

passes for signature or approval becomes jointly responsible with the accountable classifier for the classification assigned. Such official has discretion to decide whether a subordinate who has classification authority shall be identified as the accountable classifier when he or she has exercised that authority.

(c) *Classification Planning.* (1) Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification must be considered from the outset to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project or procurement action.

(2) The official charged with developing any plan, program or project in which classification is a factor, shall include under an identifiable title or heading, classification guidance covering the information involved. The guidance shall conform to the requirements contained in § 159a.17.

(d) *Challenges to Classification.* If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily, they shall communicate that belief to their security manager or the classifier of the information to bring about any necessary correction.

(1) Each DoD Component shall establish procedures whereby holders of classified information may challenge the decision of the classifier.

(2) Challenges to classification made under this subsection shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification shall also include the reason or reasons why the challenger believes that the information is classified improperly or unnecessarily.

(3) Challenges received under this subsection shall be acted upon within 30 days of receipt. The challenger shall be notified of any changes made as a result of the challenge or the reasons why no change is made.

(4) Pending final determination of a challenge to classification, the information or document in question shall be safeguarded as required for the level of classification initially assigned.

(5) The fact that an employee or military member of the Department of Defense has issued a challenge to classification shall not in any way result in or serve as a basis for adverse personnel action.

(6) The provisions of this paragraph do not apply to or affect declassification review actions undertaken under the mandatory review requirements of § 159a.26 of this part or under the provisions of 32 CFR part 285.

§ 159a.15 Classification principles, criteria, and considerations.

(a) *Reasoned Judgment.* Reasoned judgment shall be exercised in making classification decisions. A positive basis must exist for classification. Both advantages and disadvantages of classification must be weighed. If, after consideration of the provisions of this section, there is reasonable doubt, the provisions of § 159a.10(a)(2) apply.

(b) *Identification of Specific Information.* Before a classification determination is made, each item of information that may require protection shall be identified. This requires identification of that specific information that comprises the basis for a particular national advantage or advantages that, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting national security.

(c) *Specific Classifying Criteria.* A determination to classify shall be made only by an original classification authority when, *first*, the information is within paragraphs (c) (1) through (10) of this section; and *second*, 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. The determination involved in the first step is separate and distinct from that in the second. Except as provided in paragraph (d) of this section, the fact that the information falls under one or more of the criteria shall

not mean that the information *automatically* meets the damage criteria. Information shall be considered for classification if it concerns:

- (1) Military plans, weapons, or operations;
- (2) 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) A confidential source; or
- (10) Other categories of information that are related to national security and that require protection against unauthorized disclosure as determined by the Secretary of Defense or Secretaries of the Military Departments. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through channels to the appropriate Secretary for determination. Each such determination shall be reported promptly to the Director of Security Plans and Programs, ODUSD(P), for promulgation in an Appendix to this part and reporting to the Director, ISOO.

(d) *Presumption of Damage.* 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.

(e) *Limitations on Classification.* (1) classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

(2) Basic scientific research information not clearly related to national security may not be classified.

(3) A product of nongovernment research and development that does not incorporate or reveal classified infor-

mation to which the producer or developer was given prior access may not be classified until and unless the government acquires a proprietary interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952.

(4) References to classified documents that do not reveal classified information may not be classified or used as a basis for classification.

(5) Classification may not be used to limit dissemination of information that is not classifiable under the provisions of E.O. 12356 or this part or to prevent or delay public release of such information.

(6) Information may be classified or reclassified after receiving a request for it under the Freedom of Information Act, the Privacy Act, or the mandatory review provisions of this part (§159a.26) if such classification is consistent with this part and is accomplished personally and on a document-by-document basis, except as provided in paragraph (e)(7) of this section, by the Secretary or Deputy Secretary of Defense, by the Secretaries or Under Secretaries of the Military Departments, by the senior official designated by each Secretary under §5.3(a) of E.O. 12356, or by an official with original Top Secret classification authority.

(7) The Secretary of Defense and the Secretaries of the Military Departments may reclassify information previously declassified and disclosed, and they may classify unclassified information that has been disclosed, if they determine in writing that the information requires protection in the interest of national security and the information may reasonably be recovered. Any such reclassification or classification shall be reported to the DUSD(P) for subsequent reporting to the Director, ISOO.

(f) *Classifying Scientific Research Data.* Ordinarily, except for information that meets the definition of Restricted Data, basic scientific research or its results shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific breakthrough and there is sound reason to believe that it is not known or within the state-of-the-art of other nations, and it supplies

the United States with an advantage directly related to national security.

(g) *Classifying Documents.* Each document and portion thereof shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference citation, standing alone, reveals classified information. The overall classification of a document or group of physically-connected documents shall be at least as high as that of the most highly classified component. The subject or title of a classified document normally should be unclassified. When the information revealed by a subject or title warrants classification, an unclassified short title should be added for reference purposes.

(h) *Classifying Material Other Than Documents.* (1) Items of equipment or other physical objects shall be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or by their operation, test, application, or use. The overall classification assigned to end items of equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

(2) If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

(i) *State of the Art and Intelligence.* Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state-of-the-art in other nations may often be a vital consideration.

(j) *Effect of Open Publication.* Classified information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Appearance in the public domain of information currently clas-

sified or being considered for classification does not preclude initial or continued classification. However, such disclosures require immediate determination of the degree of damage to the national security and reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. Holders should continue classification until advised to the contrary by a competent government authority.

(k) *Reevaluation of Classification Because of Compromise.* Classified information, and information related thereto, that has been lost or possibly compromised, shall be reevaluated and acted upon as follows:

(1) The original classifying authority, upon learning that a loss or possible compromise of specific classified information has occurred, shall prepare a written damage assessment and;

(i) Reevaluate the information involved and determine whether (A) Its classification should be continued without change; (B) The specific information, or parts thereof, should be modified to minimize or nullify the effects of the reported compromise and the classification retained; (C) Declassification, downgrading, or upgrading is warranted; and (D) Counter-measures are appropriate and feasible to negate or minimize the effect of the compromise.

(ii) Give prompt notice to all holders of such information when the determination is within categories (A), (C), or (D) of paragraph (k)(1)(i) of this section.

(2) Upon learning that a compromise or probable compromise has occurred, any official having original classification jurisdiction over related information shall reevaluate the related information and determine whether one of the courses of action enumerated in paragraph (k)(1)(i) of this section should be taken or, instead, whether upgrading of the related information is warranted. When such a determination is within categories (B), (C), or (D) of

paragraph (k)(1)(i) of this section, that upgrading of the related items is warranted, prompt notice of the determination shall be given to all holders of the related information.

(l) *Compilation of Information.* Certain information that would otherwise be unclassified may require classification when combined or associated with other unclassified information. However, a compilation of unclassified items of information should normally not be classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification under paragraph (c) of this section. Classification on this basis shall be fully supported by a written explanation that will be provided with the material so classified.

(m) *Extracts of Information.* Information extracted from a classified source shall be derivatively classified or not classified in accordance with the classification markings shown in the source. The overall and internal markings of the source should supply adequate classification guidance. If internal markings or classification guidance are not found in the source, and no reference is made to an applicable and available classification guide, the extracted information shall be classified according either to the overall marking of the source, or guidance obtained from the classifier of the source material.

§ 159a.16 Duration of original classification.

(a) *General.* When a determination is made by an official with authority to classify originally information as Top Secret, Secret, or Confidential, such official must also determine how long the classification shall remain in effect.

(b) *Duration of Classification.* (1) Information shall be classified as long as required by national security considerations.

(2) 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 classified originally. Such dates or events shall be consistent with na-

tional security. Any event specified for declassification shall be an event certain to occur.

(3) Original classification authorities may not be able to predetermine a date or event for automatic declassification in which case they shall provide for the indefinite duration of classification.

(4) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this part.

(c) *Subsequent Extension of Duration of Classification.* The duration of classification specified at the time of original classification may be extended only by officials with requisite original classification authority and only if all known holders of the information can be notified of such action before the date or event previously set for declassification. Any decision to continue classification of information designated for automatic declassification under E.O. 12065 or predecessor orders, other than on a document-by-document basis, shall be reported to the DUSD(P) who shall, in turn, report to the Director, ISOO.

§ 159a.17 Classification guides.

(a) *General.* (1) A classification guide shall be issued for each classified system, program, plan, or project as soon as practicable before the initial funding or implementation of the system, program, plan or project. Successive operating echelons shall prescribe more detailed supplemental guides that are considered essential to assure accurate and consistent classification. In preparing classification guides, originators shall review DoD 5200.1-H⁵.

(2) Classification guides shall:

(i) Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly;

(ii) State which the classification designations (that is, Top Secret, Secret, or Confidential) applies to each element or category of information;

(iii) State declassification instructions for each element or category of information in terms of a period of

⁵See footnote 2 to § 159a.3.