CHAPTER 9

SECURITY EDUCATION AND TRAINING

Section 1

Policy

9-100 General Policy

Heads of DoD Components shall ensure that personnel of their organization receive such security education and training as may be required to:

a. Provide necessary knowledge and information to enable quality performance of security functions;

b. Promote understanding of Information Security Program policies and requirements and their importance to the national security;

c. Instill and maintain continuing awareness of security requirements and the intelligence threat; and

d. Assist in promoting a high degree of motivation to support program goals.

9-101 Methodology

Security education and training may be accomplished through establishment of programs within the Component, use of external resources such as the Department of Defense Security Institute, or a combination of the two.

Section 2

Initial Orientation

9-200 **Cleared Personnel**

a. All personnel in the organization who are cleared for access to classified information shall be provided an initial orientation to the Information Security Program before being allowed access to classified information. This initial orientation is intended to produce a basic understanding of the nature of classified information and the importance of its protection to the national security, place employees on notice of their responsibility to play a role in the security program, and provide them enough information to ensure proper protection of classified information in their possession. Security educators should consider including:

(1) Roles and Responsibilities

(a) Who are the senior agency official and agency security personnel and what are their responsibilities?

(b) What are the responsibilities of agency employees who create or handle classified information?

(c) Who should be contacted in case of questions or concerns about security matters?

(2) Elements of Classifying and Declassifying Information

(a) What is classified information and why is it important to protect it.?

(b) What are the levels of classified information and the damage criteria associated with each level?

(c) What classification markings are to be used and why is it important that they be properly applied?

(d) What are the general requirements for declassifying information?

(e) What are the procedures for challenging the classification status of information?

(3) Elements of Safeguarding

(a) What are the proper procedures for safeguarding classified information?

(b) What constitutes a compromise of classified information and what are the penalties associated with compromises?

(c) What are the general conditions and restrictions for access to classified information?

(d) What should an individual do when he or she believes safeguarding standards have been violated?

(e) What steps should be taken in an emergency evacuation situation?

(f) What are the appropriate policies and procedures for transmission of classified information?

b. Before being granted access to classified information, employees must sign Standard Form 312, "Classified Information Nondisclosure Agreement." Cleared personnel who have signed an earlier nondisclosure agreement, the SF 189, need not sign SF 312, but they may elect to replace their SF 189 with a signed SF 312. SFS 189 and 312 shall be maintained for 50 years from the date of signature.

9-201 Uncleared Personnel

Members of the organization who are not cleared for access to classified information should be included in the security education program if they will be working in situations where inadvertent access to classified information might occur or will have access to unclassified information that might be of value to intelligence collectors. They should be provided with a brief explanation of the nature and importance of classified information and actions they should take if they discover classified information unsecured, note an apparent security vulnerability, or believe they are contacted by an intelligence collector.

Section 3

Special Requirements

9-300 **General**

Members of the organization in positions that require performance of specified roles in the Information Security Program shall be provided security education and training sufficient to permit quality performance of those duties. The education and training shall be provided before, concurrent with, or not later than six months following assumption of those positions.

9-301 **Original Classifiers**

The security education and training provided to original classification authorities shall, as a minimum, address each of the following:

a. What is the difference between original and derivative classification?

b. Who can classify information originally?

c. What are the standards that an original classifier must meet to classify information?

d. What is the process for determining duration of classification?

e. What are the prohibitions and limitations on classifying information?

f. What are the basic markings that must appear on classified information?

g. What are the general standards and procedures for declassification?

h. What are the requirements and standard for creating, maintaining and publishing security classification guides?

9-302 **Declassification Authorities Other Than Original Classifiers**

The security education and training provided declassification authorities other than original classifiers shall, as a minimum, address each of the following:

a. What are the standards, methods and procedures for declassifying information under Executive Order 12958 and this Regulation?

b. What are the standards for creating and using declassification guides?

c. What is contained in the Component's declassification plan?

d. What are the Component's responsibilities for the establishment and maintenance of a declassification database?

9-303 **Derivative Classifiers, Security Personnel and Others**

Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information shall receive training that, as a minimum, addresses the following:

a. What are the original and derivative classification processes and the standards applicable to each?

b. What are the proper and complete classification markings to be applied to classified information?

c. What are the authorities, methods and processes for downgrading and declassifying information?

d. What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

e. What are the requirements for creating and updating classification and declassification guides?

f. What are the requirements for controlling access to classified information?

g. What are the procedures for investigating and reporting instances of actual or potential compromise of classified information and the penalties that may be associated with violation of established security policies and procedures?

h. What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

i. What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

j. What are the requirements for oversight of the security classification program, including self-inspections?

9-304 **Others**

Additional security education and training may be required for personnel who::

a. Use automated information systems to store, process, or transmit classified information;

b. Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely;

c. Will be escorting, handcarrying, or serving as a courier for classified material;

d. Are authorized access to classified information requiring special control or safeguarding measures; or

e. Are involved with international programs; or

f. Are involved with acquisition programs subject to DoD Directive 5000.1

Section 4

Continuing Security Education/Refresher Training

9-400 **Continuing Security Education**

Security education should be a continuous, rather than a periodic influence on individual security performance. Periodic briefings, training sessions, and other formal presentations should be supplemented with other information and promotional efforts to ensure maintenance of continuous awareness and performance quality. The use of job performance aids and other substitutes for formal training is encouraged when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a "read-and initial" basis shall not be considered as a sole means of fulfilling any of the specific requirements of this Chapter.

9-401 Refresher Training

As a minimum, personnel shall receive annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or

concerns identified during Component self-inspections

Section 5

Termination Briefings

9-500 General

The DoD Components shall establish procedures to ensure that cleared employees who leave the organization or whose clearance is terminated receive a termination briefing. This briefing shall emphasize their continued responsibility to:

a. Protect **classified** information to which they have had access;

b. Provide instructions for reporting any unauthorized attempt to gain access to such information;

c. Advise the individuals of the prohibition against retaining material when leaving the organization; and

d. Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

Section 6

Program Oversight

9-600 **General**

Heads of the DoD Components shall ensure that security education programs are appropriately evaluated during self-inspections and other oversight activities. This evaluation shall include assessment of the quality and effectiveness of security education efforts, as well as ensuring appropriate coverage of the target populations. Heads of the Components shall require maintenance of whatever records of programs offered and employee participation they deem necessary to permit effective oversight.