

PART 9—SECURITY INFORMATION REGULATIONS

Sec.

- 9.1 Basis.
- 9.2 Objective.
- 9.3 Senior agency official.
- 9.4 Original classification.
- 9.5 Original classification authority.
- 9.6 Derivative classification.
- 9.7 Identification and marking.
- 9.8 Classification challenges.
- 9.9 Declassification and downgrading.
- 9.10 Mandatory declassification review.
- 9.11 Systematic declassification review.
- 9.12 Access to classified information by historical researchers and certain former government personnel.
- 9.13 Safeguarding.

AUTHORITY: E.O. 12958 (60 FR 19825, April 20, 1995) as amended; Information Security Oversight Office Directive No. 1, 32 CFR 2001 (68 FR 55168, Sept. 22, 2003).

SOURCE: 72 FR 30972, June 5, 2007, unless otherwise noted.

§ 9.1 Basis.

These regulations, taken together with the Information Security Oversight Office Directive No. 1 dated September 22, 2003, and Volume 5 of the Department's Foreign Affairs Manual, provide the basis for the security classification program of the U.S. Department of State ("the Department") implementing Executive Order 12958, "Classified National Security Information", as amended ("the Executive Order").

§ 9.2 Objective.

The objective of the Department's classification program is to ensure that national security information is protected from unauthorized disclosure, but only to the extent and for such a period as is necessary.

§ 9.3 Senior agency official.

The Executive Order requires that each agency that originates or handles classified information designate a senior agency official to direct and administer its information security program. The Department's senior agency official is the Under Secretary of State for Management. The senior agency official is assisted in carrying out the provisions of the Executive Order and the Department's information security

program by the Assistant Secretary for Diplomatic Security, the Assistant Secretary for Administration, and the Deputy Assistant Secretary for Information Sharing Services.

§ 9.4 Original classification.

(a) *Definition.* Original classification is the initial determination that certain information requires protection against unauthorized disclosure in the interest of national security (*i.e.*, national defense or foreign relations of the United States), together with a designation of the level of classification.

(b) *Classification 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 that the original classification authority is able to identify or describe.

(2) *Secret* shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) *Confidential* shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(c) *Classification requirements and limitations.* (1) Information may not be considered for classification unless it concerns:

(i) Military plans, weapons systems, or operations;

(ii) Foreign government information;

(iii) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(iv) Foreign relations or foreign activities of the United States, including confidential sources;

(v) Scientific, technological, or economic matters relating to the national security; which includes defense against transnational terrorism;

(vi) United States Government programs for safeguarding nuclear materials or facilities;

(vii) Vulnerabilities or capabilities of systems, installations, infrastructures,

Department of State

§ 9.6

projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(viii) Weapons of mass destruction.

(2) In classifying information, the public's interest in access to government information must be balanced against the need to protect national security information.

(3) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error, or 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 the national security.

(4) A reference to classified documents that does not directly or indirectly disclose classified information may not be classified or used as a basis for classification.

(5) Only information owned by, produced by or for, or under the control of the U.S. Government may be classified.

(6) The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

(d) *Duration of classification.* (1) Information shall be classified for as long as is required by national security considerations, subject to the limitations set forth in section 1.5 of the Executive Order. When it can be determined, a specific date or event for declassification in less than 10 years shall be set by the original classification authority at the time the information is originally classified. If a specific date or event for declassification cannot be determined, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years.

(2) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under the Executive Order are met.

(3) Information marked for an indefinite duration of classification under predecessor orders, such as "Originating Agency's Determination Required" (OADR) or containing no declassification instructions shall be subject to the declassification provisions of Part 3 of the Order, including the provisions of section 3.3 regarding automatic declassification of records older than 25 years.

§ 9.5 Original classification authority.

(a) Authority for original classification of information as *Top Secret* may be exercised by the Secretary and those officials delegated this authority in writing by the Secretary. Such authority has been delegated to the Deputy Secretary, the Under Secretaries, Assistant Secretaries and other Executive Level IV officials and their deputies; Chiefs of Mission, Charge d'Affaires, and Principal Officers at autonomous posts abroad; and to other officers within the Department as set forth in Department Notice dated May 26, 2000.

(b) Authority for original classification of information as *Secret or Confidential* may be exercised only by the Secretary, the Senior Agency Official, and those officials delegated this authority in writing by the Secretary or the Senior Agency Official. Such authority has been delegated to Office Directors and Division Chiefs in the Department, Section Heads in Embassies and Consulates abroad, and other officers within the Department as set forth in Department Notice dated May 26, 2000. In the absence of the Secret or Confidential classification authority, the person designated to act for that official may exercise that authority.

§ 9.6 Derivative classification.

(a) *Definition.* Derivative classification is the incorporating, paraphrasing, restating or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material. Duplication or reproduction of existing classified information is not derivative classification.

(b) *Responsibility.* Information classified derivatively from other classified information shall be classified and