

Pt. 2

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.

[60 FR 31633, June 16, 1995. Redesignated at 65 FR 2334, Jan. 14, 2000]

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.
- 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)].

31 CFR Subtitle A (7–1–01 Edition)

- 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

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

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), 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.