Federal Register

Friday
June 25, 1982

Part VIII

Information Security Oversight Office

National Security Information

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

[Directive No. 1]

National Security Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Implementing Directive; final rule.

SUMMARY: The Information Security Oversight Office is publishing this Directive (final rule) pursuant to section 5.2(b)(1) of Executive Order 12356, relating to national security information. The National Security Council approved this Directive on June 22, 1982. The Executive order prescribes a uniform information security system; it also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of national security information.

EFFECTIVE DATE: August 1, 1982.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO. Telephone: 202-535-7251.

SUPPLEMENTARY INFORMATION: This Directive is issued pursuant to the provisions of section 5.2(b)(1) of Executive Order 12356. The purpose of the Directive is to assist in implementing the Order; users of the Directive shall refer concurrently to that Order for guidance.

List of Subjects in 32 CFR Part 2001

Archives and records, Authority delegations, Classified information, Executive orders, Freedom of information, Information, Intelligence, National defense, National security information, Presidential documents, Security information, Security measures.

Title 32 of the Code of Federal Regulations, Part 2001, is revised to read as follows:

PART 2001—NATIONAL SECURITY INFORMATION

Subpart A—Original Classification

Sec.
2001.1 Classification levels.
2001.2 Classification authority.
2001.3 Classification categories.
2001.4 Duration of classification.
2001.5 Identification and markings.
2001.6 Limitations on classification.

Subpart B—Derivative Classification

2001.20 Use of derivative classification.
2001.21 Classification guides.
2001.22 Derivative identification and markings.

Subpart C—Declassification and Downgrading

2001.30 Listing declassification and downgrading authorities.
2001.31 Systematic review for declassification.
2001.32 Mandatory review for declassification.
2001.33 Assistance to the Department of State.
2001.34 FOIA and Privacy Act requests.

Subpart D—Safeguarding

2001.40 General.
2001.41 Standards for security equipment.
2001.42 Accountability.
2001.43 Storage.
2001.44 Transmittal.
2001.45 Special access programs.
2001.46 Reproduction controls.
2001.47 Loss or possible compromise.
2001.48 Disposition and destruction.
2001.49 Responsibilities of holders.
2001.50 Emergency planning.
2001.51 Emergency authority.

Subpart E—Implementation and Review

2001.60 Agency regulations.
2001.61 Security education.
2001.62 Oversight.

Subpart F—General Provisions

2001.70 Definitions.
2001.71 Publication and effective date.

Authority: Section 5.2(b)(1), E.O. 12356, 47 FR 14874, April 6, 1982.

Subpart A—Original Classification

§ 2001.1 Classification levels.

(a) *Limitations [1.1(b)].*[1] Markings other than "Top Secret," "Secret," and "Confidential," 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 markings, such as "Secret Sensitive" or "Agency Confidential," to identify national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify nonclassified executive branch information.

(b) *Reasonable doubt [1.1(c)].* (1) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" information in accordance with Subpart D, pending the determination about its classification. Upon the determination of a need for classification, the information that is classified shall be marked as provided in § 2001.5.

(2) When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level in accordance with Subpart D, pending the determination about its classification level. Upon the determination of its classification level, the information shall be marked as provided in § 2001.5.

[1] Bracketed references pertain to related sections of Executive Order 12356.

§ 2001.2 Classification authority.

(a) *Requests for original classification authority [1.2 and 5.2(b)(5)].* A request for original classification authority pursuant to section 1.2 of Executive Order 12356 (hereinafter "the Order") shall include a complete justification for the level of classification authority sought, a description of the information that will require original classification, and the anticipated frequency of original classification actions.

(b) *Listing classification authorities [1.2].* Agencies shall maintain a current listing of officials delegated original classification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

(c) *Exceptional cases [1.2(e)].* Information described in section 1.2(e) of the Order shall be protected as provided in § 2001.1(b).

§ 2001.3 Classification categories.

(a) *Classification in context of related information [1.3(b)].* Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(b) *Unofficial publication or disclosure [1.3(d)].* Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Order or predecessor orders, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences.

§ 2001.4 Duration of classification.

(a) *Information not marked for declassification [1.4].* Information classified under predecessor orders that is not subject to automatic declassification shall remain classified until reviewed for declassification.

(b) *Authority to extend automatic declassification determinations [1.4(b)].* 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 Information Security Oversight Office.

§ 2001.5 Identification and markings [1.5(a), 1.5(b) and 1.5(c)].

A uniform information security system requires that standard markings be applied to national security information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents created after the effective date of the Order 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.

(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 determinations; 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 the portion marking requirement has been waived as authorized, 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 parenthetical designations 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, this fact may be indicated by a statement to that effect. If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(b) *Classification authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as follows:

"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 a 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:

"DECLASSIFY ON: (date)"

(2) For information to be declassified automatically upon occurrence of a specific event:

"DECLASSIFY ON: (description of event)"

(3) For information not to be declassified automatically:

"DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED or 'OADR' "

(4) 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 [1.5(c)].* 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 instruction:

(i) For an unclassified transmittal document:

"UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED"

(ii) For a classified transmittal document:

"UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal document standing alone)"

(2) *"Restricted Data" and "Formerly Restricted Data" [6.2(a)].* "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence sources or methods [1.5(c)].* Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by the Director of Central Intelligence:

"WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED"

(4) *Foreign government information [1.5(c)].* Documents that contain foreign government information 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) *Computer output [1.5(c)].* Documents that are generated as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(6) *Agency prescribed markings [1.5(c), 4.2(a), and 5.3(c)].* Officials delegated original classification authority by the President may prescribe additional markings to control reproduction and dissemination, including markings required for special access programs authorized by section 4.2(a) of the Order.

(f) *Electrically transmitted information (messages) [1.5(c)].* National security information that is transmitted electrically shall be marked as follows:

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

(2) A "CLASSIFIED BY" line is not required;

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

(i) For information to be declassified automatically on a specific date:

"DECL: (date)"

(ii) For information to be declassified upon occurrence of a specific event:

"DECL: (description of event)"

(iii) For information not to be automatically declassified which requires the originating agency's determination (see also § 2001.5(d)(3)):

"DECL: OADR"

(iv) 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)"

(4) Portion marking shall be as prescribed in § 2001.5(a)(3);

(5) Special markings as prescribed in § 2001.5(e) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended;

(ii) Information concerning intelligence sources or methods: "WNINTEL," unless proscribed by the Director of Central Intelligence;

(iii) Foreign government information: "FGI," 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 message shall be marked as if it were wholly of U.S. origin.

(6) Paper copies of electrically transmitted messages shall be marked as provided in § 2001.5(a) (1) and (2).

(g) *Changes in classification markings [1.4(b) and 4.1(b)].* When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is 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.

§ 2001.6 Limitations on classification [1.6(c)].

Before reclassifying information as provided in section 1.6(c) of the Order, the authorized official shall consider the following factors, which shall be addressed in the report to the Director of the Information Security Oversight Office:

(a) The elapsed time following disclosure;

(b) The nature and extent of disclosure;

(c) The ability to bring the fact of reclassification to the attention of persons to whom the information was disclosed;

(d) The ability to prevent further disclosure; and

(e) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Subpart B—Derivative Classification

§ 2001.20 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

§ 2001.21 Classification guides.

(a) *General [2.2(a)].* 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 declassified automatically without the approval of the originating agency.

(b) *Requirement for review [2.2(a)].* 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.

(c) *Waivers [2.2(c)].* An authorized official's 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.

§ 2001.22 Derivative identification and markings [1.5(c) and 2.1(b)].

Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.5(a) through (e) as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(a) *Classification authority.* The authority for classification shall be shown as follows:

"CLASSIFIED BY (description of source document or classification guide)"

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown as follows:

"CLASSIFIED BY MULTIPLE SOURCES"

In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

(b) *Declassification and downgrading instructions.* Dates or events for automatic declassification or downgrading, or the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on a "DECLASSIFY ON" line as follows:

"DECLASSIFY ON: (date; description of event; or 'ORIGINATING AGENCY'S DETERMINATION REQUIRED' (OADR))"

Subpart C—Declassification and Downgrading

§ 2001.30 Listing declassification and downgrading authorities [3.1(b)].

Agencies shall maintain a current listing of officials delegated declassification or downgrading authority by name, position, or other identifier. If possible, this listing shall be unclassified.

§ 2001.31 Systematic review for declassification [3.3].

(a) *Permanent records.* Systematic review is applicable only to those classified records and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-permanent records.* Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) *Responsibilities.* (1) In meeting responsibilities assigned by section 3.3(a) of the Order, the Archivist shall:

(i) Establish procedures, in consultation with the Director of the Information Security Oversight Office, for the systematic declassification review of permanent classified records accessioned into the National Archives and classified presidential papers or records under the Archivist's control;

(ii) Conduct systematic declassification reviews in accordance with guidelines provided by the head of the agency that originated the information; or, with respect to foreign government information, in accordance with guidelines provided by the head of the agency having declassification jurisdiction over the information, or, if no guidelines have been provided, in accordance with the general guidelines provided by the Director of the Information Security Oversight Office after coordination with the agencies having declassification authority over the information; or, with respect to presidential papers or records, in accordance with guidelines developed by the Archivist and approved by the National Security Council;

(iii) Conduct systematic declassification reviews of accessioned records and presidential papers or records as they become 30 years old, except for file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and information concerning cryptology created after 1945;

(iv) Conduct systematic declassification reviews of accessioned records and presidential papers or records in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945 and cryptology records created after 1945 as they become fifty years old;

(v) Establish systematic review priorities for accessioned records and presidential papers or records based on the degree of researcher interest and the potential for declassifying a significant portion of the information;

(vi) Re-review for declassification accessioned records and presidential papers or records upon the determination that the followup review will be productive, both in terms of researcher interest and the potential for declassifying a significant portion of the information.

(2) The Archivist may review for declassification, with the concurrence of the originating agency, accessioned records and presidential papers or records, prior to the timeframes established in paragraphs (c)(1) (iii) and (iv) of this section.

(3) Officials delegated original classification authority by the President under the Order or predecessor orders shall:

(i) Within six months of the effective date of the Order issue guidelines for systematic declassification review and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designed to assist the Archivist in the conduct of systematic reviews;

(ii) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;

(iii) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(4) Within six months of the effective date of the Order the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist and the agencies having declassification authority over the information, general guidelines for the systematic declassification review of foreign government information. Also within six months, agency heads may issue, in consultation with the Archivist and the Director of the Information Security Oversight Office, specific systematic declassification review guidelines for foreign government information over which the agency head has declassification authority. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

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

§ 2001.32 Mandatory review for declassification [3.4].

(a) *U.S. originated information.* (1) Each agency head shall publish in the Federal Register the identity of the person(s) or office(s) to which mandatory declassification review requests may be addressed.

(2) *Processing.* (i) *Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Agency responses to mandatory declassification review requests shall be governed by the amount of search and review time required to process the request. In responding to mandatory declassification 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 request. Agencies shall make a final determination within one year from the date of receipt except in unusual circumstances. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its

possession that were originated by another agency, it shall forward the request to that agency. The forwarding agency shall include a copy of the records requested together with its recommendations for action. Upon receipt, the originating agency shall process the request in accordance with § 2001.32(a)(2)(i). Upon request, the originating agency shall communicate its declassification determination to the referring agency.

(iii) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 30 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(b) *Foreign government information.* Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2001.32(a). 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.

(c) *Cryptologic and intelligence information.* Mandatory declassification 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.

(d) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 483a of title 31, United States Code. The schedules of fees published in the Federal Register by agencies in implementation of Executive Order 12065 shall remain in effect until they are revised.

§ 2001.33 Assistance to the Department of State [3.3(b)].

Heads of agencies should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

§ 2001.34 FOIA and Privacy Act requests [3.4].

Agency heads shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification. For information in special access programs established under the provisions of section 4.2 of the Order, the safeguarding requirements of Subpart D may be modified by the agency head responsible for creating the special access program as long as the modified requirements provide appropriate protection for the information.

§ 2001.41 Standards for security equipment [4.1(b) and 5.1(b)].

The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2001.42 Accountability [4.1(b)].

(a) *Top Secret.* Top Secret control officials shall be designated to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually. Agency heads may waive the requirement for an annual inventory of storage systems containing large volumes of Top Secret information upon a determination that the safeguarding of this information is not jeopardized by the inventory waiver. Waivers shall be in writing and be available for review by the Information Security Oversight Office.

(b) *Secret and Confidential.* Agency heads shall prescribe accountability or control requirements for Secret and Confidential information.

§ 2001.43 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum requirements for physical barriers.* (1) *Top Secret.* Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2001.41. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position changeable combination padlock. Heads of agencies shall prescribe supplementary controls for storage of Secret information in cabinets equipped with a steel lock bar. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, closed areas or similar facilities shall be controlled in accordance with requirements established by the appropriate agency head. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(b) *Combinations.* (1) *Equipment in service.* Combinations to dial-type locks shall be changed only by persons having an appropriate security clearance, and shall be changed whenever such equipment is placed in use; whenever a person knowing the combination no

longer requires access to it; whenever a combination has been subjected to possible compromise; whenever the equipment is taken out of service; or 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 level of classified information that is protected by the lock.

(2) *Equipment out of service.* When security equipment is taken out of service it shall be inspected to ensure that no classified information remains, and the built-in combination lock shall be reset to the standard combination 50–25–50. Combination padlocks shall be reset to the standard combination 10–20–30.

(c) *Keys.* Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

§ 2001.44 Transmittal [4.1(b)].

(a) *Preparation and receipting.* Classified information to be transmitted outside of a facility 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 addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads if conditions provide at least equivalent protection to prevent access by unauthorized persons.

(b) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for the purpose, or over authorized secure communications circuits.

(c) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) *The 50 States, the District of Columbia, and Puerto Rico.* Secret information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information, by the U.S. Postal Service registered mail, or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the head of the agency concerned.

(2) *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2001.44(c)(1) by one of the means established for Top Secret information, or by U.S. registered mail through Military Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

(d) *Transmittal of Confidential.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by the U.S. Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

(e) *Hand carrying of classified information.* Agency regulations shall prescribe procedures and appropriate restrictions concerning the escort or hand carrying of classified information, including the hand carrying of classsified information on commercial carriers.

§ 2001.45 Special access programs [1.2(a) and 4.2(a)].

Agency heads designated pursuant to section 1.2(a) of the Order may create or continue a special access program if:

(a) Normal management and safeguarding procedures do not limit access sufficiently; and

(b) the number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2001.46 Reproduction controls [4.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electrically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret and Confidential documents may be reproduced to the extent required by operational needs.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

§ 2001.47 Loss or possible compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The agency under whose cognizance the loss or possible compromise occurred shall initiate an inquiry to (a) determine cause, (b) place responsibility, and (c) take corrective measures and appropriate administrative, disciplinary, or legal action.

§ 2001.48 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, United States Code, which govern disposition of Federal records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude recognition or reconstruction of the classified information or material.

§ 2001.49 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for: (a) Protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct supervision of

authorized persons; and (b) meeting accountability requirements prescribed by the head of the agency.

§ 2001.58 Emergency planning [4.1(b)].

Agencies shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2001.59 Emergency authority [4.1(b)].

Those officials delegated original classification authority by the President may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

Subpart E—Implementation and Review

§ 2001.60 Agency regulations [5.3(b)].

Each head of an agency shall issue regulations in accordance with 5 U.S.C. 552(a) to implement the Order and 32 CFR Part 2001 no later than December 31, 1982. Those portions that affect members of the public shall include, at a minimum, information relating to the agency's mandatory declassification review program and instructions for submitting suggestions or complaints regarding the agency's information security program.

§ 2001.61 Security education [5.3(a)].

Each agency that creates or handles national security information is required under the Order to establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

§ 2001.62 Oversight [5.3(a)].

Agency heads shall require that periodic formal reviews be made to ensure compliance with the provisions of the Order and ISOO directives.

Subpart F—General Provisions

§ 2001.70 Definitions [6.1].

(a) *Original classification authority.* The authority vested in an executive branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(b) *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 on a derivative basis.

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

(d) *Multiple sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from more than one source.

(e) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(f) *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."

(g) *Intelligence activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(h) *Special activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies, or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

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

§ 2001.71 Publication and effective date [6.2(e)].

Part 2001 shall be published in the Federal Register. It shall become effective August 1, 1982.

Steven Garfinkel,

Director, Information Security Oversight Office.

June 23, 1982.

[FR Doc. 82-17295 Filed 6-23-82; 10:37 am]

BILLING CODE 6820-AF-M