(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, 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 marked in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide and shall comply with the standards set forth in sections 2.1–2.2 of the Executive Order and the ISOO implementing directives in 32 CFR 2001.22.

(c) *Department of State Classification Guide*. The Department of State Classification Guide (DSCG) is the primary authority for the classification of information in documents created by Department of State personnel. The Guide is classified ''Confidential'' and is found on the Department of State's classified Web site.

§ 9.7 Identification and marking.

(a) Classified information shall be marked pursuant to the standards set forth in section 1.6 of the Executive Order; ISOO implementing directives in 32 CFR 2001, Subpart B; and internal Department guidance in 12 Foreign Affairs Manual (FAM).

(b) Foreign government information shall retain its original classification markings or be marked and classified at a U.S. classification level that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(c) Information assigned a level of classification under predecessor executive orders shall be considered as classified at that level of classification.

§ 9.8 Classification challenges.

(a) *Challenges*. Holders of information pertaining to the Department of State who believe that its classification status is improper are expected and encouraged to challenge the classification status of the information. Holders of information making challenges to the classification status of information shall not be subject to retribution for such action. Informal, usually oral, challenges are encouraged. Formal challenges to classification actions shall be in writing to an original classification authority (OCA) with jurisdiction over the information and a copy of the challenge shall be sent to the Office of Information Programs and Services (IPS) of the Department of State, SA–2, 515 22nd St. NW., Washington, DC 20522–6001. The Department (either the OCA or IPS) shall provide an initial response in writing within 60 days.

(b) *Appeal procedures and time limits*. A negative response may be appealed to the Department's Appeals Review Panel (ARP) and should be sent to: Chairman, Appeals Review Panel, c/o Information and Privacy Coordinator/Appeals Officer, at the IPS address given above. The appeal shall include a