

(1) The Comprehensive Review is signed by the responsible committee officer and approved by the bureau/office policy making officer. It is submitted in original only.

(2) The Annual Report will be prepared on Standard Forms 248 and 249 in original and one copy. (Instructions for preparation are printed on the back of the forms.)

(3) The Report of Closed Meeting(s) is signed by the committee chairman and submitted in original and 8 copies.

(4) The Advisory activities reports are submitted in 9 copies each, except Presidential advisory committee reports are submitted in 12 copies.

#### §8.11 Records.

(a) The records of an advisory committee consist of all papers and documents which are prepared for or by and/or made available to the committee, and are maintained by the office responsible for the committee. Such records are *inter alia* agenda, drafts, minutes, notices, press releases, reports, studies, transcripts, and working papers.

(b) The Advisory Committee Management Officer maintains the Department's official records relating to the management of all committees.

#### §8.12 Financial records.

Accurate records will be kept by the responsible committee office of all operating and salary costs of a committee. (See instruction item 17 on SF-248.)

#### §8.13 Availability of records.

The records of a committee are to be made available upon request in accordance with the Department's regulations promulgated in accordance with the provisions of the Freedom of Information Act (40 FEDERAL REGISTER 7256-7529, February 19, 1975).

#### §8.14 Public inquiries.

Public inquiries concerning the implementation of the Federal Advisory Committee Act and the management of the advisory committees of the Department should be addressed to the Advisory Committee Management Officer, Management Systems Staff, Department of State, Washington, DC 20520.

## PART 9—SECURITY INFORMATION REGULATIONS

Sec.

- 9.1 General policy.
- 9.2 Implementation and oversight responsibilities.
- 9.3 Responsibility for safeguarding classified information.
- 9.4 Classification.
- 9.5 Classification designations.
- 9.6 Requirements for classification.
- 9.7 Classification authority.
- 9.8 Limitations on classification.
- 9.9 Duration of classification.
- 9.10 Derivative classification.
- 9.11 Derivative classification guides.
- 9.12 Identification and markings.
- 9.13 Transferred material.
- 9.14 Declassification and downgrading.
- 9.15 Systematic review for declassification guidelines.
- 9.16 Mandatory review.
- 9.17 Schedule of fees.
- 9.18 Access by Presidential appointees.

#### APPENDIX A TO PART 9—DEFINITIONS

AUTHORITY: E.O. 12356, National Security Regulations of April 2, 1982 (47 FR 14874, April 6, 1982); Information Security Oversight Office Directive No. 1 (47 FR 27836, June 25, 1982).

SOURCE: 47 FR 55594, Dec. 10, 1982, unless otherwise noted.

#### §9.1 General policy.

(a) E.O. 12356 (hereinafter called "the Order") recognizes that it is essential that the public be informed concerning the activities of its government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. With this object, the Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

(b) The purpose of these regulations is to assist in the implementation of the Order and Information Security Oversight Office (hereinafter referred to as ISOO), Directive No. 1, (hereinafter called "the Directive"), and users of these regulations may refer to the Order and Directive for additional guidance.

**§9.2 Implementation and oversight responsibilities.**

The Order requires each agency that originates or handles classified information to promulgate implementing regulations. The Order further requires that each agency originating or handling classified material shall designate a senior official to direct and administer its information security program. This official shall be responsible for actively overseeing the agency's program, including a security education program, to ensure effective implementation of the Order.

(a) In addition, this official shall have the following responsibilities:

(1) To establish and monitor agency policies and procedures to prevent over or under classification, to ensure the protection from unauthorized disclosure of properly classified information, including intelligence information, and to ensure orderly and effective declassification of agency documents which no longer require protection, in accordance with the terms of the Order.

(2) To review proposed classified disclosures of an exceptional nature bearing upon issues of concern to the Congress and the public.

(3) To issue any needed guidelines for classification or declassification.

(4) To recommend to the agency head the following:

(i) Proposals for reclassification in accordance with section 1.6(c) of the Order;

(ii) Other categories of information, as defined in section 1.3(a)(10) of the Order, which require protection against unauthorized disclosure but which are not specifically protected by sections 1.3(a) (1) through (9) of the Order;

(iii) Waivers, for specified classes of documents or information of the requirement to indicate which portions of documents are classified and which are not, as provided by section 1.5(b) of the Order; and

(iv) Waivers for specified classes of documents or information, of the requirement to prepare derivative classification guides, as provided by section 2.2(c) of the Order.

(5) To prepare a list of officials, by name or position, delegated Top Secret, Secret, and Confidential classification authority.

(6) To receive, and if necessary act on, suggestions and complaints with respect to that agency's administration of its information security program.

(7) To provide guidance concerning corrective or disciplinary action in unusually important cases involving unauthorized disclosure or refusal to declassify.

(8) To maintain liaison with the Director of ISOO and to furnish reports and information as required by section 5.2 of the Order.

(b) *Department of State.* Within the Department of State, the senior official is the Deputy Assistant Secretary, Classification/Declassification Center, hereinafter referred to as (DAS/CDC).

(c) *AID.* Within AID (a component of the International Development Cooperation Agency), the senior official is the Inspector General.

(d) *USIA.* Within USIA, the senior official is the Director, Office of the Public Liaison.

**§9.3 Responsibility for safeguarding classified information.**

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

(b) *Individual.* Each employee is responsible for becoming familiar with and adhering to all security regulations.

(c) *Supervisory.* The ultimate responsibility for safeguarding classified information rests upon each supervisor to the same degree that the supervisor is charged with functional responsibility for the organizational unit. While certain employees may be assigned specific security responsibilities, such as Top Secret Control Officer or Unit Security Officer, it is nevertheless the basic responsibility of supervisors to ensure that classified material entrusted to their organizational units is handled in accordance with the procedures prescribed in these regulations. Each supervisor should ensure that no one employee is assigned unreasonable security responsibilities in addition to usual administrative or functional duties.

## Department of State

## § 9.5

(d) *Organizational.* The Offices of Security in State, AID, and USIA are responsible for physical, procedural, and personnel security in their respective agencies. In the Department of State, the Office of Communications (COMSEC) is responsible for communications security.

### § 9.4 Classification.

(a) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" pending a determination about its classification by an original classification authority. When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level pending the determination of its classification level by an original classification authority. Determinations hereunder shall be made within 30 days.

(b) Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Information may not be classified to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(c) The President or an agency head or official designated under section 1.2 (a)(2), 1.2 (b)(1), or 1.2 (c)(1) of the Order may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security, and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of ISOO.

(d) It is permitted to classify or reclassify information after an agency has received a request for it under the Freedom of Information Act or the Privacy Act, or the mandatory review provisions of the Order, provided that such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior official,

or an official with original Top Secret classification authority. Every effort should be made to classify properly at the time of origin. When a determination is made that a document requires classification or reclassification, however, all holders of the document should be notified and, in the Department of State, a copy of the classification or reclassification memorandum should be sent to the Foreign Affairs Information Management Center (FAIM). In addition, if the classification or reclassification was done in any office other than the DAS/CDC, that office should send a copy of the pertinent memorandum to the CDC.

(e) For the Department of State, these functions will be performed by the DAS/CDC.

(f) For AID, the function will be performed by the Administrator.

(g) For USIA, the function will be performed by the Director of Public Liaison.

(h) Information classified in accordance with these regulations shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

### § 9.5 Classification designations.

(a) Only three (3) designations of classification are authorized: "Top Secret," "Secret," and "Confidential."

(1) *Top Secret.* Information may be classified "Top Secret" if its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. This classification should be used with the utmost restraint. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret.* Information may be classified "Secret" if its unauthorized disclosure could reasonably be expected to

## §9.6

## 22 CFR Ch. I (4-1-03 Edition)

cause serious damage to the national security. This classification should be used sparingly. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) *Confidential*. Information may be classified "Confidential" if its unauthorized disclosure could reasonably be expected to cause damage to the national security. Except as otherwise provided by statute, no other terms shall be used to identify classified information. Terms or phrases such as "For Official Use Only" or "Limited Official Use" shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these national security information designations, such as "Secret Sensitive" or "Agency Confidential" to identify national security information.

(b) *Foreign government information*. If classified by the foreign government, the information shall either retain its original classification or be assigned a U.S. classification designation which will ensure a degree of protection at least equivalent to that required by the entity that furnished the information. If not given a specific classification by the foreign government, the information will be assigned an appropriate classification dependent on the sensitivity of the subject matter and the degree of damage its unauthorized disclosure could reasonably be expected to cause to the national security. Classification designations assigned by the U.S. agency shall be marked on the foreign government information in accordance with the provisions of §9.12.

### §9.6 Requirements for classification.

With the exception of the Atomic Energy Act of 1954, as amended, these regulations are the only basis for classifying information in the agencies named herein. To be eligible for classification, information must meet the two following requirements:

(a) First, it must deal with one of the following criteria:

(1) Military plans, weapons, or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) Confidential sources; or

(10) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. In the Department of State, the DAS/CDC, as the senior official, shall recommend such other categories of information to the Secretary. Any determination made under this subsection shall be reported promptly to the Director of ISOO.

(b) Second, an official with original classification authority must determine that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or record copy of the information.

## Department of State

## § 9.10

### § 9.7 Classification authority.

(a) In the Department of State authority for original classification of information as "Top Secret" may be exercised only by the Secretary of State and those officials delegated this authority in writing, by position or by name, by the Secretary or the DAS/CDC, as the senior official, on the basis of their frequent need to exercise such authority. Normally these will not be below the level of Deputy Assistant Secretary in the Department; or Chief of Mission, Charge d'Affairs, or principal officer at an autonomous consular post overseas.

(b) Authority for original classification of information as "Secret" may be exercised by officials with Top Secret authority, the Administrator of AID, and the Director of USIA. This authority may be delegated to such subordinate officials as the senior official in the Department, the administrator of AID or the Director of USIA may designate in writing, by position or by name, on the basis of their frequent need to exercise such authority. Normally, these will not be below the level of office director, section head (in a mission abroad), country public affairs officer, or equivalent.

(c) Authority for original classification of information as "Confidential" may be exercised by officials with Top Secret or Secret classification authority, and the President of the Overseas Private Investment Corporation; and may be delegated to such subordinate officials as the senior official in the Department, the Administrator of AID, the Director of USIA, or the President of OPIC may designate in writing, by position or by name, on the basis of their frequent need to exercise such authority.

(d) Delegated original classification authority at any level may not be re-delegated.

(e) In the absence of an authorized classifier, the person designated to act for that official may exercise the classifying authority.

(f) In the Department of State the Classification/Declassification Center, and in AID and USIA the Office of Security, shall maintain a current listing, by classification designation, of the positions or officials carrying

original classification authority. The listing shall be reviewed as needed to ensure that such delegations have been held to a minimum, and that officials so designated have a continuing need to exercise such authority.

### § 9.8 Limitations on classification.

A reference to classified documents which does not directly or indirectly disclose classified information may not be classified or used as a basis for classification.

### § 9.9 Duration of classification.

(a) Information shall be classified for as long as is required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Information classified under predecessor orders that is not subject to automatic declassification or that is marked for review before declassification shall remain classified until reviewed for declassification.

(c) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions as soon as possible. The authority to extend the classification of information subject to automatic declassification under predecessor orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the ISOO.

### § 9.10 Derivative classification.

(a) Derivative classification is made by a person, not necessarily having original classification authority, based on an originally classified document or as directed by a classification guide.

## §9.11

## 22 CFR Ch. I (4–1–03 Edition)

The derivative classifier may be one who reproduces, extracts, restates, paraphrases, or summarizes classified materials, or applies markings in accordance with source material or a classification guide.

(b) Derivative classifiers must respect original classification markings. Only if the derived document, by means of paraphrasing, excising, etc., has clearly lost the original grounds for classification, may its original classification be removed or lowered.

(c) Subject to paragraph (b) of this section, markings on derivatively classified material, including declassification instructions, shall be carried forward from the original material, or shall be as directed by the classification guide.

### §9.11 Derivative classification guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information, except as provided in paragraph (e) of this section.

(b) Each guide shall be approved personally and in writing by an official who:

(1) Has program or supervisory responsibility over the information or is the senior agency official who directs and administers the information security program; and

(2) Is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Classification guides shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which classification level applies to each element or category of information; and

(3) Prescribe declassification instructions for each element or category of information in terms of (i) a period of time, (ii) the occurrence of an event, or (iii) a notation that the information shall not be automatically declassified without the approval of the originating agency.

(d) Classification guides shall be reviewed at least every two years and updated as necessary. Each agency shall maintain a list of its classification guides in current use.

(e) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. In the Department of State, the DAS/CDC, as senior official, shall make recommendations to the Secretary concerning such waivers. In AID, the Inspector General shall make recommendations to the Administrator concerning such waivers. In USIA, the Director of the Office of Public Liaison shall make recommendations to the Director concerning such waivers. The Director of ISOO shall be notified of any waivers. The decision to waive the requirement to issue classification guides for specific classes of documents or information should be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

### §9.12 Identification and markings.

Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper documents, or the originator shall provide holders or recipients of the information with written instructions for protecting the information. These markings include one of the three (3) classification levels defined in §9.5, the identity of the original classification authority (except as noted under paragraph (b)(ii) of this section) the agency and office of origin (except as noted under paragraph (b)(ii) of this section) and the date or event for declassification or the notation "Originating Agency's Determination Required" (OADR).

## Department of State

## §9.12

(a) *Classification level.* The markings “Top Secret,” “Secret,” and “Confidential” are used to indicate: That information requires protection as national security information under the Order; the highest level of classification contained in a document; and the classification level of each page and, in abbreviated form, each portion of a document.

(1) *Overall marking.* The highest level of classification of information in a document shall be marked in such a way as to distinguish it clearly from the informational text. These markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) *Page marking.* Each interior page of a classified document shall be marked at the top and bottom either according to the highest classification of the content of the page, including the designation “UNCLASSIFIED” when it is applicable, or with the highest overall classification of the document.

(3) *Portion-marking.* Agency heads may waive the portion marking requirement for specified classes of documents or information only upon a written determination that (i) there will be minimal circulation of the specified documents or information and minimal potential usage of these documents or information as a source for derivative classification determination; or (ii) there is some other basis to conclude that the potential benefits of portion marking are clearly outweighed by the increased administrative burdens. Unless this requirement has been waived, each portion of a document, including subjects and titles, shall be marked by placing a parenthetical designation immediately preceding or following the text to which it applies. The symbols “(TS)” for Top Secret, “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified shall be used for this purpose. If the application of these symbols is not practicable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification, and the information that is not classified. If all portions of a document are

classified at the same level, it may be marked with a statement to that effect, e.g., “Confidential—Entire Text.” If a subject or title requires classification, an unclassified identifier may be assigned to facilitate reference.

(A) For the Department of State, the Secretary has waived the portion marking requirement for the following classes of documents under section 2001.5(a)(3)(i) of the Directive—documents which will have minimal circulation and minimal potential usage as a source for derivative classification:

(1) Documents containing Top Secret information;

(2) Action/informational memoranda prepared for Assistant Secretaries and above;

(3) Instructions to posts and negotiating delegations;

(4) In-house research studies; and

(5) Inter and intra-office memoranda.

(B) The Secretary has also waived the portion marking requirement for documents, both telegraphic and non-telegraphic, containing foreign government information, under section 2001.5(a)(3)(ii) of the Directive.

(4) *Omitted markings.* Information assigned a level of classification under predecessor orders shall be considered as classified at the level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in section 3.1(b) of the Order.

(b) *Classification authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as “CLASSIFIED BY” (“identification of original classification authority”).

(c) *Agency and office of origin.* If the identity of the originating agency and office is not apparent on the face of the document, it shall be placed below the “CLASSIFIED BY” line.

(d) *Declassification and downgrading instructions.* Declassification and, as applicable, downgrading instructions shall be shown as follows:

(1) For information to be declassified automatically on a specific date or event: “DECLASSIFY ON: (date)” or “DECLASSIFY ON: (description of event)”.

(2) For information not to be automatically declassified: “DECLASSIFY ON: Originating Agency Determination Required or OADR”.

(3) For information to be downgraded automatically on a specific date or upon occurrence of a specific event: “DOWNGRADE TO (classification level) ON (date or description of event)”.

(e) *Special markings*—(1) *Transmittal documents*. A transmittal document shall indicate on its face the highest classification of any information transmitted by it. It shall also include the following or similar instructions:

(i) For an unclassified transmittal document: “Unclassified When Classified Enclosure is Removed;” or

(ii) For classified transmittal document: “Upon Removal of Attachments This Document Is (classification level of the transmittal document standing alone).”

(2) *Restricted Data or Formerly Restricted Data*. Restricted Data and Formerly Restricted Data information shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence sources or methods*. Documents that contain information relating to intelligence sources or methods shall include the following markings unless otherwise prescribed by the Director of Central Intelligence: “WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED.”

(4) *Foreign government information (FGI)*. Documents that contain FGI shall include either the marking “FOREIGN GOVERNMENT INFORMATION”, or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(5) *Electrically transmitted information (messages, cables)*. National security information that is transmitted electrically shall be marked as follows:

(i) The highest level of classification shall appear before the first line of text;

(ii) A “Classified By” line is not required; i.e., name and office of classifier may be omitted; and

(iii) The duration of classification shall appear as follows:

(A) For information to be declassified automatically on a specific date or event: “DECL: (date)” or “DECL: (description of event).”

(B) For information not to be automatically declassified which requires the originating agency’s determination: “DECL: OADR.”

(C) For information to be automatically downgraded: “DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur).”

(iv) Portion marking shall be as prescribed in paragraph (a)(3) of this section.

(v) Special markings as prescribed in section 2001.5(e) 2, 3, & 4 of the Directive shall appear after the marking for the highest level of classification. These include:

(A) Restricted Data or Formerly Restricted Data: Electrically transmitted information containing Restricted Data or Formerly Restricted Data shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(B) Information concerning intelligence sources and methods; “WNINTEL,” unless proscribed by the Director of Central Intelligence.

(C) Foreign government information: “FGI” or a marking that otherwise indicates that the information is foreign government information. If the fact must be concealed, the marking shall not be used and the message shall be marked as if it were wholly of U.S. origin.

(vi) Paper copies of electrically transmitted messages shall be marked as provided in paragraph (a) through (e) of this section.

(6) *Changes in classification markings*. When a change is made in the level or the duration of classified information, all holders of record shall be promptly notified. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is

## Department of State

## §9.15

unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

### §9.13 Transferred material.

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of the Order.

(b) In the case of classified information that is not officially transferred as described in section 3.2(a) of the Order, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purpose of the Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with the Order, the Directive, and agency guidelines.

### §9.14 Declassification and downgrading.

(a) *General.* Information should be declassified or downgraded as soon as national security considerations permit. Information will be protected in accordance with the provisions of the Order for as long as it meets the classification requirements prescribed by these regulations. Agencies shall coordinate their review of classified information with other agencies or foreign governments that have a direct interest in the subject matter.

(b) *Authority to declassify or downgrade.* Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a

supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to section 5.3(a)(1) of the Order. In addition, if the Director of ISOO determines that information is classified in violation of the Order, the Director may require the agency which classified the information to declassify it. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until a decision has been made on the appeal.

(c) The agency shall maintain a current, unclassified, listing of officials delegated declassification and downgrading authority.

### §9.15 Systematic review for declassification guidelines.

(a) The agency may schedule classified records of permanent historical or other value for bulk review for declassification and may either perform such review itself, or may refer the records, together with guidelines for declassification, to the Archivist of the United States for review.

(b) For records of the Department of State, a sampling of classified records of permanent value for a given period will be selected by the Office of the Historian (PA/HO), and reviewed by the Systematic Review Office of the Classification/Declassification Center. The Systematic Review Office will prepare guidelines, which will be transmitted by the Secretary of State to the Archivist of the United States, not later than February 1, 1983, for use in reviewing the remainder of the permanently valuable classified records of the given period when these records are accessioned to the National Archives.

(c) AID will prepare guidelines, and transmit them to the Archivist of the United States not later than February 1, 1983, for use in reviewing permanently valuable classified records that have been accessioned to the National Archives. The Records Management Branch, Communications and Records Management Division, (M/SER/MO), is designated as the office responsible for systematic review matters within the agency. The Branch Staff will provide

## §9.16

## 22 CFR Ch. I (4-1-03 Edition)

assistance to the Archivist in the systematic review process.

(d) For information concerning records of ICA, contact the agency's Declassification Officer, Office of Administration.

(e) The agency guidelines will identify categories of information which cannot be automatically declassified but must be reviewed item-by-item to determine if there is a need for continued protection.

(f) These guidelines may be authorized by the agency head for use by other agencies, in addition to the National Archives, having custody of the originating agency's classified information of the period covered.

(g) These guidelines shall be reviewed and updated every five years, unless earlier review is requested by the Archivist.

(h) For foreign government information, the agency will prepare by February 1, 1983, specific guidelines for systematic review of foreign government information in records accessioned to the National Archives, and will revise such guidelines every five years or earlier as requested by the Archivist.

(i) *Special procedures.* The agency shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities) sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

### §9.16 Mandatory review.

Each agency shall review for declassification any classified information requested, under the Mandatory Review provisions of the Order except as noted in paragraph (d) of this section, provided that: The requester is a U.S. citizen, resident alien, Federal agency, or state or local government; the request describes the information with sufficient specificity to enable the agency to locate the records containing the information with a reasonable amount of effort; and the agency receiving the request is the agency that originated the information. When an agency receives a request for information in its custody which was origi-

nated by another agency, it shall refer the information and request to the originating agency for its review and direct response to the requester.

(a) *Foreign government information.* Except as provided in this paragraph, agencies shall process mandatory review requests for classified records containing foreign government information in accordance with §2001.32(a) of the ISOO Directive. The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If the agency receiving the request is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(b) Information requested shall be declassified if it no longer requires protection under the provisions of the Order. It will then be released to the requester unless withholding is otherwise authorized under applicable law, such as the Freedom of Information or Privacy Act. If the information requested cannot be declassified in its entirety, the agency will make reasonable efforts to release those declassified portions that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of administrative appeal, which must be filed within 60 days of receipt of the denial, and shall enclose a copy of the agency's regulations governing the appeal process.

(c) Initial requests may be addressed to:

(1) Department of State: The Information and Privacy Coordinator, Room 1239, Bureau of Administration, Department of State, Washington, DC 20520, with the envelope clearly marked MANDATORY REVIEW REQUEST;

(2) AID: Director, Office of Public Affairs for AID; Room 4899, 2201 C Street, NW., Washington, DC 20523; or

(3) USIA: Freedom of Information and Privacy Act Coordinator, Office of Administration, 1776 Pennsylvania Avenue, NW., Washington, DC 20547.

(d) In responding to mandatory review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the case. Agencies shall make a final determination in one year from the date of receipt, except in unusual circumstances.

(e) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from mandatory review. However, the Archivist of the United States has the authority to review, downgrade, and declassify such information which is under the control of the Administrator of General Services or the Archivist, for example in Presidential Libraries, pursuant to section 2107, 2107 note, or 2203 of title 44, United States Code. The Archivist will consult with agencies having primary subject matter interest concerning the declassification of the requested material. Any decision by the Archivist may be appealed to the Director of ISOO, with the right of further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(f) Requests for classified information not specifically identified as being made under the Mandatory Review provisions of the Order will be processed under the terms of the FOIA, the Privacy Act, or other appropriate procedures.

(g) In considering requests for mandatory review, the agency may decline to review again any request for material which has been recently reviewed and denied, unless the request constitutes an appeal of an initial denial.

(h) Mandatory review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(i) In response to a request for information under the Freedom of Informa-

tion Act, the Privacy Act of 1974, or the mandatory review provisions of the Order, an agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under these regulations.

(j) For detailed regulations for the internal processing of mandatory review initial requests and appeals see:

(1) Department of State: 5 FAM 900, 22 CFR 171.22 and 171.60;

(2) AID: AID Handbook 18, part III, chapter 11; or

(3) USIA: 22 CFR part 503.

#### §9.17 Schedule of fees.

For State, see 22 CFR 171.6 and 171.13; For AID, see 22 CFR 212.35; or For USIA, see 22 CFR 503.6(c).

#### §9.18 Access by presidential appointees.

For procedures of the Department of State, see 22 CFR 171.25; For procedures of AID, see 22 CFR 171.25; or For procedures of USIA, see 22 CFR part 503.

#### APPENDIX A TO PART 9—DEFINITIONS

For the purpose of these security regulations, the following definitions of terms shall apply.

*Agency.* A Federal agency, including department, agency, commission etc, as defined in 5 U.S.C. 552(e).

*Original classification.* The initial determination that, in the interest of national security, information requires protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

*Original classification authority.* The authority vested in an executive branch official to make a determination of original classification. A person having original classification authority may also have the authority to prolong or restore classification.

*Originating agency.* The agency responsible for the initial determination that particular information is classified.

*Information.* Any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

*National security information.* Information that has been determined pursuant to this Order or any predecessor Order to require protection against unauthorized disclosure and that is so designated.

*Foreign government.* Includes foreign governments and international organizations of governments.

*Foreign government information.* Foreign government information is: (1) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (2) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

*National security.* The national defense or foreign relations of the United States.

*Confidential source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

*Classification guide.* A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively.

*Derivative classification.* A determination that information is in substance the same as information currently classified, together with the designation of the level of classification.

*Special access program.* Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know." It does not include special captions such as NODIS, LIMDIS.

*Intelligence activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to the Order.

*Unauthorized disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

## **PART 9a—SECURITY INFORMATION REGULATIONS APPLICABLE TO CERTAIN INTERNATIONAL ENERGY PROGRAMS; RELATED MATERIAL**

Sec.

- 9a.1 Security of certain information and material related to the International Energy Program.
- 9a.2 General policy.
- 9a.3 Scope.
- 9a.4 Classification.
- 9a.5 Declassification and downgrading.
- 9a.6 Marking.
- 9a.7 Access.
- 9a.8 Physical protection.

AUTHORITY: E.O. 11932 (41 FR 32691), E.O. 11652 (37 FR 5209, National Security Council Directive of May 17, 1972 (37 FR 10053)).

SOURCE: 42 FR 46516, Sept. 16, 1977; 42 FR 57687, Nov. 4, 1977, unless otherwise noted.

### **§ 9a.1 Security of certain information and material related to the International Energy Program.**

These regulations implement Executive Order 11932 dated August 4, 1976 (41 FR 32691, August 5, 1976) entitled "Classification of Certain Information and Material Obtained from Advisory Bodies Created to Implement the International Energy Program."

### **§ 9a.2 General policy.**

(a) The United States has entered into the Agreement on an International Energy Program of November 18, 1974, which created the International Energy Agency (IEA). This program is a substantial factor in the conduct of our foreign relations and an important element of our national security. The effectiveness of the Agreement depends significantly upon the provision and exchange of information and material by participants in advisory bodies created by the IEA. Confidentiality is essential to assure the free and open discussion necessary to accomplish the tasks assigned to those bodies.