a. Information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of the national security.

b. Basic scientific research and its results may not be classified unless clearly related to the national security.

3. LEVELS OF CLASSIFICATION. Information identified as requiring protection against unauthorized disclosure in the interest of national security shall be classified Top Secret, Secret, or Confidential. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information.

a. Top Secret. 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 OCA is able to identify or describe.

b. Secret. 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 OCA is able to identify or describe.

c. Confidential. Confidential shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

4. ORIGINAL CLASSIFICATION

a. Original classification is the initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

b. Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing. Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the Department of Defense. The authority shall be delegated to, and retained by, only those officials who have a demonstrable and continuing need to exercise it.

c. Authority to classify information at any lower level of classification is inherent in delegation of OCA.

(1) Top Secret OCA. Information may be originally classified Top Secret only by the Secretary of Defense, the Secretaries of the Military Departments, or those officials to whom the Secretary of Defense or the Secretaries of the Military Departments have delegated this authority in writing.

(2) Secret and Confidential OCA. Information may be originally classified Secret or Confidential only by the Secretary of Defense, the Secretaries of the Military Departments, and those officials to whom such authority has been delegated in writing by the Secretary of Defense, the Secretaries of the Military Departments, or the senior agency officials of the Military Departments or Department of Defense appointed in accordance with section 5.4(d) of Reference (d), provided those senior agency officials have also been delegated original Top Secret classification authority.

5. REQUESTS FOR OCA

a. Requests for OCA for officials serving in the OSD and the DoD Components, other than the Military Departments, including the Office of the Chairman of the Joint Chiefs of Staff, the Joint Staff, and the Combatant Commands, shall be submitted to the USD(I). These requests shall specify the position title for which the authority is requested, provide a brief, mission-specific justification for the request, and be submitted through established organizational channels. Heads of DoD Components, excluding the Military Departments, delegated Top Secret OCA are not authorized to delegate Secret and Confidential classification authority to subordinate officials.

b. Requests for OCA shall be approved only when:

(1) There is a demonstrable and continuing need to exercise OCA during the normal course of operations. (As a general rule, absent a security classification guide, an OCA must exercise this authority an average of twice a year to justify and retain designation as an OCA.)

(2) Such demonstrable and continuing need cannot be met through issuance of security classification guides by existing OCAs in the chain of command.

(3) Referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical for reasons such as geographical separation.

(4) Sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making.

c. OCA is designated by virtue of position. Each OCA delegation shall be in writing and the authority shall not be redelegated except as provided in paragraph 4.c. of this enclosure. Each

delegation shall identify the official to whom authority is delegated by position title. The Director of Security, OUSD(I), shall be notified in writing of all OCA delegations.

(1) Only senior positions (typically general and/or flag officer or Senior Executive Service or equivalent level) assigned a unique mission with responsibility in one of the subject areas cited in paragraph 1.b. of this enclosure may be designated an OCA.

(2) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to exercise the OCA when they have been officially designated to assume the duty position of the OCA in an "acting" capacity during the OCA's absence and have certified in writing that they have received the OCA training required by Enclosure 5 of Volume 3 of this Manual.

d. Before exercise of the authority and annually thereafter, persons in positions with delegated OCA must certify in writing that they have received training in the fundamentals of proper security classification and declassification, the limitations of their authority, the sanctions that may be imposed, and OCA duties and responsibilities, as required by Enclosure 5 of Volume 3 of this Manual.

e. Activity security managers must ensure that OCA delegation letters and OCA training certifications are maintained and can be retrieved by the office assigned that responsibility when requested by appropriate authorities.

6. ORIGINAL CLASSIFICATION PROCESS. All DoD OCAs are responsible to the Secretary of Defense for their classification decisions. In making a decision to originally classify information, they shall:

a. Determine that the information is owned by, produced by or for, or is under the control of the U. S. Government.

b. Determine the information falls within one or more of the categories of information listed in paragraph 1.b. of this enclosure.

c. Determine the information has not already been classified by another OCA.

d. Determine that classification guidance is not already available in the form of security classification guides, plans, or other memorandums. Within the Department of Defense, the majority of existing classification guidance is indexed and promulgated via the DTIC, available at www.dtic.mil.

e. Determine that there is a reasonable possibility that the information can be provided protection from unauthorized disclosure. OCAs shall balance the cost to protect the information against the risks associated with its disclosure. The advantages must outweigh the disadvantages of classification.

f. Determine and assign the appropriate level of classification (i.e., Top Secret, Secret, or Confidential) to be applied to the information, based on reasoned judgment as to the degree of damage, which the OCA can describe, that could be caused by unauthorized disclosure. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

(1) Determine the probable operational, technological, and resource impact of classification.

(2) If decisions must be rendered verbally due to exigencies of an ongoing operation or other emergency, issue written confirmation within 7 calendar days of the decision and provide the required declassification and marking instructions.

(3) Be prepared to present, as required, depositions and expert testimony in courts of law concerning classification of national security information and to justify their original decisions.

(4) Be prepared to produce a written description of the damage, as necessary, for a classification challenge, a security classification review, a damage assessment, a request for mandatory review for declassification, a request for release under section 552 of title 5, U.S.C. (also known and hereinafter referred to as "The Freedom of Information Act" (FOIA) (Reference (av))), when pertinent to judicial proceedings, or as other statute or regulation may require.

g. Determine the appropriate duration of classification to be applied to the information. Section 13 of this enclosure discusses the specific options available in making this decision.

h. Document the classification decision and clearly and concisely communicate it in writing to persons who shall possess the information by issuing classification guidance or by ensuring documents containing the information are properly marked to reflect the decision. Classification guidance may be communicated by issuance of a security classification or declassification guide or in the form of a memorandum, plan, order, or letter. If issued by other than a classification or declassification guide, the guidance should be incorporated in a guide in a timely fashion. Enclosure 6 of this Volume discusses classification guides; Volume 2 of this Manual provides marking guidance.

7. CHANGING THE LEVEL OF CLASSIFICATION. OCAs may change the level of classification of information under their jurisdiction, provided the information continues to meet the standards for classification identified in this enclosure. Documents shall be re-marked with the new classification level, the date of the action, and the authority for the change. Changing the classification level may also require changing portion markings for information contained within the document. Additionally, the OCA shall update appropriate security classification guides and immediately notify all known holders of the information of the changes. Sections 18 and 19 of Enclosure 5 of this Volume provide additional guidance on downgrading and upgrading classified information.