ENCLOSURE 6

SECURITY CLASSIFICATION GUIDES

1. GENERAL. Reference (d) requires issuance of classification guidance to facilitate proper and uniform derivative classification of information. Issuance of timely and precise classification guidance by the responsible OCA is a prerequisite to effective and efficient information security and assures that security resources are expended to protect only that information warranting protection in the interests of national security.

a. The responsible OCA shall issue a security classification guide for each system, plan, program, or project involving classified information and shall ensure it is reviewed and updated as provided by this enclosure. DoD 5200.1-H (Reference (bj)) provides guidance to assist in development of a security classification guide.

b. A security classification guide shall be issued as early as practical in the life cycle of the system, plan, program, or project, preferably prior to release of information regarding the system, plan, program, or project.

c. When possible, OCAs should communicate with others who are responsible for classification guidance for similar activities to ensure consistency and uniformity of classification decisions. Additionally, when possible OCAs should seek user input when reviewing guides for revision.

d. A security classification guide shall be classified by the approving OCA if it meets the requirement for being classified. If the guidance does not warrant classification, it shall be marked and protected as For Official Use Only (FOUO). Security classification guides shall not be released to the public nor posted on publicly accessible websites. If requested in accordance with FOIA, the section of the security classification guide that addresses the specific items to be classified, including the reasons for classification, shall be denied pursuant to exemption (b)(2) of the FOIA.

2. CONTENT OF SECURITY CLASSIFICATION GUIDES. Security classification guides shall:

a. Identify specific items or elements of information to be protected.

b. State the specific classification assigned to each item or element of information. Where an item or element of information may qualify for one of multiple classification levels (e.g., Unclassified to Secret), criteria must be provided for determining which classification level is applicable. Simply citing a range is not permissible.

c. State a concise reason for classifying each item, element, or category of information and cite the applicable classification category(ies) in section 1.4 of Reference (d).

d. State the declassification instructions for each item or element of classified information, including citation of the approved automatic declassification exemption category, if any.

(1) For information exempted from automatic declassification because disclosing it may reveal FGI or violate a statute, treaty, or international agreement (see subparagraphs 13.b.(1)(f) and 13.b.(1)(i) of Enclosure 5 of this Volume), the guide shall identify the government or specify the applicable statute, treaty, or international agreement as appropriate.

(2) Automatic declassification exemptions (25X1-25X9) authorized in accordance with section 13 of Enclosure 5 of this Volume may be cited in classification guides for use on derivatively classified documents once the declassification guide has been submitted to the ISCAP. The ISCAP must be notified in advance of the declassification guide's approval of the intent to cite such exemptions in applicable classification guides (refer to paragraph 13.c. of Enclosure 5 of this Volume), and the information being exempted must remain in active use.

(3) Where applicable, the security classification guide should refer to the declassification guide for specific declassification guidance.

e. Identify any special handling caveats (e.g., dissemination controls) that apply to items, elements, or categories of information. Where applicable, use remarks or a releasability annex to identify those elements of information approved, in accordance with established disclosure policies, by the appropriate disclosure authority(s) for routine release to specified foreign governments and international organizations.

f. Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of approval.

g. Provide a point of contact for questions about the guide and suggestions for improvement.

3. CUI AND UNCLASSIFIED ELEMENTS OF INFORMATION. OCAs and developers of security classification guides are encouraged to specify in security classification guides specific items or elements of unclassified information or CUI to be protected. Cite the appropriate classification (e.g., (U)) or CUI designation (e.g., FOUO), and identify any special handling caveats (e.g., export controls) that apply. FOUO information is information that should be withheld from the public because of foreseeable harm to an interest protected by the FOIA, as implemented by DoD 5400.7-R (Reference (bk)). See Volume 4 of this Manual for further information on CUI.

4. DATA COMPILATION CONSIDERATIONS. Posting of unclassified defense and U.S. Government information to publicly accessible Internet sites makes access to the information from anywhere in the world easy and affordable. Search capabilities and data mining tools make discovery and correlation of available information fast and simple. This ability to discover and analyze militarily-relevant data creates the need to pay particular attention to classified

compilations of data elements. Where specific combinations of unclassified data elements are known to be classified, CONSISTENTLY withholding specified data elements from public Internet posting and, to the extent possible consistent with statute and other regulations, public release can mitigate the ability of others to create the classified compilation. Thus, OCAs should consider including in security classification guides, where appropriate, prohibitions on posting one or more of the specific data elements that are known to make up a classified compilation of unclassified data elements to publicly accessible Internet sites. See section 15 of Enclosure 4 for guidance on classification by compilation.

5. APPROVAL OF SECURITY CLASSIFICATION GUIDES. An OCA shall personally approve, in writing, security classification guides. This OCA shall be an official who:

a. Has program or supervisory responsibility for the information, or is the senior agency official for Department of Defense or for the originating Military Department.

b. Is authorized to originally classify information at the highest level the guide specifies.

6. DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES. The originating organization shall:

a. Distribute security classification guides to those organizations and activities that may classify information the guide covers.

b. Forward one copy of each guide (including those issued as regulations, manuals, or other Component issuances) to the Office of Security Review, Washington Headquarters Service. Guides that cover SCI or SAP information and that contain information that requires special access controls are exempt from this requirement. The mailing address to use is:

Department of Defense
Office of Security Review
1155 Defense Pentagon
Washington, DC 20301-1155

c. Provide one copy of each approved guide (including those issued as regulations, manuals, or other issuances, but not those covering Top Secret, SCI or SAP information, or guides deemed by the guide's approval authority to be too sensitive for automatic secondary distribution) to the Administrator, DTIC, along with DD Form 2024. Each guide furnished to DTIC shall bear the appropriate distribution statement required by Reference (aj). (See also Enclosure 3 of Volume 2 for guidance on distribution statements.) DTIC's mailing address is:

Defense Technical Information Center
ATTN: DTIC-OA (Security Classification Guides)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

For information on e-mail or electronic submission, contact TR@dtic.mil.

d. Provide one copy of each approved guide to the activity security manager.

e. Provide one copy to the DoD Component declassification program manager.

7. INDEX OF SECURITY CLASSIFICATION GUIDES. Security classification guidance (e.g., security classification guides, memorandums, directives, regulations) issued in accordance with this enclosure shall be indexed in an on-line accessible database maintained by DTIC. Originators of guides shall submit DD Form 2024 to the Administrator, DTIC, upon approval of the guide, with each update, revision, or review, or whenever the guide is cancelled or superseded. If the originator determines that listing the guide in the DTIC-maintained database is inadvisable for security reasons (e.g., involves SAPs), the originator shall separately report issuing the guide to the Director of Security, OUSD(I), and explain why the guide should not be listed.

8. REVIEW OF SECURITY CLASSIFICATION GUIDES. Each security classification guide shall be reviewed by the issuing OCA at least once every 5 years to ensure it is current and accurate. When necessitated by significant changes in Executive orders or by changes in operations, plans, or programs, reviews will be conducted sooner. The OCA shall make changes identified as necessary in the review process. If no changes are required, the OCA shall submit to DTIC a new DD Form 2024 with the date of the next required review and annotate the record copy of the guide with this fact and the date of the review.

9. REVISION OF SECURITY CLASSIFICATION GUIDES. Guides shall be revised whenever necessary to promote effective derivative classification. Revised guides shall be reported as required in section 7 of this enclosure.

10. CANCELLING SECURITY CLASSIFICATION GUIDES

a. Guides shall be canceled only when:

(1) All information the guide specifies as classified has been declassified; or

(2) A new security classification guide incorporates the classified information covered by the old guide and there is no reasonable likelihood that any information not incorporated by the new guide shall be the subject of derivative classification. The impact on systems, plans, programs, or projects must be considered when deciding to cancel a guide.

b. Upon canceling a guide, the responsible official shall consider the need for publishing a declassification guide, according to section 4 of Enclosure 5.

c. The OCA, or successor organization, shall maintain a record copy of any canceled guide as required by Reference (at).

11. REPORTING CHANGES TO SECURITY CLASSIFICATION GUIDES. Revision, reissuance, review, supersession, and cancellation of a guide shall be reported to DTIC using DD Form 2024, according to section 7 of this enclosure. Copies of changes, reissued guides, and cancellation notices will be distributed according to section 6 of this enclosure.

12. FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEWS. As periodically directed by the USD(I), but at least every 5 years, the DoD Component Heads shall accomplish comprehensive reviews of classification guidance issued by the DoD Component.

a. Reviews shall ensure the DoD Component's classification guidance reflects current conditions. The reviews shall also identify classified information that no longer requires protection and can be declassified.

b. Reviews shall focus on a review of security classification guides, but should consider all forms of classification guidance issued (e.g., memorandums, DoD Component regulation or directive).

c. Reviews shall include an evaluation of classified information to determine if it continues to meet the standards for classification specified in section 1 of Enclosure 4 of this Volume, using a current assessment of likely damage.

d. OCAs, DoD Component subject matter experts, and users of the classification guidance shall be consulted to provide a broad range of perspectives. Contributions of subject matter experts with sufficient expertise in narrow specializations must be balanced by the participation of managers and planners who have broader organizational vision and relationships. Additionally, to the extent practicable, input should also be obtained from external subject matter experts and external users of the classification guidance.

e. Detailed reports summarizing results and findings shall be prepared and submitted in accordance with the direction provided and shall be unclassified and releasable to the public, except when the existence of the guide or program is itself classified. OUSD(I) shall provide a composite DoD report to ISOO and release an unclassified version to the public.