub-contractors, potential contractors, and grantees. Determinations whether particular information is or is not Restricted Data are not within the scope of this Instruction.

II. DEFINITIONS

The definitions given below shall apply hereafter in the Department of Defense Information Security Program.

SOURCE: U.S. Department of Defense. Security classification of official information. [Washington] 1964. 1 v. (various pagings) At head of title: Department of Defense Instruction. "Number 5210.47, Dec. 31, 1964."

#Second amendment (Ch 4, 11/6/67)

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

Classified Information: Official information which has been determined to require, in the interests of national defense, protection against unauthorized disclosure and which has been so designated.

Declassification: The determination that classified information no longer requires, in the interests of national defense, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Document: Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps; charts; photographs; negatives; moving or still films; film strips; paintings; drawings; engravings; sketches; reproductions of such things by any means or process; and sound, voice or electronic recordings in any form.

Downgrade: To determine that classified information requires, in the interests of national defense, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

Formerly Restricted Data: Information removed from Restricted Data category upon determination jointly by the Atomic Energy Commission and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. (See subparagraph VIII, D. 13, below, regarding foreign dissemination.)

Information: Knowledge which can be communicated by any means.

Material: Any document, product or substance on or in which information may be recorded or embodied.

Official Information: Information which is owned by, produced by or is subject to the control of the United States Government.

Regrade: To determine that certain classified information requires, in the interests of national defense, a higher or a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher or lower degree.

Research: All effort directed toward increased knowledge of natural phenomena and environment and toward the solution of problems in all fields of science. This includes basic and applied research.

Basic Research, which is the type of research directed toward the increase of knowledge, the primary aim being a greater knowledge or understanding of the subject under study.

Applied Research, which is concerned with the practical application of knowledge, material and/or techniques directed toward a solution to an existent or anticipated military or technological requirement.

Restricted Data: All data (information) concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act. (See Section 11w, Atomic Energy Act of 1954, as amended, and "Formerly Restricted Data.")

Technical Information: Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use and maintenance of munitions and other military supplies and equipment.

Technical Intelligence: The product resulting from the collection, evaluation, analysis and interpretation of foreign scientific and technical information which covers (1) foreign developments in basic and applied research, and in applied engineering techniques; and (2) scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems and materiel, the research and development related thereto, and the production methods used in their manufacture.

III. POLICIES

A. Protecting Essential Information

1. The Preamble, Executive Order 10501, as amended, provides in part as follows:

> "Whereas the interests of national defense require the preservation of the ability of the United States to protect and defend itself against all hostile or destructive action by covert or overt means, including espionage as well as military action /,_7.... it is essential that certain official information affecting the national defense be protected uniformly against unauthorized disclosure."

2. The primary objective of the Classification Management Program is to assure that official information is classified accurately under Executive Order 10501, as amended, when in the interests of national defense it needs protection against unauthorized disclosure.

3. Consistent with the above objective, the use and application of security classification to accomplish such protection shall be limited to only that information which is truly essential to national defense because it provides the United States with:

   a. A military or defense advantage over any foreign nation or group of nations; or

   b. A favorable international posture; or

   c. A defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert;

   which could be damaged, minimized or lost by the unauthorized disclosure or use of the information.

B. Informing the Public

The Department of Defense, in accordance with the policy of the United States Government, shall inform the American public of the activities of the Department of Defense to the maximum extent consistent with the best interests of national defense and security. Nothing contained herein, however, shall be construed to authorize or require the public release of official information. In this connection see reference (c).

C. Regrading and Declassification

In order to preserve the effectiveness and integrity of the classification system, assigned classifications shall be responsive at all times to the current needs of national defense. When classified information is determined in the interests of national defense to require a different level of protection than that presently assigned, or no longer to require any such protection, it shall be regraded or declassified.

D. Improper Classification

Unnecessary classification and higher than necessary classification shall be scrupulously avoided.

E. Misuse of Classification

Classification shall apply only to official information requiring protection in the interests of national defense. It may not be used for the purpose of concealing administrative error or inefficiency, to prevent personal or departmental embarrassment, to influence competition or independent initiative, or to prevent release of official information which does not require protection in the interests of national defense.

F. Safeguarding privately owned information

1. Privately owned information, in which the Government has not established a proprietary interest or over which the Government has not exercised control, in whole or in part, is not subject to classification by the private owner under the authority of this Instruction. However, a private owner, believing his information requires protection by security classification, is encouraged to provide protection on a personal basis and to contact the nearest office of the Army, Navy, or Air Force for assistance and advice.

2. Section 793 (d), Title 18 United States Code provides penalties for improper disclosure of "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."

3. Sections 224 to 227 of the Atomic Energy Act of 1954, as amended, provide penalties for the improper obtaining, disclosure or use of Restricted Data.

G. Safeguarding official information which is not subject to security classification

Official information which does not qualify for security classification or has been declassified, and which pursuant to lawful authority requires protection from unauthorized disclosure or public release for reasons other than national security or defense, shall be handled in accordance with references (e) and (g).

IV. CLASSIFICATION CATEGORIES

A. General

All official information which requires protection in the interests of national defense shall be classified in one of the three categories described below. Unless expressly provided by statute, no other classifications are authorized for United States classified information. Appendix A gives

examples of information which may come within the various categories. Section VI. below provides specific criteria for determining whether information falls within these categories.

B. TOP SECRET - The highest level of classification, TOP SECRET, shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation; such as, leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense. The use of the TOP SECRET classification shall be severely limited to information or material which requires the utmost protection. (See Part I, Appendix A.)

C. SECRET - The second highest level of classification, SECRET, shall be applied only to that information or material the unauthorized disclosure of which could result in serious damage to the Nation; such as, by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations. (See Part II, Appendix A).

D. CONFIDENTIAL - The lowest level of classification, CONFIDENTIAL, shall be applied only to that information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the Nation. (See Part III, Appendix A.) The designation "CONFIDENTIAL - MODIFIED HANDLING AUTHORIZED," which is not a separate classification category, identifies certain CONFIDENTIAL information pertaining to combat or combat-related operations which, because of combat or combat-related operational conditions, cannot be afforded

the full protection prescribed for CONFIDENTIAL information. The designation C-MHA shall be applied to that CONFIDENTIAL information pertaining to military operations involving planning, training, operations, communications and logistical support of combat units when combat or combat-related conditions, actual or simulated, preclude the full application of the rules and procedures governing dissemination, use, transmission and safekeeping prescribed for the protection of CONFIDENTIAL information. The designation may be applied prior to the introduction of the information into combat areas, actual or simulated, when the information is intended for such use and dissemination, but the rules and procedures for handling the information shall not be modified until the information is so introduced. C-MHA cannot be applied to material containing Restricted Data.

E. FOREIGN CLASSIFIED INFORMATION

1. Section 3 (e), Executive Order 10501, provides as follows:

> "Information Originated by a Foreign Government or Organization: Defense information of a classified nature furnished to the United States by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information."

2. Foreign security classifications generally parallel United States classifications. A Table of Equivalents is contained in Appendix B.

3. TOP SECRET, SECRET, and CONFIDENTIAL. If the foreign classification marking is in English, no additional U. S. classification marking is required. If the foreign classification marking is in a language other than English, an equivalent U. S. classification marking as shown in Appendix B will be added.

4. RESTRICTED.* Many foreign governments, and international organizations such as, for example, NATO, CENTO, and SEATO, use a fourth security classification "RESTRICTED" to denote a foreign requirement for security protection of a lesser degree than CONFIDENTIAL. Such foreign RESTRICTED information released to the United States Government under international agreement requiring its protection, usually does not require or warrant United States security classification under Executive Order 10501. Under the agreement covering the release of information, however, certain protection is required. In the usual case, therefore, in order to satisfy this requirement, a document or other material containing foreign RESTRICTED information shall show, or be marked additionally to show, in English, the name of the foreign government or international organization of origin and the word "RESTRICTED," e.g., UK-RESTRICTED; NATO-RESTRICTED. (See Appendix B.) Any document or other material marked as aforesaid shall be protected in the manner specified in reference (d). Documents or other material on hand falling in this category which already have been marked so as to require protection as "CONFIDENTIAL" or "C-MHA," as they are withdrawn from the file for any purpose, shall be re-marked in accordance with this subparagraph and the previously applied marking shall be obliterated or excised. Henceforth, the provisions of this subparagraph shall apply thereto.

5. The origin of all material bearing foreign classifications, including material extracted and placed in Department of Defense documents or material, shall be clearly indicated on or in the body of the material to assure, among other things, that the information is not released to nationals of a third country without consent of the originator.

* The effective date of this paragraph 4 is postponed. See paragraph XIV. B.

V. AUTHORITY TO CLASSIFY

A. Original Classification

1. Original classification is involved when -

   a. An item of information is developed which intrinsically requires classification and such classification cannot reasonably be derived from a previous classification still in force involving in substance the same or closely related information; or

   b. An accumulation or aggregation of items of information, regardless of the classification (or lack of classification) of the individual items, collectively requires a separate and distinct classification determination.

2. For the purpose of assuring both positive management control of classification determinations and ability to meet local operational requirements in an orderly and expeditious manner, the Assistant Secretary of Defense (Manpower) will exercise control over the granting and exercise of authority for original classification of official information. Pursuant thereto, such authority must be exercised only by those individuals who at any given time are the incumbents of those offices and positions designated in or pursuant to subparagraph 3 below and Appendix C, including the officials who are specifically designated to act in the absence of the incumbents. The following general principles are applicable:

   a. Appendix C designates specifically the officials who may exercise original TOP SECRET or SECRET classification authority and who among them may make additional designations. All such additional designations shall be specific and in writing.

   b. The authority to classify is personal to the holder of the authority. It shall not be exercised for him or in his name by anyone else, nor shall it be delegated for exercise by any substitute or subordinate.

AUTOMATIC, TIME-PHASED DOWNGRADING AND DECLASSIFICATION OF CLASSIFIED DEFENSE INFORMATION, DOD 5200.10 (Department of Defense); Selected excerpts

SOURCE:
U.S. Department of Defense. Downgrading and declassification of classified defense information [Washington, 1962] 4, 24 p. At head of title: Department of Defense Directive. "Number 5200.10, July 26, 1962."

DEPARTMENT OF DEFENSE REGULATION
Governing
Automatic, Time-Phased Downgrading and Declassification
of
Classified Defense Information

1. Purpose. The purpose of this regulation is to apply the provisions of Section 4 and Section 5(a), Executive Order 10501, as amended by Executive Order 10964, 20 September 1961; and to implement the provisions of DoD Directive 5200.9 and 5200.10. It establishes a continuing system based on the passage of time for automatically downgrading, or automatically downgrading and declassifying, classified defense information originated by or under the jurisdiction of the Department of Defense (DoD), the Federal Aviation Agency (FAA), and the National Aeronautics and * Space Administration (NASA). It also declassifies by category, effective * January 1, 1964, certain Group-3 documents and materials originated prior * to January 1, 1940, described in subparagraphs 6. a. (3), (4), (5), and (6) * of this regulation. This regulation is not a guide for the assignment of a * classification to information; it applies only to defense information which is assigned a classification by competent authority.

2. Explanation of Terms. The meanings of some terms used in this regulation are given below:

a. DECLASSIFY: To cancel the security classification of an item of classified material.

#First amendment (Ch 3, 11/15/63)

b. DOWNGRADE: To assign a lower security classification to an item of classified material.

c. WEAPON SYSTEM: A general term used to describe a weapon and those components required for its operation.

3. Scope and Application:

a. DoD, FAA, and NASA Information

(1) This regulation applies to all classified information originated by or under the jurisdiction of the Department of Defense or by its contractors, or by a predecessor agency of the Department of Defense or its contractors. Specifically, this includes all classified material originated by the Office of the Secretary of Defense and Department of Defense agencies; the present and former Joint Chiefs of Staff and Joint Staff; the Department of the Army and former War Department; the Department of the Navy; the Department of the Air Force and former Army Air Forces; the United States Coast Guard when acting as a part of the Navy; joint committees or agencies comprised entirely of representatives from within the Department of Defense or its predecessor agencies; other Government agencies whose functions have been officially transferred to the Department of Defense; and contractors in the performance of contracts awarded by or on behalf of the Department of Defense, its components, or its predecessors.

(2) By agreement between the Department of Defense, the Federal Aviation Agency, and the National Aeronautics and Space Administration, this regulation also applies to all classified information originated by or under the jurisdiction of FAA and NASA. This includes all classified information originated by the Federal Aviation Agency, its components and predecessors, including the Civil Aeronautics Administration of the Department of Commerce, and the Airways Modernization Board; the National Aeronautics and Space Administration, its components and predecessors, including the National Advisory Committee for Aeronautics; joint committees, boards and agencies comprised entirely of representatives from the above agencies or from the Department of Defense, its components and predecessors; and contractors in the performance of contracts awarded by or on behalf of FAA, NASA, their components or predecessor agencies.

b. Other Departments and Agencies

By Executive Order 10964, the automatic, time-phased downgrading and declassification system applies to all classified information originated by or under the jurisdiction of all departments and agencies of the Executive Branch. However, custodians of classified material originated by or under the jurisdiction of US departments or agencies other than those described in a above, shall defer action with regard to such material until advised of the implementing instructions issued by the department or agency concerned. Pending that implementation, such material (other than Group-1 material defined herein) shall not be marked or assigned to a Group under this regulation; if the information is incorporated into DoD, FAA, or NASA material, an appropriate explanation shall be included in the text (for example: "Paragraph 2 contains information classified by the State Department; the automatic downgrading-declassification group cannot be determined until appropriate instructions are issued by that department").

c. Authority of Classifying Officials:

(1) Nothing in this regulation shall be construed to relieve of responsibility, or to limit the authority of, those officials designated by competent authority to classify, downgrade, or declassify official defense information. Immediate action should be taken by such officials to downgrade or declassify information when it needs less protection or when it no longer requires such protection.

(2) Any DoD, FAA or NASA classified information, whether or not affected by this regulation, may be downgraded or declassified by the official who has been given that authority under pertinent regulations. Pursuant to that authority, the official who has primary functional responsibility for an item of classified information can prescribe earlier downgrading and declassifying (including assigning it to a less restrictive Group) than that provided by this regulation. However, except as authorized in paragraphs 5 and 6b he cannot assign information to a more restrictive Group than provided herein.

D. Material Officially Transferred

When material is transferred by or pursuant to statute or Executive Order from one department or agency to another, the recipient is the classifying, downgrading, and declassifying authority for all purposes under this regulation. Official transfers result in the material becoming part of the official files or the property of the recipient (e.g., Army Air Forces material officially transferred to the newly established Department of the Air Force in 1948). Transfers merely for the purpose of storage do not constitute an official transfer of classification authority.

e. Material Not Officially Transferred.

When any department or agency has in its possession any classified material which has become 5 years old, and a review of the material indicates that it should be downgraded or declassified and it appears that either (i) the material originated in an agency which has since become defunct and whose files and other property have not been officially transferred to another department or agency within the meaning of d above, or (ii) it is impossible for the possessing department or agency to identify the originating agency, the possessing department or agency shall have power to downgrade or declassify the material or to assign it to a downgrading-declassification Group according to this regulation. If it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the possessing department or agency shall not exercise the power stated in this subparagraph, except with the consent of the other department or agency, until 30 days after it has notified such other department or agency of the nature of the material and of its intention to downgrade or declassify it. During that 30-day period, the other department or agency may, if it so desires, express its objections to downgrading or declassifying the particular material, but the power to make the ultimate decision shall reside in the possessing department or agency.

f. General Information.

The effect of the automatic, time-phased downgrading and declassification system is that all classified information and material heretofore and hereafter received or originated by the Executive Branch, its components, and its contractors, is assigned to one of four groups, described in the following paragraphs. (The attachment shows in graphic form how each Group is affected by the automatic time-phased system.) Upon receipt of this regulation and without further notice, each holder of classified material originated by or under the jurisdiction of DoD, FAA, or NASA, is authorized and required to Group, mark, downgrade, or declassify, as prescribed herein, the material in his custody or possession. In addition, classified material originated by or under the jurisdiction of other Executive departments and agencies shall be Grouped, marked, downgraded, or declassified in accordance with the instructions of the originating agency, when issued.

4. Group-1 Material.

Material in this Group is completely excluded from the automatic downgrading and automatic declassification provisions of this regulation either because it has been removed from such provisions or because it contains information not subject to the classification jurisdiction of the Executive Branch of the U. S. Government.

a. Definition. Specifically, Group-1 comprises material:

(1) Originated by or containing classified information clearly attributed to foreign governments or their agencies, or to international organizations and groups, including the Combined Chiefs of Staff. This does not include US classified information hereafter furnished to a foreign government or international organization; the US classified information shall be Grouped and marked as otherwise prescribed herein.

(2) Concerning communications intelligence or cryptography, or their related activities.

(a) This includes information concerning or revealing the processes, techniques, technical material, operation, or scope of communications intelligence, cryptography, and cryptographic security. It also includes information concerning special cryptographic equipment, certain special communications systems designated by the department or agency concerned, and the communications portion of cover and deception plans.

(b) However, provided the material does not reveal the foregoing information, this does not include radar intelligence or electronic intelligence, or such passive measures as physical security, transmission security, and electronic security.

(3) Containing Restricted Data or Formerly Restricted Data.

(4) Containing nuclear propulsion information or information concerning the establishment, operation, and support of the US Atomic Energy Detection System, unless otherwise specified by the pertinent AEC-DoD classification guide.

(5) Containing special munition information as defined in AG Ltr AGAM-P(M)311.5, (17 Sept 60) DCS/Ops 19 Sept 60; OPNAVINST 008190.1 series; or AFR 205-17.

(6) Information concerning standardized BW agents.

5. Group-2 Documents.

This Group is established as a means whereby authorized officials can exempt individual documents containing extremely sensitive information from both automatic downgrading and automatic declassification. This Group applies only to documents originally classified TOP SECRET or SECRET.

6. Group-3 Material

This Group contains certain types of information or subject matter that warrants some degree of classification for an indefinite period. There are two kinds of Group-3 material: (i) that containing the subject matter normally assigned to Group-3 according to a below; and (ii) documents which are individually and specifically assigned to Group-3 under the optional exemption provisions of b below. Group-3 documents and materials originated prior to January 1, 1940, which fall within the descriptions of subparagraphs 6. a. (3), (4), (5), or (6), without at the same time falling within the descriptions of subparagraphs 6. (a), (1), (2), or (7), are hereby declassified, effective January 1, 1964.

a. Definition - Normal Group-3.

The specific information or subject matter normally comprising Group-3 is as follows:

(1) Plans for an operation of war that were prepared by an organization higher than Army division, Navy task force, numbered Air Force, or other military command of comparable level. This includes but is not limited to:

(a) Plans for combat operations; and information concerning or revealing long-range operational concepts and the employment of forces.

(b) Plans on cover or deception, including information on operations relating thereto.

(c) Information concerning or revealing escape or evasion plans, procedures, and techniques.

(d) Planning and programming information which concerns or reveals service-wide force objectives, over-all force deployments, and complete service-wide combat unit priority listings; or which contains or reveals detailed service-wide planning or programming data.

(e) Targeting data on foreign areas, or information which would reveal strategic targeting plans.

(2) DoD and FAA intelligence and counterintelligence.

(3) Information concerning or revealing the capabilities, limitations, or vulnerabilities of a weapon, weapon system, or space system in current use or in development for future use. This is limited to information concerning significant combat capabilities or

8

#First amendment (Ch 3, 11/15/63)

7. Group-4 Material:

a. Definition.

Group-4 includes all classified material which does not qualify for, or is not assigned to, one of the first three Groups.

(1) Normally, information such as logistical data, production schedules, budget and cost figures, dimensions or weights, and similar subjects shall be assigned to Group-4, even if the equipment or material to which it applies is in Group-3.

(2) Defense information classified in accordance with a topic of a joint AEC-DoD classification guide shall not be assigned to Group-4 unless such an assignment is clearly indicated under the pertinent topic in the joint guide.

vulnerabilities, knowledge of which could be exploited by an enemy to counter, render ineffective, neutralize, or destroy the weapon or system; or limitations which degrade the combat effectiveness of the weapon or system. However, it specifically includes:

(a) Target detecting devices for proximity VT fuses.

(b) Biological weapon system information which reveals the scientific name or designation of the agent and the non-descriptive code designation of the agent.

(c) Technical information concerning electronic countermeasure or counter-countermeasure equipment, processes, or techniques; and technical data concerning infra-red detection or suppression.

(d) Research and development information concerning or revealing significant combat capabilities of a future weapon or space system or subsystem. This is limited to information concerning or revealing significant new technological developments or adaptations beyond normal evolutionary improvements.

(e) Information pertaining to combat-type naval vessels which reveals structural, performance, or tactical data, such as armor and protective systems, war damage reports, damage control systems, power, speed, range, propeller RPM, and maneuvering characteristics.

(4) Information which could be used by an enemy to develop target data for an attack on the United States or its allies, such as geodetic and gravimetric survey data, reductions of survey data that can be used for intercontinental datum connections or for determining the size of the earth, or the precise (in seconds of arc) coordinates of facilities that are essential elements of a weapon system or that are essential to the conduct of a war.

(5) Technical information concerning or revealing explosive ordnance demolition techniques.

(6) Defense information (other than Group-1 material) classified according to AEC-DoD classification guides, unless otherwise specified by the pertinent guide.

(7) Material prepared by a theater headquarters, military government headquarters, military mission headquarters, or other headquarters of comparable or higher level, which concern or affect the formulation and conduct of U. S. foreign policy, and plans or programs relating to international affairs.

AUTOMATIC DOWNGRADING AND AUTOMATIC DECLASSIFICATION CHART