CHAPTER 4

DECLASSIFICATION AND REGRADING

Section 1

General

4-100 **Policy**

E.O. 12958 provides that "information shall be declassified as soon as it no longer meets the standards for classification" established by the Order. It further states that, "in some exceptional cases, ...the need to protect... information [still meeting these standards] may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified." It is DoD policy that information shall remain classified as long as a. it is in the best interest of the national security to keep it protected, and b. continued classification is in accordance with the requirements of the E.O. If DoD officials have reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they shall refer the matter to the appropriate Senior Agency Official appointed in accordance with Section 5.6(c) of E.O. 12958.

4-101 Declassification Systems

E. O. 12958 established four separate and parallel systems that can bring about the declassification of information: (a) a system requiring the original classifier to decide at the time information is classified when it can be declassified, (b) a system that will cause information of permanent historical value to be automatically declassified on the 25th anniversary of its classification unless specific action is taken to keep it classified, (c) a system for reviewing information for possible declassification upon request, and (d) a process for systematic review of information for possible declassification. The Heads of the DoD Components are responsible for ensuring the establishment and maintenance of declassification programs and/or plans to meet the requirements of this subsection.

4-102 Declassification Authority

a. Information may be declassified and downgraded by the Secretary of Defense, the Secretaries of the Military Departments, those officials who have been delegated Original Classification Authority in accordance with subsection 2-201 of this Regulation, above, and officials who have been delegated declassification authority in accordance with subsection 4-102b, below. The authority to declassify information extends only to information for which the specific official has classification, program, or functional responsibility.

b. DoD Component heads may designate officials within their organizations to exercise declassification authority over specific types or categories of information. Categories of information may be as broad as all information originally classified by officials of the DoD Component. Classification authorities may designate members of their staffs to exercise declassification authority over information under their jurisdiction.

c. Persons with declassification authority shall develop and issue declassification instructions to facilitate effective review and declassification of information classified under predecessor Executive Orders. These instructions may be in the form of separate guides, sections of classification guides, memoranda, etc.

d. Declassification authority is not required for simply canceling or changing classification markings in accordance with instructions placed on a document, directions found in a security classification guide or declassification guide, or instructions received from a declassification authority.

e. Special procedures for use in systematic and mandatory review of cryptologic information are at Appendix D.

4-103 **Exceptions**

None of the provisions of this chapter apply to information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data and Formerly Restricted Data).

Section 2

Declassification Decisions by Original Classifiers

4-24)0 **Requirement**

Every time a designated original classification authority (OCA) classifies information, he or she must make a determination about the duration for which the classification will continue. This is an essential part of the original classification process.

4-201 The **"Ten-Year Rule"**

At the time they classify an item of information, original classifiers shall:

a. Attempt to determine a date within ten years from the date of classification upon which the information can be automatically declassified. If that is not possible, they shall:

b. Attempt to determine a specific event, reasonably expected to occur within 10 years, that can be set as the signal for automatic declassification of the information. If that is not possible, they shall:

c. Designate the information as being automatically declassified on a date ten years from the date of its original classification, unless the provisions of subsection 4-202, below, apply.

4-202 **Exemption from the 10-Year Rule**

If an original classifier has substantial reason to believe that information being originally classified will require protection for longer than ten years, he or she may exempt the information from the ten-year maximum duration of classification. This may be done if:

a. The unauthorized disclosure of the information could reasonably be expected to cause damage to the national security for a period in excess of 10 years, and

b. The release of the information could reasonably be expected to:

(1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) Reveal information that would assist in the development or use of weapons of mass destruction;

(3) Reveal information that would impair the development or use of technology within a United States weapon system;

(4) Reveal United States military plans, or national security emergency preparedness plans;

(5) Reveal foreign government information;

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years;

(7) Impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized;

(8) Violate a statute, treaty, or international agreement.

4-203 **Extension of Ten-Year Declassification Periods.**

If information has been assigned a date or event for declassification under the ten-year rule described in subsection 4-201, above, and the original classification authority with jurisdiction over the information has reason to believe longer protection is required, he or she may extend the classification for successive periods not to exceed 10 years consistent with agency records retention schedules. Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who decide to extend a 10-year declassification date are responsible for notifying holders of the information of the decision.

a. For information in records determined to have permanent historical value, successive extensions may not exceed 25 years from the date of the information's origin unless approved as an exception (see section 3 of this chapter).

b. Information in records not determined to have permanent historical value, may be extended past 25 years. However, provisions of normal records retention and destruction requirements must be adhered to. Consult your agency's published retention schedule.

Section 3

Automatic Declassification System At 25 Years

4-300 The **Automatic Declassification System**

a. Executive Order 12958 established a system for declassification of information in permanently valuable historical records (as defined by Title 44, U.S. Code) 25 years from the date of original classification. This system shall be applied to existing records over a five-year period beginning with the effective date of the Order (14 October 1995), and shall apply after that to all permanently valuable historical records as they become 25 years old. Only the Secretary of Defense and the Secretaries of the Military Departments may exempt information from this automatic declassification under certain circumstances. Information exempted from automatic declassification at 25 years remains subject to the mandatory and systematic declassification review provisions of this Regulation.

b. In accordance with the Executive Order, the Secretary of Defense and the Secretaries of the Military Departments have identified specific file series that are exempt from the 25-year automatic declassification, and have notified the President of these exemptions. Information in these file series shall not be subject to this automatic declassification system unless an Agency head specifically decides to remove the series from the exempted category. Information not contained within these file series shall be automatically declassified at 25 years unless specific information is exempted by an Agency head in accordance with subsection 4-301, below.

c. By 17 April 2000, the Heads of DoD Components shall ensure the declassification of information which: (1) is contained in records which have permanent historical value under Title 44 of the U.S. Code, (2) has not been exempted from automatic declassification at 25 years, and (3) will reach the 25th anniversary of its classification by that date. Declassification operations will be in accordance with plans submitted to the Director of the Information Security Oversight Office in compliance with Subsection 3.4(e) of E.O. 12958.

d. Information contained in records not determined to be permanently valuable and not scheduled for disposal or retention by the National Archives is not subject to automatic declassification. Agency retention and destruction requirements apply.

4-301 Exemption of Specific Information

a. Within the Department of Defense, classified information not contained in file series exempted from the automatic declassification system may be exempted from declassification only by the Secretary of Defense or Secretary of a Military Department. Such exemptions shall be applicable only to specific information. Information may be exempted only if its release would be expected to:

(1) Reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) Reveal information that would assist in the development or use of weapons of mass destruction;

(3) Reveal information that would impair U.S. cryptologic systems or activities;

(4) Reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) Reveal actual U.S. military war plans that remain in effect;

(6) Reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) Violate a statute, treaty, or international agreement.

b. The Secretary of Defense, the Secretary of a Military Department, or their designated Senior Agency Official, must notify the Director, Information Security

Oversight Office (1S00) of their intent to exempt information from automatic declassification. Information previously exempt in accordance with paragraph 4-300b, above, is excluded. Notification must be received by 1S00, acting as the executive secretary of the Interagency Security Classification Appeals Panel (ISCAP), 180 days before the information is scheduled for automatic declassification. The notice shall:

(1) Describe the specific information to be exempted;

(2) Explain why the information must remain classified; and

(3) Provide a specific date or event upon which the information will be declassified. (This requirement is not applicable to information exempt from search and review under the Central Intelligence Agency Information Act).

Section 4

Mandatory Review for Declassification

4-400 **General**

a. Any individual or organization may request a review for declassification of information classified under E.O. 12958 or predecessor orders. Upon receipt of such a request, the responsible DoD organization shall conduct a review if:

(1) The request describes the document or material with enough specificity to allow it to be located with a reasonable amount of effort;

(2) The information is not exempt from search and review under the Central Intelligence Agency Information Act; and

(3) The information has not been reviewed for declassification within the preceding two years.

b. Information originated by the incumbent President; the incumbent President's White House Staff; committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempt from the provisions of this section.

4-401 **Responsibilities** and Procedures

a. Heads of the DoD Components shall establish systems for promptly responding to requests for mandatory declassification review. Information reviewed shall be declassified if it no longer meets the standards for classification established by this Regulation. Information that is declassified shall be released to the requester unless withholding is appropriate under applicable law (for example, the Freedom of Information Act or the Privacy Act of 1974).

b. If documents or material being reviewed for declassification under this Section contain information that has been originally classified by another DoD Component or Government Agency, the reviewing activity shall refer the appropriate portions of the request to the originating organization. Unless the association of that organization with the requested information is itself classified, the DoD Component that received the request may notify the requester of the referral.

c. A DoD Component may refuse to confirm or deny the existence or non-existence of requested information when the fact of its existence or non-existence is properly classified.

d. If the requested information has been reviewed for declassification within the two years preceding the request, the DoD Component will so notify the requester. No further review is required.

e. The mandatory declassification review system shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal the denial of declassification. If the requester subsequently files an appeal and the appeal is denied, the requester must be notified of the right to appeal the denial to the Interagency Security Classification Appeals Panel.

f. Special procedures for use in mandatory review of cryptologic information are at Appendix D.

Section 5

Systematic Review for Declassification

4-500 General

a. Heads of the DoD Components that have classified information under E.O. 12958 or predecessor Orders shall, as permitted by available resources, establish systematic review programs to review for declassification information in the custody of the Component that: (1) is contained in permanently valuable historical records, and (2) is exempt from automatic declassification under Section 3 of this chapter. These efforts will concentrate on records that:

(a) Contain information which has been identified by the Information Security Policy Advisory Council established under E.O. 12958 or similar groups to have significant value for historical or scientific research or for promoting the public welfare, and

(b) Have a reasonable likelihood of being declassified upon review.

b. Special procedures for use in systematic review of cryptologic information are at Appendix D.

Section 6

Downgrading

4-600 **Purpose and Authority**

Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Information may be downgraded by any official who is authorized to classify or declassify the information. (See subsection 4-102, above.)

4-601 Downgrading Decisions During Original Classification

Downgrading should be considered when original classifiers are deciding on the duration of classification to be assigned. If downgrading dates or events can be identified, they must be specified along with the declassification instruction. Note that downgrading instructions DO NOT replace declassification instructions.

4-602 Downgrading at a Later **Date**

Information may be downgraded by any official who is authorized to classify or declassify the information. (See subsection 4-102, above.) The authorized official making the downgrading decision shall notify holders of the change in classification.

Section 7

Upgrading

4-700 Upgrading

Classified information may be upgraded to a higher level of classification only by officials who have been delegated the appropriate level of Original Classification Authority in accordance with Section 2, Chapter 2 of this Regulation. Information maybe upgraded only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The Original Classification Authority making the upgrading decision is responsible for notifying holders of the change in classification.

Section 8

Foreign Government Information

4-800 Policy and Procedures

Within the Department of Defense, every effort must be made to ensure that foreign government information is not subject to downgrading or declassification without the prior consent of the originating government. Foreign government information may exist in two forms:

a. Foreign government information may take the form of foreign documents in the possession of the Department of Defense. If these documents constitute permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification rule, declassification officials shall consult with the originating foreign government to determine whether it consents to declassification. If the originating foreign government does not consent, the records shall be processed for exemption from automatic declassification in accordance with subsection 4-301, above. The agency head shall determine whether exemption categories 6, 9, or both should be applied.

b. Foreign government classified information may also be included within a DoD document. Such documents shall be marked with declassification instructions consistent with subparagraph 5-204c(2) of this Regulation, below. If these documents are permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification **rule, the provisions of paragraph 4-800a., above, apply.**

4-801 Communications with Foreign Governments

DoD officials may consult directly with foreign governments regarding downgrading or declassification of foreign government information or seek assistance from the Department of State. In either case, DoD officials should first consult with the Office of the Deputy to the Under Secretary of Defense (Policy Support) for assistance and guidance.

Section 9

Challenges to Classification

4-900 Classification Challenges

a. 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 classifier of the information to bring about any necessary correction. This may be done informally or by submission of a formal challenge to the classification as provided for in E.O. 12958. Informal questioning of classification is encouraged before resorting to formal challenge. Heads of the DoD Components shall establish procedures through which authorized holders of classified information within their organizations may challenge classification decisions, and shall ensure that members of their organization are made aware of the established procedures.

(1) Formal 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 made by DoD personnel should also include the reason why the challenger believes that the information is improperly or unnecessarily classified. The challenge should be unclassified, if possible.

(2) Heads of Components shall ensure that no retribution is taken against any employee for making a challenge to a classification.

b. Heads of DoD Components shall establish procedures for handling challenges to classification received from within and from outside their Components. These procedures shall conform to the following guidelines:

(1) A system shall be established for processing, tracking, and recording formal challenges to classification.

(2) The Component shall provide a written response to the challenge within 60 days. If the Component cannot respond fully to the challenge within 60 days, the challenge must be acknowledged and an expected date of response provided. This acknowledgment must include a statement that, if no response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if

an agency has not responded to an internal appeal within 90 days of receipt.

(3) If the challenge is denied, the Component shall advise the submitter of his or her right to appeal the decision to the Interagency Security Classification Appeals Panel.

(4) If a challenge is received concerning information that has been the subject of a challenge within the preceding two years, or which is the subject of pending litigation, the Component need not process the challenge. The challenger shall be informed of the situation and appropriate appellate procedures.

c. Information that is the subject of a classification challenge shall continue to be classified and appropriately safeguarded unless and until a decision is made to declassify it.