

Pt. 2

be filed, the officer designated to receive service of process and the addresses for delivery of requests, appeals, and service of process. In addition, it references the notice of systems of records and notices of the routine uses of the information in the system required by 5 U.S.C. 552a(4) and (11) and published biennially by the Office of the Federal Register in "Privacy Act Issuances."

2. *Requests for notification and access to records and accountings of disclosures.* Initial determinations under 31 CFR 1.26, whether to grant requests for notification and access to records and accountings of disclosures for FinCEN will be made by the Freedom of Information/Privacy Act officer, FinCEN. Requests may be mailed to: Privacy Act Request, Financial Crimes Enforcement Network, Post Office Box 39, Vienna, VA 22183.

3. *Requests for amendments of records.* Initial determinations under 31 CFR 1.27(a) through (d) whether to grant requests to amend records maintained by FinCEN will be made by the Freedom of Information/Privacy Act officer, FinCEN. Requests may be mailed to: Privacy Act Request, Financial Crimes Enforcement Network, Post Office Box 39, Vienna, VA 22183.

4. *Verification of Identity.* An individual seeking notification or access to records, or seeking to amend a record, or seeking an accounting of disclosures, must satisfy one of the following identification requirements before action will be taken by FinCEN on any such request:

(i) An individual may establish identity through the mail by a signature, address, and one other identifier such as a photocopy of a driver's license or other official document bearing the individual's signature.

(ii) Notwithstanding this paragraph (4)(i), an individual may establish identity by providing a notarized statement, swearing or affirming to such individual's identity and to the fact that the individual understands the penalties provided in 5 U.S.C. 552a(i)(3) for requesting or obtaining access to records under false pretenses.

(iii) Notwithstanding this paragraph (4)(i) and (ii), the Freedom of Information Act/Privacy Act Officer or other designated official may require additional proof of an individual's identity before action will be taken on any request, if such official determines that it is necessary to protect against unauthorized disclosure of information in a particular case. In addition, a parent of any minor or a legal guardian of any individual will be required to provide adequate proof of legal relationship before such person may act on behalf of such minor or such individual.

5. *Administrative appeal of initial determinations refusing amendment of records.* Appellate determinations refusing amendment of records under 31 CFR 1.27(e) including extensions of time on appeal with respect to the records of FinCEN will be made by the Direc-

31 CFR Subtitle A (7-1-06 Edition)

tor of FinCEN or the delegate of the Director. Appeals should be addressed to: Privacy Act Amendment Appeal, Financial Crimes Enforcement Network, Post Office Box 39, Vienna, VA 22183.

6. *Statements of Disagreement.* "Statements of Disagreement" as described in 31 CFR 1.27(e)(4) shall be filed with the official signing the notification of refusal to amend at the address indicated in the letter of notification within 35 days of the date of such notification and should be limited to one page.

7. *Service of Process.* Service of process will be received by the Chief Counsel of FinCEN and shall be delivered to the following location: Office of Chief Counsel, Financial Crimes Enforcement Network, Post Office Box 39, Vienna, VA 22183.

8. *Biennial notice of systems of records.* The biennial notice of systems of records is published by the Office of the Federal Register, as specified in 5 U.S.C. 552a(f). The publication is entitled "Privacy Act Issuances." Any specific requirements for access, including identification requirements, in addition to the requirements set forth in 31 CFR 1.26 and 1.27 and paragraph 4 of this appendix are indicated in the notice for the pertinent system.

[68 FR 55311, Sept. 25, 2003]

PART 2—NATIONAL SECURITY INFORMATION

Subpart A—Original Classification

Sec.

- 2.1 Classification levels [1.1(a)].
- 2.2 Classification Authority.
- 2.3 Listing of original classification authorities.
- 2.4 Record requirements.
- 2.5 Classification categories.
- 2.6 Duration of classification.
- 2.7 Identification and markings [1.5(a), (b) (c)].
- 2.8 Limitations on classification [1.6(c)].

Subpart B—Derivative Classification

- 2.9 Derivative Classification Authority.
- 2.10 Listing derivative classification authorities.
- 2.11 Use of derivative classification [2.1].
- 2.12 Classification guides.
- 2.13 Derivative identification and markings [1.5(c) and 2.1(b)].

Subpart C—Downgrading and Declassification

- 2.14 Listing downgrading and declassification authorities [3.1(b)].
- 2.15 Declassification policy [3.1].
- 2.16 Downgrading and declassification markings.

Office of the Secretary of the Treasury

§ 2.2

- 2.17 Systematic review for declassification [3.3].
- 2.18 Mandatory declassification review [3.4].
- 2.19 Assistance to the Department of State [3.3(b)].
- 2.20 Freedom of Information/Privacy Act requests [3.4].

Subpart D—Safeguarding

- 2.21 General [4.1].
- 2.22 General restrictions on access [4.1].
- 2.23 Access by historical researchers and former presidential appointees [4.3].
- 2.24 Dissemination [4.1(d)].
- 2.25 Standards for security equipment [4.1(b) and 5.1(b)].
- 2.26 Accountability procedures [4.1(b)].
- 2.27 Storage [4.1(b)].
- 2.28 Transmittal [4.1(b)].
- 2.29 Telecommunications and computer transmissions.
- 2.30 Special access programs [1.2(a) and 4.2(a)].
- 2.31 Reproduction controls [4.1(b)].
- 2.32 Loss or possible compromise [4.1(b)].
- 2.33 Responsibilities of holders [4.1(b)].
- 2.34 Inspections [4.1(b)].
- 2.35 Security violations.
- 2.36 Disposition and destruction [4.1(b)].
- 2.37 National Security Decision Directive 197.

Subpart E—Implementation and Review

- 2.38 Departmental management.
- 2.39 Bureau administration.
- 2.40 Emergency planning [4.1(b)].
- 2.41 Emergency authority [4.1(b)].
- 2.42 Security education [5.3(a)].

Subpart F—General Provisions

- 2.43 Definitions [6.1].

AUTHORITY: 31 U.S.C. 321; E.O. 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333.

SOURCE: 55 FR 1644, Jan. 17, 1990, unless otherwise noted.

Subpart A—Original Classification

§ 2.1 Classification levels [1.1(a)].¹

(a) National security information (hereinafter also referred to as “classified information”) shall be classified at one of the following three levels:

(1) *Top Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected

to cause exceptionally grave damage to the national security.

(2) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) *Limitations [1.1(b)]*. Markings other than “Top Secret,” “Secret,” and “Confidential,” shall not be used to identify national security information. No other terms or phrases are to be used in conjunction with these markings to identify national security information, such as “Secret/Sensitive” or “Agency Confidential”. The terms “Top Secret,” “Secret,” and “Confidential” are not to be used to identify non-classified Executive Branch information. The administrative control legend, “Limited Official Use”, is authorized in Treasury Directive 71-02, “Safeguarding Officially Limited Information,” which requires that information so marked is to be handled, safeguarded and stored in a manner equivalent to national security information classified Confidential.

(c) *Reasonable Doubt [1.1(c)]*. 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 of this regulation, pending a determination about its classification. Upon a final determination of a need for classification, the information that is classified shall be marked as provided in § 2.7. 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 a determination of its classification level. Upon a final determination of its classification level, the information shall be marked as provided in § 2.7.

§ 2.2 Classification Authority.

Designations of original classification authority for national security information are contained in Treasury Order (TO) 102-19 (or successor order),

¹Related references are related to sections of Executive Order 12356, 47 FR 14874, April 6, 1982.

§ 2.3

which is published in the FEDERAL REGISTER. The authority to classify inheres within the office and may be exercised by a person acting in that capacity. There may be additional redelegations of original classification authority made pursuant to TO 102-19 (or successor order). Officials with original classification authority may derivatively classify at the same classification level.

[63 FR 14357, Mar. 25, 1998]

§ 2.3 Listing of original classification authorities.

Delegations of original Top Secret, Secret and Confidential classification authority shall be in writing and be reported annually to the Departmental Director of Security, who shall maintain such information on behalf of the Assistant Secretary (Management). These delegations are to be limited to the minimum number absolutely required for efficient administration. Periodic reviews and evaluations of such delegations shall be made by the Departmental Director of Security to ensure that the officials so designated have demonstrated a continuing need to exercise such authority. If, after reviewing and evaluating the information, the Departmental Director of Security determines that such officials have not demonstrated a continuing need to exercise such authority, the Departmental Director of Security shall recommend to the Assistant Secretary (Management), as warranted, the reduction or elimination of such authority. The Assistant Secretary (Management) shall take appropriate action in consultation with the affected official(s) and the Departmental Director of Security. Such action may include relinquishment of this authority where the Assistant Secretary (Management) determines that a firm basis for retention does not exist.

§ 2.4 Record requirements.

The Departmental Director of Security shall maintain a listing by name, position title and delegated classification level, of all officials in the Departmental Offices who are authorized under this regulation to originally classify information as Top Secret, Secret or Confidential. Officials within

31 CFR Subtitle A (7-1-06 Edition)

the Departmental Offices with Top Secret classification authority shall report in writing on TD F 71-01.14 (Report of Authorized Classifiers) to the Departmental Director of Security, the names, position titles and authorized classification levels of the officials designated by them in writing to have original Secret or Confidential classification authority. The head of each bureau shall maintain a similar listing of all officials in his or her bureau authorized to apply original Secret and Confidential classification and shall provide a copy of TD F 71-01.14, reflecting the list of officials so authorized, to the Departmental Director of Security. These listings shall be compiled and reported no less than annually each October 15th as required by Treasury Directive 71-01, "Agency Information Security Program Data".

§ 2.5 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. Such classification on an aggregate 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 under procedures contained in § 2.32.

§ 2.6 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 possible declassification.

(b) *Authority to Extend Automatic De-classification Determinations [1.4(b)].* The authority to extend classification of information subject to automatic declassification under any predecessor Executive Order to the Order 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 the classification on other than a document-by-document basis shall be reported to the Assistant Secretary (Management) who shall, in turn, report this fact to the Director of the Information Security Oversight Office.

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

The information security system requires that standard markings be applied to classified information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper and electronically created documents shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper and electronically created documents, including file folders, film, tape, etc., 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 information that requires protection as classified information under the Order; the highest level of classification contained in a document; the classification level of each page and, in abbreviated form, the classification of 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. 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 and last pages bearing text, and on the outside of the back cover (if any).

(2) *Page Marking.* Each interior page of a classified document is to 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.* Only the Secretary of the Treasury may waive the portion marking requirement for specified classes of documents or information upon a written determination that:

(i) There will be minimal circulation of the specified documents or information and minimal potential usage of the 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.

(b) 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 either 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. The symbol, "(LOU)" shall be used for Limited Official Use information. 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, as well as 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, e.g. "Entire Text is Classified Confidential." If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(c) *Classification Authority.* If the original classifier is other than the signer or approver of the document, his or her identity shall be shown at the bottom of the first and last pages as

§2.7

31 CFR Subtitle A (7-1-06 Edition)

follows: "CLASSIFIED BY (identification of original classification authority)"

(d) Bureau and Office of Origin. If the identity of the originating bureau or office is not apparent on the face of the document, it shall be clearly indicated below the "CLASSIFIED BY" line.

(e) Downgrading and Declassification Instructions. Downgrading and, as applicable, declassification instructions shall be shown as follows:

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

Classified by _____
Office _____
Declassify on (date) _____

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

Classified by _____
Office _____
Declassify on (description of event) _____

(3) For information not to be declassified automatically:

Classified by _____
Office _____
Declassify on Origination Agency's Determination Required or "OADR" _____

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

Classified by _____
Office _____
Downgrade to _____
on (date or description of event) _____

(f) Special Markings—(1) Transmittal Documents [1.5(c)]. A transmittal document shall indicate on its first page and last page, if any, the highest classification of any information transmitted by it. It shall also include on the first and last pages the following or similar instruction:

(i) For an unclassified transmittal document:

Unclassified When Classified
Enclosure(s) Detached.

(ii) For a classified transmittal document:

Upon Removal of Attachment(s)
this Document is _____

(classification level of the transmittal document alone), or:

This Document is Classified _____

with Unclassified Attachment(s).

(2) Restricted Data or Formerly Restricted Data [6.2(a)]. Restricted Data or Formerly Restricted Data shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended. Restricted Data is information dealing with the design, manufacture, or utilization of atomic weapons, production of special nuclear material or use of special nuclear material in the production of energy. Formerly Restricted Data is classified information that has been removed from the "restricted data" category but still remains classified. It relates primarily to the military utilization of atomic weapons.

(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 prescribed by the Director of Central Intelligence: "WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED" To avoid confusion as to the extent of dissemination and use restrictions governing the information involved, this marking may not be used in conjunction with special access or sensitive compartmented information controls.

(4) Foreign Government Information (FGI) [1.5(c)]. 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 information is foreign government information that must be concealed, given the relationship or understanding with the foreign government providing the information, the marking shall not be used and the document shall be marked as if it were wholly of United States origin. However, such a marking must be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the original or record copy of the document or information.

(5) National Security Information [4.1(c)]. Classified information furnished outside the Executive Branch shall show the following marking:

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to
Administrative and Criminal Sanctions

(6) *Automated Data Processing (ADP) and Computer Output [1.5(c)]*. (i) Documents that are generated via ADP or as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(ii) Removable information storage media, however, will bear external labels indicating the security classification of the information and associated security markings, as applicable, such as handling caveats and dissemination controls. Examples of such media include magnetic tape reels, cartridges, and cassettes; removable disks, disk cartridges, disk packs, and diskettes, including “floppy” or flexible disks; paper tape reels; and magnetic and punched cards. Two labels may be required on each medium: a color coded security classification label, i.e., orange Standard Form 706 (Top Secret label), red SF 707 (Secret label), blue SF 708 (Confidential label), purple SF 709 (Classified label), green SF 710 (Unclassified label); and a white SF 711 (Data Descriptor label). National stock numbers of the labels, which are available through normal Federal Supply channels, are as follows: SF 706, 7540-01-207-5536; SF 707, 7450-01-207-5537; SF 708, 7450-01-207-5538; SF 709, 7540-01-207-5540; SF 710, 7540-01-207-5539 and SF 711, 7540-01-207-5541. Treasury Directive 71-02 provides for the use of a green “Officially Limited Information” label, TD F 71-05.2, to identify information so marked.

(iii) In a mixed environment in which classified and unclassified information is processed or stored, the “Unclassified” label must be used to identify the media containing unclassified information. In environments in which only unclassified information is processed or stored, the use of the “Unclassified” label is not required. Unclassified media, however, that are on loan from (and must be returned to) vendors do not require the “Unclassified” label, but each requires a Data Descriptor label with the words, “Unclassified Vendor Medium” entered on it.

(iv) Each medium shall be appropriately affixed with a classification label and, as applicable, with a Data Descriptor label at the earliest prac-

ticable time as soon as the proper security classification or control has been established. Labels shall be conspicuously placed on media in a manner that will not adversely affect operation of the equipment in which the media is used. Once applied, the label is not to be removed. A label to identify a higher level of classification may, however, be applied on top of a lower classification level in the event that the content of the media changes, e.g., from Confidential to Secret. A lower classification label may not be applied to media already bearing a higher classification label. Personnel shall be responsible for appropriately labeling and controlling ADP and computer storage media within their possession.

(g) *Electronically Transmitted Information (Messages) [1.5(c)]*. Classified information that is transmitted electronically 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 §2.7(e)(3)): “DECL: OADR”;

(iv) For information to be automatically downgraded: “DOWNGRADE TO (classification level to which the information is to be downgraded) ON (date or description of event on which downgrading is to occur)”.

(4) Portion marking shall be as prescribed in §2.7(a)(3);

(5) Specially designated markings as prescribed in §2.7(f) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) Restricted Data or Formerly Restricted Data;

(ii) Information concerning intelligence sources or methods;

§2.8

“WNINTEL,” unless otherwise prescribed by the Director of Central Intelligence; and

(iii) Foreign Government Information (FGI).

(6) Paper copies of electronically transmitted messages shall be marked as provided in §2.7(a) (1), (2), and (3).

(h) *Changes in Classification Markings [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 on their copy of the information 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.

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

(a) Before reclassifying information as provided in section 1.6(c) of the Order, authorized officials, who must have original classification authority and jurisdiction over the information involved, shall consider the following factors which shall be addressed in a report to the Assistant Secretary (Management) who shall in turn forward a report to the Director of the Information Security Oversight Office:

(1) The elapsed time following disclosure;

(2) The nature and extent of disclosure;

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

(4) The ability to prevent further disclosure; and

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

(b) Information may be classified or reclassified after it has been requested under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5

31 CFR Subtitle A (7–1–06 Edition)

U.S.C. 552a), or the mandatory declassification review provisions of the Order if such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the Secretary of the Treasury, the Deputy Secretary, the Assistant Secretary (Management) or an official with original Top Secret classification authority. Such reclassification actions shall be reported in writing to the Departmental Director of Security.

(c) In no case may information be classified or reclassified in order 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.

Subpart B—Derivative Classification

§2.9 Derivative Classification Authority.

Designations of derivative classification authority for national security information are contained in Treasury Order 102–19 (or successor order). The authority to derivatively classify inheres within the office and may be exercised by a person acting in that capacity. There may be additional redelegations of derivative classification authority made pursuant to TO 102–19 (or successor order). Officials identified in Treasury Order 102–19 (or successor order) may also administratively control and decontrol sensitive but unclassified information using the legend “Limited Official Use” and may redelegate their authority to control and decontrol. Such redelegations shall be in writing on TD F 71–01.20 “Designation of Controlling/Decontrolling Officials” (or successor form).

[63 FR 14357, Mar. 25, 1998]

§2.10 Listing derivative classification authorities.

Delegations of derivative classification authority to officials not otherwise identified in §2.9, shall be in writing and reported annually each October

15th to the Departmental Director of Security on TD F 71-01.18 (Report of Authorized Derivative Classifiers). Such delegations shall be limited to the minimum number absolutely required for efficient administration. Periodic reviews and evaluations of such delegations shall be made by the Departmental Director of Security to ensure that officials so designated have demonstrated a continuing need to exercise such authority. If after reviewing and evaluating the information the Departmental Director of Security determines that such officials have not demonstrated a continuing need to exercise such authority, the Departmental Director of Security shall recommend to the Assistant Secretary (Management), as warranted, the reduction or elimination of such authority. The Assistant Secretary (Management) shall take appropriate action in consultation with the affected official(s) and the Departmental Director of Security. Such action may include relinquishment of this authority where the Assistant Secretary (Management) determines that a firm basis for retention does not exist.

§2.11 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 approved classification guide. If an individual 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 an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade or declassify the information for a final determination. A sample marking of derivatively classified documents is set forth in §2.13.

§2.12 Classification guides.

(a) *General* [2.2(a)]. A classification guide is a reference manual which as-

sists document drafters and document classifiers in determining what types or categories of material have already been classified. The classification guide shall, at a minimum:

- (1) Identify and 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 i.e., "OADR".

(b) *Review and Record Requirements* [2.2(a)]. (1) Each classification guide shall be kept current and shall be reviewed at least once every two years and updated as necessary. Each office within the Departmental Offices and the respective offices of each Treasury bureau possessing original classification authority for national security information shall maintain a list of all classification guides in current use by them. A copy of each such classification guide in current use shall be furnished to the Departmental Director of Security who shall maintain them on behalf of the Assistant Secretary (Management).

(2) Each office and bureau that prepares and maintains a classification guide shall also maintain a record of individuals authorized to apply derivative classification markings in accordance with a classification guide. This record shall be maintained on TD F 71-01.18 (Report of Authorized Derivative Classifiers) which shall be reported annually each October 15th to the Departmental Director of Security.

(c) *Waivers* [2.2(c)]. Any authorized official desiring a waiver of the requirement to issue a classification guide shall submit in writing to the Assistant Secretary (Management) a request for approval of such a waiver. Any request for a waiver shall contain, at a minimum, an evaluation of the following factors:

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

§2.13

(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.

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

Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in §2.7 (a) through (f), 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:

Derivatively Classified by _____
Office _____
Derived from _____
Declassify on _____

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown on the "DERIVED FROM" line as follows: "MULTIPLE CLASSIFIED SOURCES". In these cases, the derivative classifier must 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 "MULTIPLE CLASSIFIED SOURCES" shall cite the *source* document on its "DERIVED FROM" line rather than the term: "MULTIPLE CLASSIFIED SOURCES". Preparers of such documentation shall ensure that the identification of the derivative classifier is indicated. Use of the term "MULTIPLE CLASSIFIED SOURCES," is *not* to be a substitute for the identity of the derivative classification authority.

(b) *Downgrading and Declassification Instructions.* Dates or events for automatic downgrading or declassification shall be carried forward from the source document. This includes the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indi-

31 CFR Subtitle A (7-1-06 Edition)

cate that the document is not to be downgraded or declassified automatically, or instructions as directed by a classification guide, which shall be shown on a "DOWNGRADE TO" or "DECLASSIFY ON" line as follows:

DOWNGRADE TO _____
ON (*date, description of event, or OADR*) or,
DECLASSIFY ON (*date, description of event, or OADR*)

Subpart C—Downgrading and Declassification

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

Downgrading and declassification authority may be exercised by the official authorizing the original classification, if that official is still serving in the same position; a successor in that capacity; a supervisory official of either; or officials delegated such authority in writing by the Secretary of the Treasury or the Assistant Secretary (Management). Such officials may *not* downgrade or declassify information which is classified at a level exceeding their own designated classification authority. A listing of officials delegated such authority, in writing, shall be identified on TD F 71-01.11 (Report of Authorized Downgrading and Declassification Officials) and reported annually each October 15th to the Departmental Director of Security who shall maintain them on behalf of the Assistant Secretary (Management). Current listings of officials so designated shall be maintained by Treasury bureaus and offices within the Departmental Offices.

[55 FR 1644, Jan. 17, 1990; 55 FR 13134, Apr. 9, 1990]

§2.15 Declassification policy [3.1].

In making determinations under section 3.1(a) of the Order, officials shall respect the intent of the Order to protect foreign government information and confidential foreign sources.

§2.16 Downgrading and declassification markings.

Whenever a change is made in the original classification or in the dates of downgrading or declassification of any classified information, it shall be promptly and conspicuously marked to

indicate the change, the authority for the action, the date of the action, and the identity of the person taking the action. Earlier classification markings shall be cancelled or otherwise obliterated when practicable. See also § 2.7(h).

§ 2.17 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 Classified 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 declassification review request.

(c) *Systematic Declassification Review Guidelines [3.3(a)].* As appropriate, guidelines for systematic declassification review shall be issued by the Assistant Secretary (Management) in consultation with the Archivist of the United States, the Director of the Information Security Oversight Office and Department officials, to assist the Archivist in the conduct of systematic reviews. Such guidelines shall be reviewed and updated at least every five years unless earlier review is requested by the Archivist.

(d) *Foreign Government Systematic Declassification Review Guidelines [3.3(a)].* As appropriate, guidelines for systematic declassification review of foreign government information shall be issued by the Assistant Secretary (Management) in consultation with the Archivist of the United States, the Director of the Information Security Oversight Office, Department officials and other agencies having declassification authority over the information. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(e) *Special Procedures.* The Department shall be bound by the special procedures for systematic review of classi-

fied 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.

§ 2.18 Mandatory declassification review [3.4].

(a) Except as provided by section 3.4 (b) of the Order, all information classified by the Department under the Order or any predecessor Executive Order shall be subject to declassification review by the Department, if:

(1) The request is made by a United States citizen or permanent resident alien, a Federal agency, or a state or local government;

(2) The request describes the document or material containing the information with sufficient specificity to enable the Department to locate it with a reasonable amount of effort; and

(3) The requester provides substantial proof as to his or her United States citizenship or status as a permanent resident alien, e.g., a copy of a birth certificate, a certificate of naturalization, official passport or some other means of identity which sufficiently describes the requester's status. A permanent resident alien is any individual, who is not a citizen or national of the United States, who has been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws, such status not having changed. Permanent means a relationship of continuing or lasting nature, as distinguished from temporary, but a relationship may be permanent even though it is one that may be dissolved eventually at the instance either of the United States or of the individual, in accordance with law.

(b) *Processing—(1) Initial Requests for Classified Records Originated by the Department.* Requests for mandatory declassification review shall be directed to the Departmental Office of Security, 1500 Pennsylvania Avenue, NW., Washington, DC 20220. Upon receipt of each request for declassification, pursuant to section 3.4 of the Order, the following procedures shall apply:

§ 2.18

(i) The Departmental Office of Security shall acknowledge the receipt of the request in writing.

(ii) 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 Treasury personnel to locate the records containing the information sought with a reasonable amount of effort. Whenever a request does not reasonably describe the information sought, the requester shall be notified by the Departmental Office of Security that unless additional information is provided or the scope of the request is narrowed, no further action will be undertaken.

(iii) The Departmental Office of Security shall determine the appropriate office or bureau to take action on the request and shall forward the request to that office or bureau.

(iv) In responding to mandatory declassification review requests, the appropriate reviewing officials shall make a prompt declassification determination. The Departmental Office of Security shall notify the requester if additional time is needed to process the request. Reviewing officials shall also identify the amount of search and/or review time required to process the request. The Department 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, reasonable efforts, consistent with other applicable laws, will be made to release those declassified portions of the requested information which constitute a coherent segment. Upon the denial or partial denial of an initial request, the Departmental Office of Security shall also notify the requester of the right of an administrative appeal which must be filed with the Assistant Secretary (Management) within 60 days of receipt of the denial.

(v) When the Department receives a mandatory declassification review request for records in its possession that were originated by another agency, the Departmental Office of Security shall forward the request to that agency. The Departmental Office of Security shall include a copy of the records re-

31 CFR Subtitle A (7-1-06 Edition)

quested together with the Department's recommendations for action. Upon receipt, the originating agency shall process the request in accordance with the Directive 32 CFR 2001.32(a)(2)(i). The originating agency shall also be requested to communicate its declassification determination to Treasury.

(vi) When another agency forwards to the Department a request for information in that agency's custody that has been classified by Treasury, the Departmental Office of Security shall:

(A) Advise the other agency as to whether it can notify the requester of the referral;

(B) Review the classified information in coordination with other agencies that have a direct interest in the subject matter; and

(C) Respond to the requester in accordance with the procedures in § 2.18(b)(1)(iv). If requested, Treasury's determination shall be communicated to the referring agency.

(vii) Appeals of denials of a request for declassification shall be referred to the Assistant Secretary (Management) who 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 Assistant Secretary (Management) shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The Assistant Secretary (Management) shall notify the requester in writing of the final determination and, as applicable, the reasons for any denial.

(viii) Except as provided in this paragraph, the Department shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2.18(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 upon receipt of the request, the Department determines that Treasury is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation

Office of the Secretary of the Treasury

§ 2.22

with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(ix) Mandatory declassification review requests for cryptologic information and/or 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.

(x) The fees to be charged for mandatory declassification review requests shall be for search and/or review and duplication. The fee charges for services of Treasury personnel involved in locating and/or reviewing records shall be at the rate of a GS-10, Step 1, for each hour or fraction thereof, except that no charge shall be imposed for search and/or review consuming less than one hour.

(A) Photocopies per page up to 8½" by 14" shall be charged at the rate of 10 cents each except that no charge will be imposed for reproducing ten (10) pages or less when search and/or review time requires less than one hour.

(B) When it is estimated that the costs associated with the mandatory declassification review request will exceed \$100.00, the Departmental Office of Security shall notify the requester of the likely cost and obtain satisfactory written assurance of full payment or may require the requester to make an advance payment of the entire fee before continuing to process the request. The Department reserves the right to request prepayment after a mandatory declassification review request is processed and before documents are released. In the event the requester does not agree to pay the actual charges, he or she shall advise how to proceed with the mandatory declassification review request. Failure of a requester to pay charges after billing will result in future requests not being honored.

(C) In order for a requester's initial request to be processed it shall be accompanied by a statement that he or she is agreeable to paying fees for search and/or review and copying. In the event the initial request does not include this statement, processing of the request will be held in abeyance

until such time as the required statement is received. Failure to provide a response within a reasonable amount of time will serve as the basis for administratively terminating the mandatory declassification review request.

(D) Payment of fees shall be made by check or money order payable to the Treasurer of the United States. Fees levied by the Department of the Treasury for mandatory declassification review requests are separate and distinct from any other fees which might be imposed by a Presidential Library, the National Archives and Records Administration or another agency or department.

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

The Secretary of the Treasury shall assist the Department of State in its preparation of the "Foreign Relations of the United States" series by facilitating access to appropriate classified material in Treasury custody and by expediting declassification review of documents proposed for inclusion in the series.

§ 2.20 Freedom of Information/Privacy Act requests [3.4].

The Department of the Treasury shall process requests for records containing classified national security information that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, as amended, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2.21 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.

§ 2.22 General restrictions on access [4.1].

(a) *Determination of Need-To-Know.* Classified information shall be made available to a person only when the possessor of the classified information establishes in each instance, except as

§2.23

provided in section 4.3 of the Order, that access is essential to the accomplishment of official United States Government duties or contractual obligations.

(b) *Determination of Trustworthiness.* A person is eligible for access to classified information only after a showing of trustworthiness as determined by the Secretary of the Treasury based upon appropriate investigations in accordance with applicable standards and criteria.

(c) *Classified Information Nondisclosure Agreement.* Standard Form 312 (Classified Information Nondisclosure Agreement) or the prior SF 189, bearing the same title, are nondisclosure agreements between the United States and an individual. The execution of either the SF 312 or SF 189 agreement by an individual is necessary before the United States Government may grant the individual access to classified information. Bureaus and the Departmental Offices must retain executed copies of the SF 312 or prior SF 189 in file systems from which the agreements can be expeditiously retrieved in the event the United States must seek their enforcement. Copies or legally enforceable facsimiles of the SF 312 or SF 189 must be retained for 50 years following their date of execution. The national stock number for the SF 312 is 7540-01-280-5499.

§2.23 Access by historical researchers and former presidential appointees [4.3].

(a) Access to classified information may be granted only as is essential to the accomplishment of authorized and lawful United States Government purposes. This requirement may be waived, however, for persons who:

(1) Are engaged in historical research projects, or

(2) Previously have occupied policymaking positions to which they were appointed by the President.

(b) Access to classified information may be granted to historical researchers and to former Presidential appointees upon a determination of trustworthiness; a written determination that such access is consistent with the interests of national security; the requestor's written agreement to safe-

31 CFR Subtitle A (7-1-06 Edition)

guard classified information; and the requestor's written consent to have his or her notes and manuscripts reviewed to ensure that no classified information is contained therein. The conferring of historical researcher status does not include authorization to release foreign government information or other agencies' classified information per §2.24 of this part. By the terms of section 4.3(b)(3) of the Order, former Presidential appointees not engaged in historical research may *only* be granted access to classified documents which they "originated, reviewed, signed or received while serving as a Presidential appointee." Coordination shall be made with the Departmental Director of Security with respect to the required written agreements to be signed by the Department and such historical researchers or former Presidential appointees, as a condition of such access and to ensure the safeguarding of classified information.

(c) If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to 31 U.S.C. 9701, the requestor shall be so notified and the fees may be imposed. Treasury's fee schedule identified in §2.18(b)(1)(x), applicable to mandatory declassification review, shall also apply to fees charged for services provided to historical researchers and former Presidential appointees for search and/or review and copying.

§2.24 Dissemination [4.1(d)].

Except as otherwise provided by section 102 of the National Security Act of 1947, 61 Stat. 495, 50 U.S.C. 403, classified information originating in another agency may not be disseminated outside the Department without the consent of the originating agency.

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

The Administrator of General Services issues (in coordination with agencies originating classified information), establishes and publishes uniform standards, specifications, and supply schedules for security equipment designed to provide for secure storage and to destroy classified information.

Treasury bureaus and the Departmental Offices may establish more stringent standards for their 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.

§ 2.26 Accountability procedures
[4.1(b)].

(a) *Top Secret Control Officers.* Each Treasury bureau and the Departmental Offices shall designate a primary and alternate Top Secret Control Officer. Within the Departmental Offices, the Top Secret Control Officer function will be established in the Office of the Executive Secretary for collateral Top Secret information and in the Office of the Special Assistant to the Secretary (National Security) with respect to sensitive compartmented information. The term "collateral" refers to national security information classified Confidential, Secret, or Top Secret under the provisions of Executive Order 12356 or prior Orders, for which special intelligence community systems of compartmentation (such as sensitive compartmented information) or special access programs are not formally established. Top Secret Control Officers so designated must have a Top Secret security clearance and shall:

(1) Initially receive all Top Secret information entering their respective bureau, including the Departmental Offices. Any Top Secret information received by a Treasury bureau or Departmental Offices employee shall be immediately hand carried to the designated Top Secret Control Officer for proper accountability.

(2) Maintain current accountability records of Top Secret information received within their bureau or office.

(3) Ensure that Top Secret information is properly stored and that Top Secret information under their control is personally destroyed, when required. Top Secret information must be destroyed in the presence of an appropriately cleared official who shall actually witness such destruction. Accordingly, the use of burnbags to store Top Secret information, pending final de-

struction at a later date, is not authorized.

(4) Ensure that prohibitions against reproduction of Top Secret information are strictly followed.

(5) Conduct annual physical inventories of Top Secret information. An inventory shall be conducted in the presence of an individual with an appropriate security clearance. The inventory shall be completed annually and signed by the Top Secret Control Officer and the witnessing individual.

(6) Ensure that Top Secret documents are downgraded, declassified, retired or destroyed as required by regulations or other markings.

(7) Attach a TD F 71-01.7 (Top Secret Document Record) to the first page or cover of each copy of Top Secret information. The Top Secret Document Record shall be completed by the Top Secret Control Officer and shall serve as a permanent record.

(8) Ensure that all persons having access to Top Secret information sign the Top Secret Document Record. This also includes persons to whom oral disclosure of the contents is made.

(9) Maintain receipts concerning the transfer and destruction of Top Secret information. Record all such actions on the Top Secret Document Record which shall be retained for a minimum of three years.

(10) As received, number in sequence each Top Secret document in a calendar year series (e.g. TS 89-001). This number shall be posted on the face of the document and on all forms required for control of Top Secret information.

(11) Attach a properly executed TD F 71-01.5 (Classified Document Record of Transmittal) when a Top Secret document is transmitted internally or externally.

(12) Verify, prior to releasing Top Secret information, that the recipient has both a security clearance and is authorized access to such information.

(13) Report, in writing, all Top Secret documents unaccounted for to the Assistant Secretary (Management) who shall take appropriate action in conjunction with the Departmental Director of Security.

(14) Assure that no individual within his or her office or bureau transmits

§2.26

31 CFR Subtitle A (7-1-06 Edition)

Top Secret information to another individual or office without the knowledge and consent of the Top Secret Control Officer.

(15) Ensure upon receipt that a Standard Form 703 (Top Secret Cover Sheet) is affixed to such information.

(16) Notify office and/or bureau employees annually in writing of the designated control point for all incoming and outgoing Top Secret information.

(17) Be notified as to the transmission, per §2.28(b), whenever Top Secret information is sent outside of a Treasury bureau or office within the Departmental Offices.

(b) *Top Secret Control Officer Listings.* In order for the Departmental Director of Security to maintain a current listing of Top Secret Control Officers within the Department, each Treasury bureau and the Departmental Offices shall annually report each October 15th in writing to the Departmental Office of Security, the identities of the office(s) and names of the officials designated as their primary and alternate Top Secret Control Officers. Any changes in these designations shall be reported to the Departmental Director of Security within thirty days.

(c) *Top Secret Document Record.* Upon receipt in the Department a green, color coded, TD F 71-01.7 (Top Secret Document Record) shall be attached by the Top Secret Control Officer to the first page or cover of the original and each copy of Top Secret information. The Top Secret Document Record shall remain attached to the Top Secret information until it is either transferred to another United States Government agency, downgraded, declassified or destroyed. The Top Secret Document Record, which shall initially be completed by the Top Secret Control Officer, shall identify the Top Secret information attached, and shall serve as a permanent record of the information. All persons, including stenographic and clerical personnel, having access to the information attached to the Top Secret Document Record must list their name and the date on the TD F 71-01.7 prior to accepting responsibility for its custody. The TD F 71-01.7 shall also indicate those individuals to whom only oral disclosure of the contents is made. Whenever any Top Secret information

is transferred to another United States Government agency, downgraded, declassified or destroyed, the Top Secret Control Officer shall record the action on the Top Secret Document Record and retain it for a minimum of three years after which time it may be destroyed. In order to maintain the integrity of the color coding process the photocopying and use of non-color coded Top Secret Document Record forms is prohibited.

(d) *Classified Document Record of Transmittal.* TD F 71-01.5 (Classified Document Record of Transmittal) shall be the exclusive classified document accountability record for use within the Department of the Treasury. No other logs or records shall be required except for the use of TD F 71-01.7 which is applicable to Top Secret information. TD F 71-01.5 shall be used for single or multiple document receipting and for internal and external routing. The inclusion of classified information on TD F 71-01.5 is to be avoided. In the event the subject title is classified, a recognizable short title shall be used, e.g., first letter of each word in the subject title. Several items may be transmitted to the same addressee with one TD F 71-01.5. TD F's 71-01.5 shall be maintained for a three year period after which the form may be destroyed. No record of the actual destruction of the TD F 71-01.5 is necessary.

(1) *Top Secret Information.* Top Secret information shall be subject to a continuous receipt system regardless of how brief the period of custody. TD F 71-01.5 shall be used for this purpose. Top Secret accountability records shall be maintained by Top Secret Control Officers separately from the accountability records of other classified information.

(2) *Secret Information.* Receipt on TD F 71-01.5 shall be required for transmission of Secret information between bureaus, offices and separate agencies. Responsible office heads shall determine administrative procedures required for the internal control within their respective offices. The volume of classified information handled and personnel resources available must be considered in determining the level of adequate security measures while at the

same time maintaining operational efficiency.

(3) *Confidential and Limited Official Use Information.* Receipts for Confidential and Limited Official Use information shall not be required unless the originator indicates that receipting is necessary.

[55 FR 1644, Jan. 17, 1990; 55 FR 13134, Apr. 9, 1990]

§ 2.27 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 information established under the provisions of § 2.25. Top Secret information stored outside the United States must be in a facility afforded diplomatic status. One or more of the following supplementary controls is required:

(i) The area that houses the security container or vault shall be subject to the continuous protection of U.S. guard or duty personnel;

(ii) U.S. Guard or duty personnel shall inspect the security container or vault at least once every two hours; or

(iii) The security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes.

Within the United States, the designated security officer in each Treasury bureau and the Department Offices shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Any vault used for the storage of sensitive compartmented information shall be configured to the specifications of the Director of Central Intelligence. Prior to an office or bureau operating such a vault, formal written certification for its use must first be obtained from the Special Assistant to the Secretary (Na-

tional Security) as the senior Treasury official of the Intelligence Community.

(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 § 2.25. 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, and may continue to be stored in a steel filing cabinet equipped with a steel lock-bar secured by a GSA-approved three-position, dial-type, changeable, combination padlock. The modification, however, of steel filing cabinets to barlock-type as storage equipment for classified information and material is prohibited and efforts are to be made to selectively phase out the use of such barlock cabinets for storage of Secret information. Exceptions may be authorized only by the Departmental Director of Security upon written request from the designated bureau security officer. The designated security officer in each Treasury bureau and the Departmental Offices shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, evidence vaults, closed areas or similar facilities shall be controlled in accordance with requirements approved by the Department. At a minimum, such requirements shall prescribe the use of GSA-approved, key-operated, high-security padlocks. For Secret and Confidential information stored outside the United States, it shall be stored in the manner authorized for Top Secret, in a GSA-approved safe file, or in a barlock cabinet equipped with a security-approved combination padlock if the cabinet is located in a security-approved vault and/or in a restricted area to which access is controlled by United States citizen personnel on a 24-hour basis.

(b) *Combinations*—(1) *Equipment in Service.* Combinations to dial-type, changeable, combination locks shall be

§ 2.27

changed only by persons having an appropriate security clearance, and shall be changed,

(i) Whenever such equipment is placed in use;

(ii) Whenever a person knowing the combination no longer requires access to it;

(iii) Whenever a combination has been subjected to possible compromise;

(iv) Whenever the equipment is taken out of service; or

(v) At least once each 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 combination lock. When securing a combination lock, the dial must be turned at least four (4) complete times in the same direction after closing. Defects in or malfunctioning of storage equipment protecting classified national security or officially limited information must be reported immediately to the designated office or bureau security official for appropriate action.

(2) *Equipment Out of Service.* When security equipment, used for the storage of classified national security or officially limited information, is taken out of service, it shall be physically inspected to ensure that no classified information or officially limited information remains therein. Built-in, three-position, dial-type, changeable, combination locks shall be reset to the standard combination 50-25-50 and combination padlocks shall be reset to the standard combination 10-20-30. The designated security officer in each Treasury bureau and the Departmental Offices shall prescribe such supplementary controls deemed necessary to fulfill their individual needs to be consistent with § 2.27.

(3) *Security Container Check Sheet.* Each piece of security equipment used for the storage of classified information will have attached conspicuously to the outside a Standard Form 702 (Security Container Check Sheet) on which an authorized person will record the date and actual time each business day that they initially unlock and finally lock the security equipment, fol-

31 CFR Subtitle A (7-1-06 Edition)

lowed by their initials. Users of this form are to avoid citations which reflect the opening, locking and checking of the security equipment at standardized (non-actual) times, e.g., opened at 8:00 a.m. and closed/checked at 4:00 p.m. Bureaus and the Departmental Offices may continue to use Optional Form 62 (Safe or Cabinet Security Record) in lieu of the SF 702 until September 30, 1990, or such time as their supplies of Optional Form 62 are exhausted. The reprinting or photostatic reproduction and use of Optional Form 62 is *not* authorized. On each normal workday, regardless of whether the security equipment was opened on that particular day, the security equipment shall be checked by authorized personnel to assure that no surreptitious attempt has been made to penetrate the security equipment. Such examinations normally consist of a quick or casual visual check to note either any obvious marks or gashes, or defects or malfunction of the security equipment which are different from their prior observations or experience in operating the equipment concerned. Any such discrepancies in the appearance of or functioning of the security equipment, based upon this visual check, should be reported to appropriate security officials. The "Checked By" column of the SF 702 or Optional Form 62 shall be annotated to reflect the date and time of this action followed by that person's initials. Security equipment used for the storage of classified information that has been opened on a particular day shall not be left unattended at the end of that day until it has been locked by an authorized person and checked by a second person. In the event a second person is not available within the office, the individual who locked the equipment shall also annotate the "Checked By" column of the SF 702 or Optional Form 62. Reversible "OPEN-CLOSED" or "LOCKED-UNLOCKED" signs, available through normal supply channels, shall also be used on such security equipment. The respective side of the sign shall be displayed to indicate when the container is open or closed. Except for the SF 702 or Optional Form 62, the top surface area of security equipment is *not* to be used for

storage and must be kept free of extraneous material. SF 702 and/or Optional Form 62 shall be utilized on all security equipment used for storing information bearing the control legend "Limited Official Use". The designated security officer in each Treasury bureau and the Department Offices may, as warranted, prescribe supplementary use of the SF 702 or Optional Form 62 to apply to other authorized legends approved by the Department for officially limited information.

(4) *Safe Combination Records.* Combinations to security equipment containing classified information shall be recorded on Standard Form 700 (Security Container Information), national stock number 7540-01-214-5372. Bureaus and the Departmental Offices may continue to use Treasury Form 4032 (Security Container Information) in lieu of the SF 700 until September 30, 1990, or such time as their supplies of Treasury Form 4032 are exhausted. The reprinting of Treasury Form 4032 is not authorized. Each part of the SF 700 shall be completed in its entirety. The names, addresses and home telephone numbers of personnel responsible for the combination, and the classified information stored therein, must be indicated on part 1 of the SF 700. The completed part 1 shall be posted in the front interior of the top, control or locking drawer of the security equipment concerned. Part 2 shall be inserted in the envelop (part 2A) provided, and forwarded via appropriate secure means to the designated bureau or Departmental Offices central repository for security combinations. Part 2 shall have the highest level of classified information, stored in the security equipment concerned, annotated in both the top and bottom border areas of the completed SF 700. Part 2A shall have the highest level of classified information, stored in the security equipment concerned, annotated in the blank space immediately above the word, "WARNING" which appears on the SF 700. The completion of the SF 700 or Treasury Form 4032 does not constitute a classification action but serves as an administrative requirement to ensure the protection of classified information stored in such security equipment. SF 700 shall be utilized

on all security equipment used for storing information bearing the control legend "Limited Official Use". The designated security officer in each Treasury bureau and the Departmental Offices may prescribe supplementary use of the SF 700 to apply to other authorized legends approved by the Department for officially limited information, as warranted.

(c) *Keys.* The designated security officer in each Treasury bureau and the Departmental Offices 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 information being protected by the padlock.

(d) *Classified Document Cover Sheets.* Classified document cover sheets alert personnel that documents or folders are classified and require protection from unauthorized scrutiny. Individuals who prepare or package classified documents are responsible for affixing the appropriate document cover sheet. Orange Standard Form 703 (Top Secret Cover Sheet), red SF 704 (Secret Cover Sheet) and blue SF 706 (Confidential Cover Sheet) are the only authorized cover sheets for collateral classified information. The national stock numbers of these cover sheets are as follows: SF 703, 7540-01-213-7901; SF 704, 7540-01-213-7902; and SF 705, 7540-01-213-7903. In order to maintain the integrity of the color coding process the photocopying and use of non-color coded classified document cover sheets is prohibited. Bureaus and offices shall maintain a supply of classified document cover sheets appropriate for their needs. Classified document cover sheets are designed to be reused and will be removed before classified information is filed to conserve filing space and prior to the destruction of classified information. Document cover sheets are to be used to shield classified documents while in use and particularly when the transmission is made internally within a headquarters by courier, messenger or by personal contact. File folders containing classified information should be otherwise marked, e.g., at the top and bottom of the front and

§ 2.28

back covers, to indicate the overall classification of the contents rather than permanently affixing the respective classified document cover sheet. Treasury Directive 71-02 provides for the use of a green cover sheet, TD F 71-01.6 (Limited Official Use Document Cover Sheet) for information bearing the control legend "Limited Official Use". Bureaus or offices electing to create and use other cover sheets for officially limited information must obtain prior written approval from the Departmental Director of Security.

(e) *Activity Security Checklist*. Standard Form 701 (Activity Security Checklist) provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability in the event that irregularities are discovered. Bureaus and the Departmental Offices may include additional information on the SF 701 to suit their unique needs. The SF 701, available through normal supply channels has a national stock number of 7540-01-213-7900. It shall be the only form used in situations that call for use of an activity security checklist. Completion, storage and disposition of SF 701 will be determined by each bureau and the Departmental Offices.

§ 2.28 Transmittal [4.1(b)].

(a) *Preparation*. Classified information to be transmitted outside of a Treasury 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 security 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. Whenever classified material is to be transmitted and the size of the material is not suitable for use of envelopes or similar wrappings, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings. Material used for packaging such bulk classified information shall be of sufficient strength and durability as to provide security protection while in transit, to prevent items from breaking out of the container, and to facilitate detection of any tampering therewith.

31 CFR Subtitle A (7-1-06 Edition)

(b) *Receipting*. A receipt, Treasury Department Form 71-01.5 (Classified Document Record of Transmittal), shall be enclosed in the inner cover, except that Confidential and Limited Official Use information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee and describe the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Within a Treasury facility, such information may be transmitted between offices by direct contact of the officials concerned in a single sealed opaque envelope with no security classification category being shown on the outside of the envelope. Classified information shall never be delivered to unoccupied offices or rooms. Senders of classified information should maintain appropriate records of outstanding receipts for which return of the original signed copy is still pending. TD F's 71-01.5 shall be maintained for a three year period after which they may be destroyed. No record of the actual destruction of the TD F 71-01.5 is required.

(c) *Transmittal of Top Secret*. The transmittal of Top Secret information outside of a Treasury facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for that purpose, e.g., Defense Courier Service, or over authorized secure communications circuits. Top Secret information may *not* be sent via registered mail.

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

(1) *The 50 States, 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 United States Postal Service registered mail or express mail service; or by protective services provided by United States air or surface commercial carriers under such conditions as may be prescribed by the Departmental Director of Security. United States Postal Service express mail service

shall be used only when it is the most effective means to accomplish a mission within security, time, cost and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the United States Postal Service Express Mail Label 11-B may not be executed under any circumstances. All Secret express mail shipments are to be processed through mail distribution centers or delivered directly to a United States Postal Service facility or representative. The use of external (street side) express mail collection boxes is prohibited. Only the express mail services of the United States Postal Service are authorized.

(2) *Other Areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2.28(d)(1) by one of the means established for Top Secret information, or by United States registered mail through Military Postal Service facilities provided that the information does not at any time pass out of United States 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 United States Government owned and United States Government contract vehicles or aircraft, ships of the United States Navy, civil service manned United States Naval ships, and ships of United States Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are United States citizens, and who are appropriately cleared, may be designated as escorts. Secret information may not be sent via certified mail.

(e) *Transmittal of Confidential and Limited Official Use Information.* Confidential and Limited Official Use information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and United States territories or possessions by one of the means established for higher classifications, or by the United States Postal Service registered mail. Outside these areas, confidential and Limited Official Use information shall be transmitted only as is authorized for higher classi-

fications. Confidential and Limited Official Use information may not be sent via certified mail.

(f) *Hand Carrying of Classified Information in Travel Status—(1) General Provisions.* Personnel in travel status shall physically transport classified information across international boundaries only when absolutely essential. Whenever possible, and when time permits, the most desirable way to transmit classified information to the location being visited is by other authorized means identified in § 2.28 (c), (d) and (e). The physical transportation of classified information on non-United States flag aircraft should be avoided if possible. Treasury Directive 71-03, "Screening of Airline Passengers Carrying Classified Information or Material" provides specifics on the requirements for transporting classified information.

(2) *Specific Safeguards.* If it is determined that the transportation of classified information by an individual in travel status is in the best interest of the United States Government, the following specific safeguards shall be fulfilled:

(i) Classified information shall be in the physical possession of the individual and shall have adequate safeguards at all times if proper storage at a United States Government facility is not available. Under no circumstances shall classified information be stored in a hotel safe or room, locked in automobiles, private residences, train compartments, or any vehicular detachable storage compartments.

(ii) An inventory of all Top Secret classified information, including teletype messages, shall be made prior to departure and a copy of same shall be retained by the traveller's office until the traveller's return at which time all Top Secret classified information shall be accounted for. These same procedures are recommended for information classified Secret, Confidential or Limited Official Use.

(iii) Classified information shall never be displayed or used in any manner in public conveyances or rooms. First class or business travel is not authorized when the justification for commercially available transportation

§ 2.29

is based on the need for reviewing classified materials while enroute. Travelers are responsible for reviewing and familiarizing themselves with required classified materials, under appropriately secure circumstances, in advance of their travel and not during such travel.

(iv) In order to avoid unnecessary delays in the screening process prior to boarding commercial air carriers, the traveler shall have in his or her possession written authorization, on Treasury or bureau letterhead, to transport classified information and either an identification card or credential bearing both a photograph and descriptive data. Courier authorizations shall be signed by an appropriate security representative authorized to direct official travel. This courier authorization, along with official travel orders, shall, in most instances, permit the individual to exempt the classified information from inspection. If difficulty is encountered, the traveler should tactfully refuse to exhibit or disclose the classified information to inspection and should insist on the assistance of the local United States diplomatic representative at the port of entry or departure.

(v) Upon completion of the visit, the traveler shall have the information returned to his or her office by approved means. All Top Secret and Secret classified information, including teletype messages transported for the purpose of the visit shall be accounted for. It is highly recommended that Confidential and Limited Official Use information also be accounted for. If any Top Secret or Secret classified items are left with the office being visited for its retention and use, the individual shall obtain a receipt.

[55 FR 1644, Jan. 17, 1990, as amended at 55 FR 50321, Dec. 6, 1990]

§ 2.29 Telecommunications and computer transmissions.

Classified information shall not be communicated by telecommunications or computer transmissions except as may be authorized with respect to the transmission of classified information over authorized secure communications circuits or systems.

31 CFR Subtitle A (7-1-06 Edition)

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

Only the Secretary of the Treasury 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.

§ 2.31 Reproduction controls [4.1(b)].

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

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

(c) Reproductions 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 possible declassification.

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

(a) *Report of Loss or Possible Compromise.* Any Treasury employee who has knowledge of the loss or possible compromise or classified information shall immediately report the circumstances to their designated office or bureau security officer who shall take appropriate action to assess the degree of damage. In turn, the Departmental Director of Security shall be immediately notified by the affected office or bureau security officer of such reported loss or possible compromise. The Departmental Director of Security shall also notify the department or agency which originated the information and any other interested department or agency so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the loss or possible compromise. Compromises

may occur through espionage, unauthorized disclosures to the press or other members of the public, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Inquiry.* The Departmental Director of Security shall notify the Assistant Secretary (Management) who shall then direct an immediate inquiry to be conducted for the purpose of taking corrective measures and assessing damages. Based on the results of this inquiry, it may be deemed appropriate to notify the Inspector General who shall determine whether the Office of the Inspector General or a Treasury bureau will conduct any additional investigation. Upon completion of the investigation by the Inspector General, the Inspector General shall recommend to the Assistant Secretary (Management) and concurrently to the Departmental Director of Security, the appropriate administrative, disciplinary, or legal action to be taken based upon jurisdictional authority of the Treasury components involved.

(c) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date and circumstances of the compromise.

(2) Classification and description of the specific information which has been lost.

(3) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(4) An assessment of the possible advantage to foreign powers resulting from the compromise.

(5) An assessment of whether,

(i) The classification of the information involved should be continued without change;

(ii) The specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained;

(iii) Downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change, and

(6) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(d) *System for Control of Damage Assessments.* Each Treasury bureau and the Departmental Offices shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in § 2.32(a) and that records are maintained in a manner that facilitates their retrieval and use within the Department.

(e) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, the Departmental Director of Security shall advise the other affected agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment and Treasury components will provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(2) Whenever a compromise of United States classified information is the result of actions taken by foreign nationals, by foreign government officials, or by United States nationals in the employ of international organizations, the agency performing the damage assessment shall endeavor to ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(3) Whenever an action is contemplated against any person believed responsible for the loss or compromise of classified information, damage assessments shall be coordinated with appropriate legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, coordination shall be made with the Department of Justice.

§ 2.33

(4) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of sensitive compartmented information has occurred.

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

Any person having access to and possession of classified information is responsible for protecting it from persons not authorized access, i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know. This includes keeping classified documents under constant observation and turned face-down or covered when not in use and securing such information in approved security equipment or facilities whenever it is not under the direct supervision of authorized persons. In all instances, such protective means must meet accountability requirements prescribed by the Department.

§ 2.34 Inspections [4.1(b)].

Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. Security officers shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by this regulation and any bureau implementing regulation are in effect at all times. At a minimum such checks shall ensure that all classified information is stored in approved security containers, including removable storage media, e.g., floppy disks used by word processors that contain classified information; burn bags, if utilized, are either stored in approved security containers or destroyed; and classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 2.35 Security violations.

Any individual, at any level of employment, determined to have been responsible for the unauthorized release or disclosure or potential release or

31 CFR Subtitle A (7-1-06 Edition)

disclosure of classified national security information, whether it be knowingly, willfully or through negligence, shall be notified on TD F 71-21.1 (Record of Security Violation) that his or her action is in violation of this regulation, the Order, the Directive, and Executive Order 10450, as amended. Treasury Directive 71-04, entitled, "Administration of Security Violations" sets forth provisions concerning security violations which shall apply to each Treasury employee and persons under contract or subcontract to the Department authorized access to Treasury classified national security information.

(a) Repeated abuse of the classification process, either by unnecessary or over-classification, or repeated failure, neglect or disregard of established requirements for safeguarding classified information by any employee shall be grounds for appropriate adverse or disciplinary action. Such actions may include, but are not necessarily limited to, a letter of warning, a letter of reprimand, suspension without pay, or dismissal, as appropriate in the particular case, under applicable personnel rules, regulations and procedures. Where a violation of criminal statutes may be involved, any such case shall be promptly referred to the Department of Justice.

(b) After an affirmative adjudication of a security violation, and as the occasion demands, reports of accountable security violations shall be placed in the employee's personnel security file, and as appropriate, in the employee's official personnel folder. The security official of the office or bureau concerned shall recommend to the respective management official or bureau head that disciplinary action be taken when such action is indicated.

§ 2.36 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 Title 44, United States Code, Chapters 21 and 33, which govern disposition of Federal

records. Classified information approved for destruction shall be destroyed by either burning, melting, chemical decomposition, pulping, mulching, pulverizing, cross-cut shredding or other mutilation in the presence of appropriately cleared and authorized persons. The method of destruction *must* preclude recognition or reconstruction of the classified information. The residue from cross-cut shredding of Top Secret, Secret, and Confidential classified, non-Communications Security (COMSEC), information contained in paper media may not exceed $\frac{3}{32}$ " by $\frac{1}{2}$ " with a $\frac{1}{64}$ " tolerance.

(a) *Diskettes or Floppy Disks.* Diskettes or floppy disks containing information or data classified up to and including Top Secret may be destroyed by the use of an approved degausser, burning, pulverizing, and chemical decomposition, or by first reformatting or reinitializing the diskette then physically removing the magnetic disk from its protective sleeve and using an approved cross-cut shredder to destroy the magnetic media. Care must be exercised to ensure that the destruction of magnetic disks does not damage the cross-cut shredder. The residue from such destruction, however, may not exceed $\frac{1}{32}$ " by $\frac{1}{2}$ " with a $\frac{1}{64}$ " tolerance. The destruction of classified COMSEC information on diskettes or floppy disks may only be effected by burning followed by crushing of the ash residue.

(b) *Hard Disks.* Hard disks, including removable hard disks, disk packs, drums or single disk platters that contain classified information must first be degaussed prior to physical destruction. The media must be destroyed by incineration, chemical decomposition or the entire magnetic disk pack, drum, or platter recording surface must be obliterated by use of an emery wheel or disk sander.

(c) *Approval of Use of Mulching and Cross-cut Shredding Equipment.* Prior to obtaining mulching or cross-cut shredding equipment, the Departmental Director of Security shall approve the use of such equipment.

(d) *Use of Burnbags.* Any classified information to be destroyed by burning shall be torn and placed in opaque containers, commonly designated as burnbags, which shall be clearly and

distinctly labeled "BURN" or "CLASSIFIED WASTE". Burnbags awaiting destruction are to be protected by security safeguards commensurate with the classification or control designation of the information involved.

(e) *Records of Destruction.* Appropriate accountability records shall be maintained on TD F 71-01.17 (Classified Document Certificate of Destruction) to reflect the destruction of all Top Secret and Secret information. As deemed necessary by the originator, or as required by special regulations, the TD F 71-01.17 shall be executed for the destruction of information classified Confidential or marked Limited Official Use. TD F's 71-01.17 shall be maintained for a three-year period after which the form may be destroyed. No record of the actual destruction of the TD F 71-01.17 is required.

(f) *Destruction of non-record Classified Information.* Non-record classified information such as extra copies and duplicates, including shorthand notes, preliminary drafts, used carbon paper and other material of similar temporary nature, shall also be destroyed by burning, mulching, or cross-cut shredding as soon as it has served its purpose, but no records of such destruction need be maintained.

[55 FR 1644, Jan. 17, 1990; 55 FR 5118, Feb. 13, 1990]

§ 2.37 National Security Decision Directive 197.

National Security Decision Directive 197, Reporting Hostile Contacts and Security Awareness, provides that United States Government employees are responsible for reporting to their designated security officer:

(a) Any suspected or apparent attempt by persons, regardless of nationality, to obtain unauthorized access to classified national security information, sensitive or proprietary information or technology and/or;

(b) Instances in which they feel they are being targeted for possible exploitation. Contacts with representatives of designated countries of concern identified in § 2.43(f) which involve requests for information which are not ordinarily provided in the course of an employee's job, regular or daily activity, and/or which might possibly lead

§ 2.38

to further requests for access to sensitive, proprietary or classified information or technology, are to be reported to designated security officers. Reports of such contacts are to be forwarded by the designated security officer to the Departmental Director of Security for appropriate action and coordination.

Subpart E—Implementation and Review

§ 2.38 Departmental management.

(a) The Assistant Secretary (Management) shall:

(1) Enforce the Order, the Directive and this regulation, and establish, coordinate and maintain active training, orientation and inspection programs for employees concerned with classified information.

(2) Review suggestions and complaints regarding the administration of this regulation.

(b) Pursuant to Treasury Directive 71-08, "Delegation of Authority Concerning Physical Security Programs", the Departmental Director of Security shall:

(1) Review all bureau implementing regulations prior to publication and shall require any regulation to be changed, if it is not consistent with the Order, the Directive or this regulation.

(2) Have the authority to conduct on-site reviews of bureau physical security programs and information security programs as they pertain to each Treasury bureau and to require such reports, information and assistance as may be necessary, and

(3) Serve as the principal advisor to the Assistant Secretary (Management) with respect to Treasury physical and information security programs.

§ 2.39 Bureau administration.

Each Treasury bureau and the Departmental Offices shall designate, in writing to the Departmental Director of Security, an officer or official to direct, coordinate and administer its physical security and information security programs which shall include active oversight to ensure effective implementation of the Order, the Directive, this regulation. Bureaus and the Departmental Offices shall revise their

31 CFR Subtitle A (7-1-06 Edition)

existing implementing regulation on national security information to ensure conformance with this regulation. Time frames for bureau and Departmental Offices implementation shall be established by the Departmental Director of Security.

§ 2.40 Emergency planning [4.1(b)].

Each Treasury bureau and the Departmental Offices shall develop plans for the protection, removal, or destruction of classified information in case of fire, natural disaster, civil disturbance, or possible enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2.41 Emergency authority [4.1(b)].

The Secretary of the Treasury 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.

§ 2.42 Security education [5.3(a)].

Each Treasury bureau that creates, processes or handles national security information, including the Departmental Offices, is required to establish a security education program. The program shall be sufficient to familiarize all necessary personnel with the provisions of the Order, the Directive, this regulation and any other implementing directives and regulations to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

(a) *Briefing of Employees.* All new employees concerned with classified information shall be afforded a security briefing regarding the Order, the Directive and this regulation and sign a security agreement as required in § 2.22(c). Employees concerned with sensitive compartmented information shall be required to read and also sign a security agreement. Copies of applicable laws and pertinent security regulations setting forth the procedures for the protection and disclosure of classified information shall be available for all new employees afforded a security

briefing. All employees given a security briefing shall be required to sign a TD F 71-01.16 (Physical Security Orientation Acknowledgment) which shall be maintained on file as determined by respective office or bureau security officials.

(b) [Reserved]

Subpart F—General Provisions

§ 2.43 Definitions [6.1].

(a) *Authorized Person.* Those individuals who have a “need-to-know” the classified information involved and have been cleared for the receipt of such information. Responsibility for determining whether individuals’ duties require that they possess, or have access to, any classified information and whether they are authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipients.

(b) *Compromise.* The loss of security enabling unauthorized access to classified information. Affected information or material is not automatically declassified.

(c) *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.

(d) *Declassification.* The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or occur automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the information or material shall be so marked with the new designation.

(e) *Derivative Classification.* A determination that information is, in substance, the same as information that is currently classified and a designation of the level of classification.

(f) *Designated Countries of Concern.* For purposes of National Security Decision Directive 197 reporting: Afghani-

stan, Albania, Angola, Bulgaria, Cambodia (Kampuchea), the People’s Republic of China (Communist China), Cuba, Czechoslovakia, Ethiopia, East Germany (German Democratic Republic including the Soviet sector of Berlin), Hungary, Iran, Iraq, Laos, Libya, Mongolian People’s Republic (Outer Mongolia), Nicaragua, North Korea, Palestine Liberation Organization, Poland, Romania, South Africa, South Yemen, Syria, Taiwan, Union of Soviet Socialist Republics (Russia), Vietnam and Yugoslavia.

(g) *Document.* Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps, charts; painting; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

(h) *Foreign Government Information.* (1) Information provided by a foreign government or governments, an international organization of governments, or any elements 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 Government 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.

(i) *Information.* Any data or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(j) *Information Security.* The administrative policies and procedures for identifying, controlling, and safeguarding from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

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

§2.43

(l) *Intelligence Sources and Methods.* A person, organization, or technical means or method which provides foreign intelligence or foreign counterintelligence to the United States and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An intelligence source also means a person or organization which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed. Intelligence methods are that which, if disclosed, reasonably could lead to the disclosure of an intelligence source or operation.

(m) *Limited Official Use.* The legend authorized for "Officially Limited Information" which provides that it be handled, safeguarded and stored in a manner equivalent to national security information classified Confidential.

(n) *Multiple Classified Sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from other than one source.

(o) *National Security.* The national defense or foreign relations of the United States.

(p) *National Security Information.* Information that has been determined pursuant to the Order or any predecessor Executive Order to require protection against unauthorized disclosure and that is so designated.

(q) *Need-to-Know.* A determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of particular work, including performance on contracts for which such access is required.

(r) *Officially Limited Information.* Information which does not meet the criterion that unauthorized disclosure would at least cause damage to the national security under the Order or a predecessor Executive Order, but which concerns important, delicate, sensitive

31 CFR Subtitle A (7-1-06 Edition)

or proprietary information which is utilized in the development of Treasury policy. This includes the enforcement of criminal and civil laws relating to Treasury operations, the making of decisions on personnel matters and the consideration of financial information provided in confidence.

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

(t) *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.

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

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

(w) *Sensitive Compartmented Information.* Information and material concerning or derived from intelligence sources, methods, or analytical processes, that requires special controls for restricting handling within compartmented intelligence systems established by the Director of Central Intelligence and for which compartmentation is established.

(x) *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".

(y) *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.

(z) *Unauthorized Disclosure.* A communication or physical transfer of classified information to an unauthorized recipient. It includes the unauthorized disclosure of classified information in a newspaper, journal, or other publication where such information is traceable due to a direct quotation or other uniquely identifiable fact.

PART 3—CLAIMS REGULATIONS AND INDEMNIFICATION OF DEPARTMENT OF TREASURY EMPLOYEES

Subpart A—Claims Under the Federal Tort Claims Act

Sec.

- 3.1 Scope of regulations.
- 3.2 Filing of claims.
- 3.3 Legal review.
- 3.4 Approval of claims not in excess of \$25,000.
- 3.5 Limitations on authority to approve claims.
- 3.6 Final denial of a claim.
- 3.7 Action on approved claims.
- 3.8 Statute of limitations.

Subpart B—Claims Under the Small Claims Act

- 3.20 General.
- 3.21 Action by claimant.
- 3.22 Legal review.
- 3.23 Approval of claims.
- 3.24 Statute of limitations.

Subpart C—Indemnification of Department of Treasury Employees

- 3.30 Policy.

AUTHORITY: 28 U.S.C. 2672; 28 CFR part 14; 5 U.S.C. 301.

SOURCE: 35 FR 6429, Apr. 22, 1970, unless otherwise noted.

Subpart A—Claims Under the Federal Tort Claims Act

§ 3.1 Scope of regulations.

(a) The regulations in this part shall apply to claims asserted under the Fed-

eral Tort Claims Act, as amended, 28 U.S.C. 2672, accruing on or after January 18, 1967, for money damages against the United States for injury to or loss of property or personal injury or death caused by the negligent or wrongful act or omission of an employee of the Department while acting within the scope of his office or employment, under circumstances where the United States if a private person, would be liable to the claimant for such damage, loss, injury, or death, in accordance with the law of the place where the act or omission occurred. The regulations in this subpart do not apply to any tort claims excluded from the Federal Tort Claims Act, as amended, under 28 U.S.C. 2680.

(b) Unless specifically modified by the regulations in this part, procedures and requirements for filing and handling claims under the Federal Tort Claims Act shall be in accordance with the regulations issued by the Department of Justice, at 28 CFR part 14, as amended.

§ 3.2 Filing of claims.

(a) *When presented.* A claim shall be deemed to have been presented upon the receipt from a claimant, his duly authorized agent or legal representative of an executed Standard Form 95 or other written notification of an incident, accompanied by a claim for money damages in a sum certain for injury to or loss of property, or personal injury, or death alleged to have occurred by reason of the incident.

(b) *Place of filing claim.* Claims shall be submitted directly or through the local field headquarters to the head of the bureau or office of the Department out of whose activities the incident occurred, if known; or if not known, to the General Counsel, Treasury Department, Washington, DC 20220.

(c) *Contents of claim.* The evidence and information to be submitted with the claim shall conform to the requirements of 28 CFR 14.4.

§ 3.3 Legal review.

Any claim that exceeds \$500, involves personal injuries or automobile damage, or arises out of an incident that is likely to result in multiple claimants, shall be forwarded to the legal division