

significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) *Confidential*. Information may be classified "Confidential" if its unauthorized disclosure could reasonably be expected to cause damage to the national security. Except as otherwise provided by statute, no other terms shall be used to identify classified information. Terms or phrases such as "For Official Use Only" or "Limited Official Use" shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these national security information designations, such as "Secret Sensitive" or "Agency Confidential" to identify national security information.

(b) *Foreign government information*. If classified by the foreign government, the information shall either retain its original classification or be assigned a U.S. classification designation which will ensure a degree of protection at least equivalent to that required by the entity that furnished the information. If not given a specific classification by the foreign government, the information will be assigned an appropriate classification dependent on the sensitivity of the subject matter and the degree of damage its unauthorized disclosure could reasonably be expected to cause to the national security. Classification designations assigned by the U.S. agency shall be marked on the foreign government information in accordance with the provisions of §9.12.

§9.6 Requirements for classification.

With the exception of the Atomic Energy Act of 1954, as amended, these regulations are the only basis for classifying information in the agencies named herein. To be eligible for classification, information must meet the two following requirements:

(a) First, it must deal with one of the following criteria:

- (1) Military plans, weapons, or operations;
- (2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- (3) Foreign government information;

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

(5) Foreign relations or foreign activities of the United States;

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

(7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) Confidential sources; or

(10) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. In the Department of State, the DAS/CDC, as the senior official, shall recommend such other categories of information to the Secretary. Any determination made under this subsection shall be reported promptly to the Director of ISOO.

(b) Second, an official with original classification authority must determine that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(c) Certain information which would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or record copy of the information.

§9.7 Classification authority.

(a) In the Department of State authority for original classification of information as "Top Secret" may be exercised only by the Secretary of State and those officials delegated this authority in writing, by position or by name, by the Secretary or the DAS/

Department of State

§ 9.10

CDC, as the senior official, on the basis of their frequent need to exercise such authority. Normally these will not be below the level of Deputy Assistant Secretary in the Department; or Chief of Mission, Charge d’Affairs, or principal officer at an autonomous consular post overseas.

(b) Authority for original classification of information as “Secret” may be exercised by officials with Top Secret authority, the Administrator of AID, and the Director of USIA. This authority may be delegated to such subordinate officials as the senior official in the Department, the administrator of AID or the Director of USIA may designate in writing, by position or by name, on the basis of their frequent need to exercise such authority. Normally, these will not be below the level of office director, section head (in a mission abroad), country public affairs officer, or equivalent.

(c) Authority for original classification of information as “Confidential” may be exercised by officials with Top Secret or Secret classification authority, and the President of the Overseas Private Investment Corporation; and may be delegated to such subordinate officials as the senior official in the Department, the Administrator of AID, the Director of USIA, or the President of OPIC may designate in writing, by position or by name, on the basis of their frequent need to exercise such authority.

(d) Delegated original classification authority at any level may not be re-delegated.

(e) In the absence of an authorized classifier, the person designated to act for that official may exercise the classifying authority.

(f) In the Department of State the Classification/Declassification Center, and in AID and USIA the Office of Security, shall maintain a current listing, by classification designation, of the positions or officials carrying original classification authority. The listing shall be reviewed as needed to ensure that such delegations have been held to a minimum, and that officials so designated have a continuing need to exercise such authority.

§ 9.8 Limitations on classification.

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

§ 9.9 Duration of classification.

(a) Information shall be classified for as long as is required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Information classified under predecessor orders that is not subject to automatic declassification or that is marked for review before declassification shall remain classified until reviewed for declassification.

(c) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions as soon as possible. The authority to extend the classification of information subject to automatic declassification under predecessor orders is limited to those officials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the ISOO.

§ 9.10 Derivative classification.

(a) Derivative classification is made by a person, not necessarily having original classification authority, based on an originally classified document or as directed by a classification guide. The derivative classifier may be one who reproduces, extracts, restates, paraphrases, or summarizes classified materials, or applies markings in accordance with source material or a classification guide.