ENCLOSURE 4

CLASSIFYING INFORMATION

1. TENTATIVE CLASSIFICATION. Individuals who submit information to OCAs for original classification decisions shall provide the OCA the information required by paragraphs 6.a. through 6.f. of this enclosure, and may, as necessary, tentatively classify information or documents as working papers, pending approval by the OCA. Final classification decisions must be made as soon as possible, but not later than 180 days from the initial drafting date of the document. Prior to the OCA's classification decision, such information shall be safeguarded as required for the specified level of classification and it shall not be used as a source for derivative classification.

2. DERIVATIVE CLASSIFICATION

a. When incorporating, paraphrasing, restating, or generating classified information in a new form or document (i.e., derivatively classifying information), it must be identified as classified information by marking or similar means. Derivative classification includes classification of information based on classification guidance in a security classification guide or other source material, but does not include photocopying or otherwise mechanically or electronically reproducing classified material.

b. Within the DoD all cleared personnel, who generate or create material that is to be derivatively classified, shall ensure that the derivative classification is accomplished in accordance with this enclosure. No specific, individual delegation of authority is required. DoD officials who sign or approve derivatively classified documents have principal responsibility for the quality of the derivative classification.

c. All persons performing derivative classification shall receive training, as specified in Enclosure 5 of Volume 3 of this Manual, on proper procedures for making classification determinations and properly marking derivatively classified documents.

3. RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS. Derivative classifiers shall:

a. Observe and respect the classification determinations made by OCAs. If derivative classifiers believe information to be improperly classified, they shall take the actions required by section 22 of this enclosure.

b. Identify themselves and the classified information by marking it in accordance with Volume 2 of this Manual.

c. Use only authorized sources for classification guidance (e.g., security classification guides, memorandums, DoD publications, and other forms of classification guidance issued by

the OCA) and markings on source documents from which the information is extracted for guidance on classification of the information in question. The use of memory alone or "general rules" about the classification of broad classes of information is prohibited.

d. Use caution when paraphrasing or restating information extracted from a classified source document. Paraphrasing or restating information may change the need for or level of classification.

e. Take appropriate and reasonable steps, including consulting a security classification guide or requesting assistance from the appropriate OCA, to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification. In cases of apparent conflict between a security classification guide and a classified source document regarding a discrete item of information, the instructions in the security classification guide shall take precedence. Where required markings are missing or omitted from source documents, consult the OCA, appropriate security classification guide, or other classification guidance for application of the omitted markings.

4. PROCEDURES FOR DERIVATIVE CLASSIFICATION

a. Derivative classifiers shall carefully analyze the material they are classifying to determine what information it contains or reveals and shall evaluate that information against the instructions provided by the classification guidance or the markings on source documents.

b. Drafters of derivatively classified documents shall portion-mark their drafts and keep records of the sources they use, to facilitate derivative classification of the finished product.

c. When material is derivatively classified based on "multiple sources" (i.e., more than one security classification guide, classified source document, or combination thereof), the derivative classifier shall compile a list of the sources used. This list shall be included in or attached to the document.

d. Duration of classification for derivatively classified documents shall be determined in accordance with section 13 of this enclosure and applied in accordance with Volume 2 of this Manual. The instructions shall not be automatically copied from source documents without consideration of adjustments that may be required (e.g., due to use of multiple sources, changes in policy, changes in classification guidance).

e. If extracting information from a document or section of a document classified by compilation, the derivative classifier shall consult the explanation on the source document to determine the appropriate classification. If that does not provide sufficient guidance, the derivative classifier shall contact the originator of the source document for assistance.

f. Infrequently, different sources of classification guidance may specify different classification for the same information. When such inconsistencies are encountered, the derivative classifier must contact the applicable OCA(s) for resolution of the inconsistency.

Pending determination, the document or material containing the information shall be protected at the highest level of classification specified by the sources.

5. DURATION OF CLASSIFICATION. Every time a classified document is created, a determination must be made regarding how long the information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification). This is an essential part of the classification process. For derivatively classified information, the most restrictive declassification instruction (i.e., the one that specifies the longest duration of classification) must be carried forward from the source document(s), security classification guide(s) or other classification guidance provided by the OCA. Specific guidance on determining the most restrictive instruction is provided in Enclosure 3 of Volume 2.

6. CLASSIFICATION OF ACQUISITION INFORMATION. Classifying information involved in the DoD acquisition process shall conform to the requirements of DoDD 5000.01 (Reference (az)) and DoDI 5000.02 (Reference (ba)), as well as this enclosure. Security classification guides should be updated to include classified critical program information identified as part of the program protection planning process required by DoDI 5200.39 (Reference (bb)).

7. CLASSIFICATION OF INFORMATION RELEASED TO THE PUBLIC

a. Classified Information Released Without Proper Authority

(1) Classified information that has been released to the public without proper authority (e.g., media leak, data spill) remains classified. It may be declassified upon such a determination by the appropriate OCA. Enclosure 6 of Volume 3 of this Manual identifies issues to be considered when making the decision. When the determination is made that the information will remain classified, the appropriate OCA will notify known authorized holders accordingly and provide the following marking guidance to be used in the event the information is not marked:

(a) Overall level of classification.

(b) Portion markings.

(c) Identity, by name or personal identifier and position, of the OCA.

(d) Declassification instructions.

(e) Concise reason for classification.

(f) Date the action was taken.

(2) Holders of the information shall take administrative action, as needed, to apply markings and controls. DoD personnel shall not publicly acknowledge the release of classified

information and must be careful not to make any statement or comment that confirms the accuracy of or verifies the information requiring protection.

b. Reclassification of Information Declassified and Released to the Public Under Proper Authority

(1) Information that has been declassified and released to the public under proper authority may be reclassified only when:

(a) The information may be reasonably recoverable without bringing undue attention to the information, which means that:

1. Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from them.

2. If the information has been made available to the public via means such as U.S. Government archives or reading rooms, it can be or has been withdrawn from public access without significant media or public attention or notice.

(b) The Secretary of Defense approves the reclassification based on a document-by-document determination and recommendation by the Head of the originating DoD Component, other than the Secretary of a Military Department, when that reclassification of the information is required to prevent significant and demonstrable damage to the national security. Reclassification and release of information under proper authority means the DoD Component with jurisdiction over the information authorized declassification and release of the information. The Secretaries of a Military Department shall approve the reclassification of information under their jurisdiction on the same basis and shall notify the USD(I&S) of the action. The Military Departments shall provide implementing guidance to their subordinate activities for submitting such requests.

(2) DoD Component Heads other than the Secretaries of the Military Departments shall submit recommendations for reclassification of information under their jurisdiction to the Secretary of Defense through the USD(I&S). Recommendations for reclassification must include, on a document-by-document basis:

(a) A description of the information.

(b) All information necessary for the original classification decision in accordance with Reference (bm), including classification level of the information and declassification instructions to be applied.

(c) When and how it was released to the public.

(d) An explanation as to why it should be reclassified. Include the applicable reason in accordance with Reference (d) and describe what damage could occur to national security. Also describe what damage may have already occurred as a result of the release.

(e) The number of recipients and/or holders and how they will be notified of the reclassification.

(f) How the information will be recovered.

(g) Whether the information is in the custody of NARA and whether the Archivist of the United States must be notified of the reclassification as specified in subparagraph 7.b.(4) of this section.

(3) Once a reclassification action has occurred, it must be reported to all recipients and holders, to the Assistant to the President for National Security Affairs (herein after referred to as "the National Security Advisor") and to ISOO within 30 days. The notification to ISOO must include how the "reasonably recoverable" decision was made, including the number of recipients or holders, how the information was recovered, and how the recipients and holders were notified. The Secretaries of the Military Departments shall notify the National Security Advisor and ISOO directly and provide an information copy to the USD(I&S). The Secretary of Defense, after making reclassification decisions, will notify the National Security Advisor and ISOO of such decisions.

(4) For documents in the physical and legal custody of NARA that have been available for public use, reclassification must also be reported to the Archivist of the United States, who shall suspend public access pending approval of the reclassification action by the Director, ISOO. The Secretaries of the Military Departments shall notify the Archivist directly and provide an information copy to USD(I&S). The Secretary of Defense will notify the Archivist as required for decisions involving other DoD Components. Disapproval of the reclassification action by the Director, ISOO, may be appealed to the President through the National Security Advisor. Public access shall remain suspended pending decision on the appeal.

(a) OCAs shall notify the Secretary of Defense of the need to appeal ISOO decisions through their DoD Component Head and the USD(I&S).

(b) Notifications shall clearly articulate the compelling national security reasons for reclassifying the information and shall counter the ISOO rationale for disapproving the reclassification.

(5) Once a final decision is rendered, OCAs shall update their security classification guidance accordingly. The reclassified information must be marked and safeguarded in accordance with the requirements of Volumes 2 and 3 of this Manual.

(6) Any cleared recipients or holders of reclassified information shall be notified and appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holder who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information to which they have had access and their obligation not to disclose the information, and shall be asked to sign an acknowledgement of the briefing and to return all copies of the information in their possession.

c. Information Declassified and Released to the Public Without Proper Authority. Information that was declassified without proper authority remains classified. See paragraph 7.a. of this enclosure and paragraph 1.c. of Enclosure 5 of this Volume.

8. CLASSIFICATION OR RECLASSIFICATION FOLLOWING RECEIPT OF A REQUEST FOR INFORMATION. Information that has not previously been released to the public under proper authority may be classified or reclassified after receiving a request for it under FOIA; section 2204(c)(1) of Reference (av) (also known as "The Presidential Records Act of 1978"); section 552a of Reference (ay) (also known and hereinafter referred to as "The Privacy Act of 1974, as amended"); or the mandatory review provisions of section 3.5 of Reference (d), only if it is done on a document-by-document basis with the personal participation or under the direction of the USD(I&S), the Secretary or Under Secretary of a Military Department, or the senior agency official appointed within a Military Department in accordance with section 5.4(d) of Reference (d). OCAs shall submit requests to the USD(I&S) through the Head of the DoD Component.

a. The provisions of this section apply to information that has been declassified in accordance with the date or event specified by the OCA as well as to information not previously classified.

b. Classification requests shall provide all information necessary for the original classification process as specified by Reference (bm).

c. The Secretaries of the Military Departments shall notify the USD(I&S) of classification decisions made in accordance with the provisions of this section.

d. Once a decision is rendered, OCAs shall update their security classification guidance as needed.

9. CLASSIFYING NON-GOVERNMENT RESEARCH AND DEVELOPMENT INFORMATION

a. Information that is a product of contractor or individual independent research and development (IR&D) or bid and proposal (B&P) efforts, as defined by DoDI 3204.01 (Reference (bc)), conducted without prior or current access to classified information associated with the specific information in question, may not be classified unless:

(1) The U.S. Government first acquires a proprietary interest in the information; or,

(2) The contractor or individual conducting the IR&D or B&P requests that the U.S. Government contracting activity place the information under the control of the security classification system without relinquishing ownership of the information.

b. The contractor or individual conducting such an IR&D or B&P effort and believing that the information generated may require protection in the interest of national security shall safeguard the information and submit it to an appropriate U.S. Government activity for a classification determination.

(1) The U.S. Government activity receiving the request shall issue security classification guidance, as appropriate, if the information is to be classified. If the information is not under the activity's classification authority, the activity shall refer the matter to the appropriate classification authority and inform the individual or contractor of the referral. The information shall be safeguarded until the matter is resolved.

(2) The U.S. Government activity authorizing classification for the information shall verify whether the contractor or individual is cleared and has been authorized to store classified information. If not, the U.S. Government activity authorizing classification shall advise whether security clearance action should be initiated.

(3) If the contractor or individual refuses to be processed for the appropriate security clearance and the U.S. Government does not acquire a proprietary interest in the information, the information may not be classified.

(4) If the information is not classified, consideration may be given to the need for other controls applicable to unclassified information (e.g., export controls). (See Volume 4 of this Manual for guidance on CUI.)

10. THE PATENT SECRECY ACT OF 1952. Sections 181 through 188 of title 35, U.S.C. (also known and hereinafter referred to as "The Patent Secrecy Act of 1952" (Reference (bd)) provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to the national security. The Department of Defense shall handle a patent application on which a secrecy order has been imposed as follows:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded commensurate with the level of classification.

b. Unclassified patent applications that do not contain information that warrants classification, but requires CUI safeguarding and dissemination controls, will be marked as a category of CUI in accordance with Volume 4 of this Manual. This same requirement applies to legacy patent applications marked with the former statement that required handling as CONFIDENTIAL.

11. REQUESTS FOR CLASSIFICATION DETERMINATION. Within 30 days of receipt OCAs shall provide a classification determination to requests for same from individuals who are not OCAs, but who believe they have originated information requiring classification. If the

information is not under the OCA's classification authority, the request shall be referred to the appropriate OCA and the requestor shall be informed of the referral. Pending a classification determination the information shall be protected consistent with the requirements of this Manual.

12. CHALLENGES TO CLASSIFICATION

a. Principles. If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the OCA to bring about any necessary correction. This may be done informally or by submitting a formal challenge to the classification in accordance with References (d) and (f).

(1) Informal questioning of classification is encouraged before resorting to formal challenge. If the information holder has reason to believe the classification applied to information is inappropriate, he or she should contact the classifier of the source document or material to resolve the issue.

(2) The Heads of the DoD Components shall ensure that no retribution is taken against any individual for questioning a classification or making a formal challenge to a classification.

(3) Formal challenges to classification made pursuant to this section shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification made by DoD personnel shall also include the reason why the challenger believes that the information is improperly or unnecessarily classified. The challenge shall be unclassified, if possible.

(4) Pending final decision on the classification level, the information that is the subject of a classification challenge will remain classified at its current classification level or the recommended change level, whichever is higher. The information will continue to be safeguarded unless and until a decision is made to declassify it.

(5) The provisions of this section do not apply to information required to be submitted for prepublication review or other administrative process pursuant to an approved NDA.

b. Procedures. The Heads of the DoD Components shall encourage classification challenges and establish procedures for handling challenges to classification received from within and from outside their Components in accordance with Reference (f). The DoD Components shall:

(1) Incorporate the following language for Component security classification guides consistent with the intent of Section 5.3 of Reference (d):

(a) Follow the guidance provided in Paragraph 12 of this enclosure for individuals who wish to challenge information they believe has been improperly or unnecessarily classified.

(b) Such challenges are encouraged, and expected, and should be forwarded through the appropriate channels to the office of primary responsibility.

(c) Pending final decision, handle and protect the information at its current classification level or at the recommended change level, whichever is higher.

(d) Challenges should include sufficient description to permit identification of the specific information under challenge with reasonable effort.

(e) Challenges should include detailed justification outlining why the information is improperly or unnecessarily classified.

(2) Establish a system for processing, tracking, and recording formal challenges to classification, including administrative appeals of classification decisions, and ensure that DoD Component personnel are made aware of the established procedures for classification challenges.

(3) Provide an opportunity for review of the information by an impartial official or panel.

(4) Except as provided in subparagraphs 12.b.(5) and (6) of this section, provide an initial written response to each challenge within 60 days. If not responding fully to the challenge within 60 days, the DoD Component shall acknowledge the challenge and provide an expected date of response. This acknowledgment shall include a statement that, if no response is received within 120 days, the challenger has the right to forward the challenge to the ISCAP for decision. The challenger may also forward the challenge to the ISCAP if the Component has not responded to an appeal within 90 days of receipt of the appeal. DoD Component responses to those challenges it denies shall include the challenger's right to appeal to the ISCAP.

(5) Not process the challenge if it concerns information that has been the subject of a challenge within the preceding 2 years or is the subject of pending litigation. The DoD Component shall inform the challenger of the situation and appropriate appellate procedures.

(6) Refer challenges involving RD to the Department of the Energy and FRD to the Deputy Assistant Secretary of Defense, Nuclear Matters (DASD(NM)) and notify the challenger accordingly. Do not include a statement about forwarding the challenge to the ISCAP in the notification letter, as these categories of information are not within the purview of the ISCAP.

(7) In case a classification challenge involves documents that contain RD and/or FRD as well as information classified under Reference (d), delete (redact) the RD and FRD portions of the documents before the document is forwarded to the ISCAP for review.