

## Office of the Secretary, Homeland Security

## § 7.10

- 7.23 Emergency release of classified information.
- 7.24 Duration of classification.
- 7.25 Identification and markings.
- 7.26 Derivative classification.
- 7.27 Declassification and downgrading.
- 7.28 Automatic declassification.
- 7.29 Documents of permanent historical value.
- 7.30 Classification challenges.
- 7.31 Mandatory review for declassification requests.

AUTHORITY: 5 U.S.C. 301; Pub. L. 107-296, 116 Stat. 2135 (6 U.S.C. 101); E.O. 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333; E.O. 13142, 64 FR 66089, 3 CFR, 1999 Comp., p. 236; 32 CFR part 2001.

SOURCE: 70 FR 61213, Oct. 21, 2005, unless otherwise noted.

### § 7.1 Purpose.

The purpose of this part is to ensure that information within the Department of Homeland Security (DHS) relating to the national security is classified, safeguarded, and declassified pursuant to the provisions of Executive Order 12958, as amended, and implementing directives from the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA).

### § 7.2 Scope.

(a) This part applies to all employees, detailees and non-contractor personnel outside the Executive Branch who are granted access to classified information by the DHS, in accordance with the standards in Executive Order 12958, as amended, and its implementing directives.

(b) This part does not apply to contractors, grantees and other categories of personnel falling under the purview of Executive Order 12829, National Industrial Security Program, and its implementing directives.

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or em-

ployees, or any other person. This part creates limited rights to administrative review of decisions. This part does not, and is not intended to, create any right to judicial review of administrative action.

### § 7.3 Definitions.

The terms defined or used in Executive Order 12958, as amended, and the implementing directives in 32 CFR parts 2001 and 2004, are applicable to this part.

## Subpart A—Administration

### § 7.10 Authority of the Chief Security Officer, Office of Security.

(a) The DHS Chief Security Officer (hereafter “Chief Security Officer”) is designated as the Senior Agency Official as required by section 5.4(d) of Executive Order 12958, as amended, and, except as specifically provided elsewhere in this part, is authorized to administer the DHS Classified National Security Information program pursuant to Executive Order 12958, as amended.

(b) The Chief Security Officer shall, among other actions:

(1) Oversee and administer the DHS’s program established under Executive Order 12958, as amended;

(2) Promulgate implementing regulations;

(3) Establish and maintain Department-wide security education and training programs;

(4) Establish and maintain an ongoing self-inspection program including the periodic review and assessment of the DHS’s classified product;

(5) Establish procedures to prevent unnecessary access to classified information, including procedures that:

(i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

(ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(6) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

## §7.11

(7) Coordinate with the DHS Chief Human Capital Officer, as appropriate to ensure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(i) Original classification authorities;  
(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information;

(8) Account for the costs associated with implementing this part and report the cost to the Director of ISOO;

(9) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 12958, as amended, that pertains to classified information that originated in a DHS component that no longer exists and for which there is no clear successor in function;

(10) Report violations, take corrective measures and assess appropriate sanctions as warranted, in accordance with Executive Order 12958, as amended;

(11) Overseeing DHS participation in special access programs authorized under Executive Order 12958, as amended;

(12) Direct and administer DHS's personnel security program in accordance with Executive Order 12968 and other applicable law;

(13) Direct and administer DHS implementation and compliance with the National Industrial Security Program in accordance with Executive Order 12829 and other applicable guidance; and

(14) Perform any other duties as the Secretary may designate.

(c) The Chief Security Officer shall maintain a current list of all officials authorized pursuant to this part to originally classify or declassify documents.

### §7.11 Components' responsibilities.

Each DHS component shall appoint a security officer or security liaison to implement this part. The security officer/security liaison shall:

## 6 CFR Ch. I (1-1-14 Edition)

(a) Implement, observe, and enforce security regulations or procedures within their component with respect to the classification, declassification, safeguarding, handling, and storage of classified national security information;

(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