CHAPTER 2

ORIGINAL CLASSIFICATION

Section 1

General Provisions

Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure, and that the interests of the national security are best served by applying the safeguards of the Information Security Program to protect it. This decision may be made only by persons who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information. The decision must be made in accordance with the requirements of this chapter.

Section 2

Original Classification Authority

2-200 **Policy**

Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials who have been specifically delegated this authority in writing. Delegations of original classification authority shall be limited to the minimum required for effective operation of the Department of Defense. The authority shall be delegated only to officials who have a demonstrable and continuing need to exercise it.

2-201 **Delegation of Authority**

a. Information may be originally classified Top Secret only by the Secretary of Defense, the Secretaries of the Military Departments, or those officials who have been specifically delegated this authority in writing by the Secretary of Defense or the Secretaries of the Military Departments.

b. Information may be originally classified Secret or Confidential only by the Secretary of Defense, the Secretaries of the Military Departments, and the senior agency officials appointed by them in accordance with Section 5.6(c) of E.O. 12958 provided those senior agency officials have also been delegated original Top Secret classification authority. Senior Agency Officials of the Military Departments may further delegate original Secret and Confidential classification authority as necessary to respond to requests received under the provisions of paragraphs c and d. below.

c. Requests for original classification authority for officials serving in OSD and the DoD Components other than the Military Departments shall be submitted to the ASD(C3I). These requests will specify the position title for which the authority is requested, provide a brief justification for the request, and be submitted through established organizational channels.

d. Requests for original classification authority shall be granted only when (1) original classification is required during the normal course of operations in the organization, (2) sufficient expertise and information is available to the prospective original classification authority to permit effective classification decision-making, (3) the need for original classification cannot be eliminated by issuance of classification guidance by existing original classification authorities, and (4) referral of decisions to existing original classification authorities at higher levels in the chain of command or supervision is not practical.

2-202 **Required Training**

Persons who have been delegated original classification authority must receive training as required by Chapter 9 of this Regulation before they can exercise the delegated authority.

Section 3

The Original Classification Process

2-300 Overview

In making a decision to originally classify information, designated DoD original classification authorities 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 that the information falls within one or more of the categories of information listed in subsection 2-301, below;

c. Determine that the unauthorized disclosure of the information could be expected to result in damage to the national security and be able to identify or describe the damage;

d. Select the appropriate level of classification to be applied to the information, based on a judgment as to the degree of damage that could be caused by unauthorized disclosure;

e. Determine the appropriate declassification instructions to be applied to the information; and

f. Communicate the classification decision as required by subsection 2-306, below.

2-301 Eligibility for Classification

Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.5 of Executive Order 12958:

a. Military plans, weapon systems, or operations;

b. Foreign government information;

c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

d. Foreign relations or foreign activities of the United States, including confidential sources;

e. Scientific, technological, or economic matters relating to the national security;

f. United States Government programs for safeguarding nuclear materials or facilities; or

g. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

2-302 Possibility of Protection

The original classification authority must determine that, if classification is applied or reapplied, there is a reasonable possibility that the information can be provided protection from unauthorized disclosure. (See paragraph 2-402d. and e., below.)

2-303 The Decision to Classify

a. The decision to apply classification involves two sub-elements, both of which require the application of reasoned judgment on the part of the classifier. The first is the determination that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security of the United States, and that the damage can be identified or described. It is not necessary for the original classifier to produce a written description of the damage at the time of classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request for release under the Freedom of Information Act.

b., The second step in this decision is to determine the probable operational, technological and resource impact of classification.

c. If there is significant doubt about the need to classify information, it shall not be classified.

2-304 Level of Classification

The original classifier, again using reasoned judgment, must determine which level of classification is to be applied. If there is significant doubt about the appropriate level of classification, the information shall be classified at the lower level.

a. 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.

b. 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.

c. 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.

2-305 **Duration of Classification**

At the time of original classification, the original classifier must make a decision about the length of time the information shall require the protection of security classification. The specific options available in making this decision are discussed in Chapter 3 of this Regulation.

2-306 **Communicating the Decision**

An original classification authority who makes a decision to originally classify information is responsible for ensuring the decision is effectively communicated to persons who will be in possession of the information. This may be accomplished by issuing classification guidance, discussed in Section 5 of this chapter, or by ensuring that a document containing the information is properly marked to reflect the decision. Marking of classified documents is covered by Chapter 5 of this Regulation.

Section 4

Special Considerations

2-400 **Compilation**

In unusual circumstances, compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that a. qualifies for classification under this Regulation, and b. is not otherwise revealed by the individual information. Classification by compilation must meet the same criteria in terms of justification as other original classification actions. (See paragraph 5-206c and subsection 5-302, below, for marking requirements.)

2-401 **The Acquisition Process**

Classification of information involved in the DoD acquisition process shall conform to the requirements of DoD Directive 5000.1, DoD Regulation 5000.2-R, and DoD Regulation 5000.2-R as well as this chapter.

2-402 **Limitations and Prohibitions**

a. 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.

b. Basic scientific research and its results maybe classified only if it clearly relates to the national security.

c. Classification may not be used to prevent or delay the release of information that does not require protection in the interest of the national security.

d. The reclassification of information which was once classified but was declassified and officially released to the public is prohibited.

e. Information may be classified or reclassified after receipt of a request for it under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of E.O. 12958 only if it is done on a document-by-document basis with the personal participation or under the direction of the Secretary of Defense or Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, or the senior agency official appointed within OSD or a Military Department in accordance with Section 5.6(c) of E.O. 12958.

f. Information that is a product of nongovernment research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may be classified only as provided in Section 6 of this chapter.

Section 5

Security Classification and/or Declassification Guides

2-500 Policy

A security classification guide shall be issued for each system, plan, program, or project in which classified information is involved.

2-501 **Content**

a. Security classification guides shall:

(1) Identify specific items, elements or categories of information to be protected;

(2) State the specific classification to be assigned to each item or element of information and, when useful, specify items of information that are unclassified;

(3) Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from automatic declassification;

(4) State a concise reason for classification for each item, element, or category of information that, at a minimum, cites the applicable classification category (ies) in Section 1.5 of E.O.12958 (See subsection 2-304, of this Regulation, above;

(5) Identify any special handling caveats that apply to items, elements, or categories of information;

(6) Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of approval; and

(7) Provide a point-of-contact for questions about the guide and suggestions for improvement.

b. For information exempted from automatic declassification because its disclosure would reveal foreign government information or violate a statute, treaty or international agreement (see subsections 4-202 and 4-301 of this Regulation, below), the guide will identify the government or specify the applicable statute, treaty or international agreement as appropriate.

2-502 **Approval, Distribution and Indexing**

a. Security classification guides shall be approved personally and in writing by an original classification authority who is authorized to classify information at the highest level established by the guide, and who has program or supervisory responsibility for the information or the organization's Information Security Program.

b. Security classification guides shall be distributed by the originating organization to those organizations and activities they believe will be derivatively classifying information covered by the guide.

c. One copy of each guide shall be forwarded to the Director of Freedom of Information and Security Review, Office of the Assistant to the Secretary of Defense for Public Affairs. Guides that cover SCI or Special Access Program information and that contain information that requires special access controls are exempt from this requirement.

d. Two copies of each approved guide (other than those covering SCI or Special Access Program information, or guides determined by the approval authority for the guide to be too sensitive for automatic secondary distribution) shall be provided to the Administrator, Defense Technical Information Center (DTIC). Each guide furnished to DTIC must bear the appropriate distribution statement required by DoD Directive 5230.24.

e. Security classification guides issued under this Regulation will be indexed in DoD 5200.1-I, the DoD Index of Security Classification Guides. Originators of guides shall submit DD Form 2024, "DoD Security Classification Guide Data Elements" to the Administrator, DTIC, upon approval of the guide. If the originator determines that listing the guide in DoD 5200.1-1 would be inadvisable for security reasons, issuance of the guide shall be separately reported to the PD(IWS&CI), OASD(C3I), with an explanation of why the guide should not be listed. Special Access Program determinations shall be reported separately to the Director, Special Programs, ODTUSD(P)PS. Report Control Symbol DD-C3I (B&AR) 1418 applies to the reporting requirements of this paragraph,

2-503 **Review, Revision and Cancellation**

a. Security classification guides shall be reviewed by the originator for currency and accuracy at least once every five years. Changes identified as necessary in the review process shall be promptly made. If no changes are required, the record copy of the guide shall be so annotated, with the date of the review.

b. Guides shall be revised whenever necessary to promote effective derivative classification. When a guide is revised or reissued, computation of declassification instructions will continue to be based on the date of original classification of the information, not the date of revision or reissue.

c. Guides shall be canceled only when (1) all information specified as classified by the guide has been declassified, or (2) when the system, plan, program, or project has been canceled, discontinued, or removed from the inventory, (3) when a major restructure has occurred as the information is incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification. Impact of the cancellation on systems, plans, programs, and projects provided to other nations under approved foreign disclosure decisions; and impact of such decisions on existing U.S. classification guides of similar systems, plans, programs or projects shall be considered in the decision. Upon cancellation of a guide, the responsible official shall consider the need for publication of a declassification guide, discussed in subsection 4-102 of this Regulation below.

d. Revision, reissuance, review, and cancellation of a guide will be reported as required for new guides in paragraph 2-502e, above. Copies of changes, reissued guides, and cancellation notices will be distributed as required by paragraphs 2-502 b., c. and d., above.

Section 6
Information from Private Sources

2-600 **Policy**

Information that is a product of contractor or individual independent research and development (IR&D) or bid and proposal (B&P) efforts conducted without prior access to classified information or current access to classified information associated with the specific information in question may not be classified unless:

a. The U.S. Government first acquires a proprietary interest in the information; or

b. The contractor conducting the IR&D/B&P requests that the U.S. Government activity place the information under the control of the security classification system without relinquishing ownership of the information.

2-601 Classification Determination

a. The individual or contractor conducting an IR&D/B&P effort and believing that information generated without prior access to classified information or current access to classified information associated with the specific information in question may require protection in the interest of national security should safeguard the information and submit it to an appropriate U.S. Government activity for a classification determination.

b. The Government activity receiving such a request shall issue security classification guidance as appropriate if the information is to be classified. If the information is not under that activity's classification authority, the activity shall refer the matter to the appropriate classification authority or inform the individual or contractor to take that action. The information shall be safeguarded until the matter has been resolved.

c. The activity that holds classification authority over the information shall verify whether the individual or contractor is cleared and has been authorized storage capability. If not, the appropriate contracting authority for the activity shall advise whether clearance action should be initiated.

d. If the individual or contractor refuses to be processed for a clearance and the Government does not acquire a proprietary interest in the information, the information may not be classified.

2-602 **Patent Secrecy Act**

The Patent Secrecy Act of 1952 provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. See DoD Directive 5535.2. A patent application on which a secrecy order has been imposed shall be handled as follows within the Department of Defense:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly.

b. If the patent application does not contain information that warrants classification the following procedures shall be followed:

(1) A cover sheet (or cover letter for transmittal) shall be placed on the application with substantially the following language:

> The attached material contains information on which secrecy orders have bee issued by the U.S. Patent Office after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952,35 U.S.C. 181-188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified CONFIDENTIAL (or other classification as appropriate).

(2.) The information shall be withheld from public release; its dissemination within the Department of Defense shall be controlled; the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified material.

c. If tiling of a patent application with a foreign government is approved under provisions of the Patent Secrecy Act of 1952 and agreements on interchange of patent information for defense purposes, the copies of the patent application prepared for foreign registration (but only those copies) shall be marked at the bottom of each page as follows:

> Withheld under the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).
>
> Handle as CONFIDENTIAL (or such other level as has been determined appropriate),