

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 Sharing other-agency classified information.
- 9.13 Access to classified information by historical researchers and certain former government personnel.
- 9.14 Pre-publication review of writings by former Department personnel.
- 9.15 Assistance to the Historian's Office.
- 9.16 Safeguarding.

AUTHORITY: E.O. 13526 (75 FR 707, January 5, 2010); Information Security Oversight Office Directive 32 CFR part 2001 (75 FR 37254, June 28, 2010).

SOURCE: 79 FR 35936, June 25, 2014, unless otherwise noted.

§ 9.1 Basis.

The regulations in this part, taken together with 32 CFR part 2001 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 13526 on Classified National Security Information ("the Executive Order" or "the 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 that it remains classified 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 Global Information 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 considerations.* (1) Information may not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of the Executive Order, and it pertains to one or more of the following:

- (i) Military plans, weapons systems, or operations;
- (ii) Foreign government information;
- (iii) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (iv) Foreign relations or foreign activities of the United States, including confidential sources;

Department of State

§ 9.5

(v) Scientific, technological, or economic matters relating to the national security;

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

(vii) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(viii) The development, production, or use of 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) The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

(d) *Classification limitations and prohibitions.* (1) 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.

(2) 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.

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

(e) *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 be marked for

declassification for up to 25 years from the date of the original decision except for:

(i) Information that would reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, in which case the duration of classification shall be up to 75 years and shall be designated with the markings "50X1-HUM" and "50X2-WMD," respectively; and

(ii) Specific information incorporated into the classification guide under section 2.2(e) of the Executive Order relating to exemptions from automatic declassification.

(2) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, 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) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, such as "Originating Agency's Determination Required" (OADR) or classified information that contains incomplete declassification instructions or lacks declassification instructions, shall be declassified in accordance with Part 3 of the Order.

§ 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 Secretaries, the Under Secretaries, the Counselor, Assistant Secretaries and equivalents; Chiefs of Mission and U.S. representatives to international organizations; and certain other officers within the Department and at posts abroad.

(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