AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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),

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

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 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 Declassification 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 indentity shall be shown at the bottom of the first and last pages as

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 in 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 practicable 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:

''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 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