

(b) Report violations of the provisions of this regulation to the Chief Security Officer committed by employees of their component, as required;

(c) Ensure that employees of their component acquire adequate security education and training, as required by the DHS classified information security procedures;

(d) Continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or reduce the level of access authorized, as appropriate; and

(e) Cooperate fully with any request from the Chief Security Officer for assistance in the implementation of this part.

§ 7.12 Violations of classified information requirements.

(a) Any person who suspects or has knowledge of a violation of this part, including the known or suspected loss or compromise of classified information, shall promptly report such violations or possible violations, pursuant to requirements set forth in DHS directives.

(b) DHS employees and detailees may be reprimanded, suspended without pay, terminated from classification authority, suspended from or denied access to classified information, or subject to other sanctions in accordance with applicable law and DHS regulations or directives if they:

(1) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under Executive Order 12958, as amended, or its predecessor orders;

(2) Knowingly, willfully, or negligently classify or continue the classification of information in violation of Executive Order 12958, as amended, or its implementing directives; or

(3) Knowingly, willfully, or negligently violate any other provision of Executive Order 12958, as amended, or DHS implementing directives; or

(4) Knowingly, willfully, or negligently grant eligibility for, or allow access to, classified information in violation of Executive Order 12958, or its implementing directives, this part, or

DHS implementing directives promulgated by the Chief Security Officer.

§ 7.13 Judicial proceedings.

(a) Any DHS official or organization receiving an order or subpoena from a Federal or State court, or an administrative subpoena from a Federal agency, to produce classified information (see 6 CFR 5.41 through 5.49), required to submit classified information for official DHS litigative purposes, or receiving classified information from another organization for production of such in litigation, shall notify the Office of the General Counsel, unless the demand for production is made by the Office of the General Counsel, and immediately determine from the agency originating the classified information whether the information can be declassified. If declassification is not possible, DHS representatives will take appropriate action to protect such information, pursuant to the provisions of this section.

(b) If a determination is made to produce classified information in a judicial proceeding in any manner, the DHS General Counsel attorney, in conjunction with the Department of Justice, shall take appropriate steps to protect classified information in judicial proceedings and retrieve the information when the information is no longer required in such judicial proceedings, in accordance with the Department of Justice procedures, and in Federal criminal cases, pursuant to the requirements of Classified Information Procedures Act (CIPA), Public Law 96-456, 94 Stat. 2025, (18 U.S.C. App.), and the "Security Procedures Established Pursuant to Public Law 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information," and other applicable authorities.

Subpart B—Classified Information

§ 7.20 Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Secretary of Homeland Security and by officials to whom such authority is delegated in writing by the Secretary. The Chief Security Officer, as the Senior

§7.21

6 CFR Ch. I (1-1-06 Edition)

Agency Official, is delegated authority to originally classify information up to and including Top Secret. No official who is delegated Top Secret original classification authority by the Secretary may further delegate such authority.

(b) The Chief Security Officer may delegate Secret and Confidential original classification authority to other officials determined to have frequent need to exercise such authority. No official who is delegated original classification authority by the Secretary or the Chief Security Officer may further delegate such authority.

(c) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level. In the absence of an official authorized to exercise classification authority, the person designated to act in lieu of such official may exercise the official's classification authority.

§7.21 Classification of information, limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) An original classification authority is classifying the information;

(2) The information is owned by, produced by or for, or is under the control of the United States Government;

(3) The information falls within one or more of the categories of information specified in section 1.4 of Executive Order 12958, as amended; and

(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and such official is able to identify or describe the damage.

(b) Information shall be classified as Top Secret, Secret, or Confidential in accordance with and in compliance with the standards and criteria in Executive Order 12958, as amended. No other terms shall be used to identify United States classified information except as otherwise provided by statute.

(c) Information shall not be classified in order to:

(1) Conceal inefficiency, violations of law, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition;

(4) Prevent or delay release of information that does not require protection in the interest of national security.

(d) Information may be reclassified after it has been declassified and released to the public under proper authority only in accordance with the following conditions:

(1) The reclassification action is taken under the personal authority and with the written approval of the Secretary or Deputy Secretary of Homeland Security, based on the determination that the reclassification of the information is necessary in the interest of the national security;

(2) The reclassification of the information meets the standards and criteria for classification pursuant to Executive Order 12958, as amended;

(3) The information may be reasonably recovered; and

(4) The reclassification action is reported promptly to the Director of ISOO.

(e) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after DHS has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 12958, as amended, section 3.5. When it is necessary to classify or reclassify such information, it shall be forwarded to the Chief Security Officer and classified or reclassified only at the direction of the Secretary or Deputy Secretary of Homeland Security.

§7.22 Classification pending review.

(a) Whenever persons who do not have original classification authority originate or develop information that they believe requires immediate classification and safeguarding, and no authorized classifier is available, that person shall:

(1) Safeguard the information in a manner appropriate for the classification level they believe it to be;