ENCLOSURE 5

SECURITY EDUCATION AND TRAINING

1. REQUIREMENT. The Heads of the DoD Components shall ensure that their personnel receive security education and training that:

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

b. Promotes understanding of DoD Information Security Program policies and requirements and their importance to national security and national interests.

c. Instills and maintains continuing awareness of security requirements.

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

2. SECURITY EDUCATION AND TRAINING RESOURCES

a. Security education and training may be accomplished by establishing programs within the DoD Component, using external resources such as the Defense Security Service Academy, or a combination of the two.

b. DoD Components may, if desired, combine into one overall program the education and training requirements of this enclosure and those for CUI specified in Volume 4 of this Manual.

3. INITIAL ORIENTATION. All personnel in the organization, including DoD civilians, military members, and on-site support contractors shall receive an initial orientation to the DoD Information Security Program.

a. This initial orientation is intended to:

(1) Define classified information and CUI and explain the importance of protecting such information.

(2) Produce a basic understanding of security policies and principles.

(3) Notify personnel of their responsibilities within the security program, and inform them of the administrative, civil, and/or criminal sanctions that can be applied when appropriate.

(4) Provide individuals enough information to ensure the proper protection of classified information and CUI in their possession, including actions to be taken if such information is discovered unsecured, a security vulnerability is noted, or a person has been seeking

unauthorized access to such information.

(5) Inform personnel of the need for review of ALL unclassified DoD information prior to its release to the public.

b. Security educators shall also consider including in the initial orientation identification of the DoD Component senior agency official and activity security management personnel, a description of their responsibilities, and whether they are involved in the protection of classified or controlled unclassified information. If not included in the initial orientation, such information must be included in the training required by paragraph 3.c. of this section.

c. In addition to the requirements in paragraphs 3.a. and 3.b. of this section, upon initial access to classified information, all personnel shall receive training on security policies and principles and derivative classification practices, including:

(1) The definition of classified information, the levels of classified information, and the damage criteria associated with each level.

(2) The responsibilities of DoD personnel who create or handle classified information, including:

(a) The requirements for controlling access to classified information, including:

1. The general conditions for and restrictions on access to classified information.

2. The steps an individual shall take when he or she is asked to verify classified information disclosed through unofficial open sources (e.g., news media, periodicals, and public websites).

(b) The policies and procedures for safeguarding classified information, including:

1. The proper methods and procedures for using, storing, reproducing, transmitting, disseminating, and destroying classified information.

2. The steps an individual shall take to safeguard classified information during an emergency evacuation situation.

3. The steps an individual shall take when he or she believes classified information has not been, or is not being, properly protected.

(c) The accountability of derivative classifiers for the accuracy of their work.

(3) An explanation that derivative classification is extracting, paraphrasing, or restating classified information based on a security classification guide, one or more source documents, or both.

(4) The authorized types of sources that can be used for derivative classification and where to obtain them, including:

(a) An explanation that a security classification guide:

1. Is precise, comprehensive guidance regarding specific program, system, operation or weapon system elements of information to be classified, including classification levels, reasons for classification, and the duration of classification.

2. Is approved and signed by the cognizant OCA.

3. Is an authoritative source for derivative classification.

4. Ensures consistent application of classification to the same information.

(b) How to use a security classification guide or other derivative source.

(c) How and where to obtain classification guidance currently available for a specific area of expertise, including:

1. The security manager and/or the program or project office.

2. The Defense Technical Information Center, at www.dtic.mil (registration required).

3. In the case of a military operation and the creation or execution of plans and orders thereto, the higher headquarters office that mandated or directed the operation or mission.

(5) The proper and complete classification markings to be used for classified information, and how those markings are to be applied, including:

(a) The importance of properly applying the authorized classification markings and the need to avoid over-classification.

(b) How to document the level of classification, duration of classification and the source(s) of classified information included in the material (e.g., document, e-mail, briefing, video) being created or generated.

(c) How to observe and respect the original classification decision(s).

(d) How to maintain lists of sources when multiple sources of classification are used.

(e) How to determine the duration of classification.

(f) How to properly use control markings to limit or expand distribution, including foreign disclosure and release markings (e.g., “REL TO” (releasable to), “NOFORN” (not

releasable to foreign nationals) and DISPLAY ONLY).

(g) How to challenge classification decisions.

(h) How to downgrade or declassify information as an authorized holder of information in accordance with the direction of the cognizant OCA or classification guide.

(i) How to mark and share "working papers" and other drafts, including the requirements for such markings.

(6) The definition of a security incident, a violation and a compromise of classified information, examples of each, and an explanation of the criminal, civil, and administrative sanctions that may be taken against an individual who fails to comply with program requirements or to protect classified information from unauthorized disclosure.

(7) The policies and procedures for sharing classified information with state, local, tribal, and private sector officials and with foreign governments and international organizations, including the markings that designate information as qualifying for sharing, if appropriate for the activity's mission or function.

(8) The policies and procedures for the marking, safeguarding, and accounting of NATO classified information.

d. In addition to the training specified by paragraphs 3.a through 3.c of this section and information assurance (IA) training required by DoDD 8570.01 (Reference (bh)), personnel who are authorized access to classified information systems shall receive training which specifically addresses:

(1) Proper use of information systems for creating, using, storing, processing, or transmitting classified information.

(2) The requirement for and application of markings, including portion markings, to information in electronic formats (e.g., documents, e-mail, briefings, web-based information, databases, spreadsheets).

(3) Marking, handling, storage, transportation, and destruction of classified computer media (e.g., floppy disks, CDs, DVDs, removable hard drives).

(4) Procedures to be followed when using classified removable data storage media.

(5) Procedures to be followed if an individual believes an unauthorized disclosure of classified data has occurred on an information system or network (typically called a "data spill").

4. SPECIAL TRAINING REQUIREMENTS

a. Individuals with specified duties in the Information Security Program, as identified in sections 5, 6, and 10 of this enclosure, shall be provided security education and training commensurate with job responsibilities and sufficient to permit effective performance of those duties. The education and training may be provided before, concurrent with, or not later than 6 months following assuming those duties, unless otherwise specified.

b. Deployable organizations shall provide, prior to deployment, enhanced security training to meet the needs of the operational environment. Where appropriate, this pre-deployment training shall specifically address security requirements associated with information sharing (e.g., release of information to state, local, tribal, or coalition partners; use and handling of FGI) and shall provide training on the classification markings that are to be applied in these situations and that designate information as qualifying for sharing.

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

(1) Travel to foreign countries where special concerns about possible exploitation exist or attend professional meetings or conferences where foreign attendance is likely.

(2) Escort, hand-carry, or serve as a courier for classified material.

(3) Are authorized access to classified information requiring special control or safeguarding measures.

(4) Are involved with international programs.

(5) Are involved with acquisition programs subject to Reference (af).

(6) Are involved with FGI, or work in coalition or bilateral environments, or in offices, activities, or organizations hosting foreign exchange officers.

(7) Submit information to OCAs for original classification decisions and therefore need additional knowledge of the original classification decision process.

5. OCA TRAINING. Training for newly appointed OCAs shall be provided prior to exercise of the authority and each OCA shall receive training annually thereafter as required in paragraph 7.b. of this enclosure. The OCA shall certify in writing that the training has been received. Personnel preparing recommendations for original classification to OCAs will receive the same training. The training shall address OCA responsibilities and classification principles, proper safeguarding of classified information, and the criminal, civil, and administrative sanctions that may be brought against an individual. At a minimum, the training shall address:

a. General requirements, including:

(1) The difference between original and derivative classification.

(2) Persons who can classify information originally.

(a) OCA is assigned to a position, not a person and, except as authorized by Enclosure 4 of Volume 1 of this Manual, may not be further delegated.

(b) Only individuals carrying out a unique mission with responsibility in one of the subject areas prescribed by section 1.4 of Reference (d) may be designated an OCA.

(c) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to exercise OCA when they have been officially designated to assume the duty position of the OCA in an acting capacity during the OCA's absence and have certified in writing that they have received required OCA training.

(3) The requirement to certify, in writing, before initially exercising OCA authority and annually thereafter, that training has been received.

(4) The prohibitions and limitations on classifying information, as stated in sections 1 and 2 of Enclosure 4 of Volume 1 of this Manual, and the need to avoid over classification.

b. The responsibility and discretion the OCA has in classifying information.

(1) OCAs must be aware that their decisions to classify information have a substantial impact on the operations of the Department and on national security. Others who work with the information use these original decisions to make proper derivative classification decisions and to assure that the information is properly protected from unauthorized disclosure.

(2) OCAs are accountable to the Secretary of Defense for their classification decisions.

(3) OCAs shall exercise a substantial degree of autonomy in operations or mission. Information warranting original classification must be developed in the normal course of actions or activity.

c. The classification principles and process specified in section 6, Enclosure 4 of Volume 1 of this Manual.

(1) Original classification requires identification of specific elements of information which could adversely affect the national security if compromised. In addition to consideration of harm to the national security, OCAs must weigh the advantages and disadvantages of classifying each element and should consider, when applicable:

(a) Degree of intended or anticipated dissemination or use.

(b) Net national advantage.

(c) Lead time advantage for operational or technological use.

(d) Cost in terms of time, money, and personnel.

(e) Impact on attaining the program objective.

(f) State of the art and public knowledge of the U.S. interest.

(g) Appearance in the public domain, inadvertent disclosure or other compromise.

(h) Basic scientific research data or unusually significant scientific findings.

(i) Association or compilation of information or data.

(2) Information is classified either because its unauthorized disclosure could reasonably be expected to cause identifiable or discernable damage to national security or because it may reveal such information when associated with other information. If information is classified in compilation with other information, a clear explanation of rationale must be provided (see section 12 of Enclosure 3 of Volume 2).

(3) OCAs shall ensure that a review for possible declassification is conducted expeditiously in the event of compromise, that damage assessments are conducted as necessary, and that formal challenges to classification, classification conflicts, and requests for classification determinations from individuals who are not OCAs are addressed as required by this Manual.

d. The procedures that must be followed when making and communicating original classification decisions.

(1) The required markings that must appear on classified information as specified in Volume 2, Enclosure 3 of this Manual.

(2) The process for determining duration of classification.

(a) Information shall be assigned a date or event for declassification that is 25 years or less from the date of origination, except for information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.

(b) Information in records with permanent historic value may be classified for longer than 25 years only if the Interagency Security Classification Appeals Panel (ISCAP) has been notified of such a date in accordance with the procedures in section 13, Enclosure 5 of Volume 1 of this Manual. The ISCAP decisions will be codified in a classification or declassification guide.

(3) The general standards and procedures for changes in classification (downgrade, upgrade, declassify) and the general requirements for automatic and systematic declassification and mandatory reviews for declassification.

(a) An OCA should organize the classification process around time and event-phased downgrading and declassification events to the maximum extent possible.

(b) An OCA may change the level of classification of information under their jurisdiction (downgrade, upgrade, declassify) as specified in section 7, Enclosure 4 of Volume 1 of this Manual.

(c) Classification may change at each phase of an operation, research and development cycle, or acquisition, as determined by the OCA with responsibility over the information.

(4) The requirements and standards for creating, issuing, and maintaining security classification guidance, including classification and declassification guides, as identified in section 8, Enclosure 4 of Volume 1 of this Manual.

e. The proper safeguarding protections to apply when using, storing, reproducing, transmitting, disseminating, and destroying classified information.

f. The criminal, civil, and administrative sanctions that may be brought against an individual who fails to classify information properly or to protect classified information from unauthorized disclosure.

6. DECLASSIFICATION AUTHORITY TRAINING. The security education and training provided declassification authorities other than original classifiers shall, at a minimum, address:

a. The standards, methods, and procedures for declassifying information pursuant to References (d) and (f) and this Manual.

b. The standards for creating, maintaining, and using declassification guides.

c. The information contained in the DoD Component's declassification plan.

d. The DoD Component's responsibilities for establishing and maintaining a declassification database.

e. The referral process and requirements.

7. ANNUAL REFRESHER TRAINING

a. At a minimum, all DoD civilians, military members, and on-site support contractors with access to classified information shall receive annual refresher training that reinforces the policies, principle, and procedures covered in their initial and specialized training. Refresher training shall also address the threat and the techniques foreign intelligence activities use while

attempting to obtain classified DoD information, and advise personnel of penalties for engaging in espionage activities and other unauthorized disclosures. Refresher training shall also address relevant changes in information security policy or procedures and issues or concerns identified during DoD Component self-inspections. Information system users shall additionally complete an annual IA awareness refresher, as required by Reference (bh).

b. Each OCA shall receive annual training as specified in section 5 of this enclosure. The OCA shall certify receipt of the training in writing. OCAs who do not receive the specified training at least once within a calendar year shall have their classification authority suspended by the DoD Component Head or the senior agency official who delegated the authority until the training has taken place, unless a waiver is granted in accordance with paragraph 7.f of this section.

c. Derivative classifiers (i.e., those who create new documents, including e-mails, based on existing classification guidance) shall receive training in derivative classification as required by paragraph 3.c. of this enclosure, with an emphasis on avoiding over-classification, at least once every 2 years. Training may, at the DoD Component's discretion, be included in the training required by paragraph 7.a. of this section. Derivative classifiers who do not receive training at least once every 2 years shall not be authorized or allowed to derivatively classify information until they have received training, unless a waiver is granted in accordance with paragraph 7.f of this section.

d. Declassification authorities shall receive training as required by section 6 of this enclosure at least once every 2 years.

e. DoD Components shall track training required by paragraphs 7.b and 7.c of this section and take appropriate action to suspend OCA authority in accordance with paragraph 7.b or disallow derivative classification in accordance with paragraph 7.c if the training is not accomplished as required.

f. A waiver to the training requirement in paragraphs 7.b or 7.c of this section may be granted by the DoD Component Head, the Deputy Component Head, or senior agency official if an individual is unable to receive required training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive the required training as soon as practicable.

8. CONTINUING SECURITY EDUCATION AND TRAINING. Security education and training shall be continuous, rather than aperiodic. Periodic briefings, training sessions, and other formal presentations shall be supplemented with other information and promotional efforts to ensure that continuous awareness and performance quality is maintained. 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 the sole means of fulfilling any of the specific requirements of this enclosure.

9. TERMINATION BRIEFINGS. The DoD Components shall establish procedures to ensure that cleared employees who leave the organization or whose clearance is terminated receive a termination briefing in accordance with paragraph C9.2.5 of Reference (l). The briefing shall:

a. Emphasize their continued responsibility to protect classified and controlled unclassified 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 prohibitions against retaining classified and controlled unclassified material when leaving the organization.

d. Identify the requirement that retired personnel, former DoD employees, and non-active duty members of the Reserve Components must submit writings and other materials intended for public release to the DoD security review process as specified by Reference (k).

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

10. MANAGEMENT AND OVERSIGHT TRAINING. Individuals designated as security managers, classification management officers, security specialists, or any other personnel whose duties significantly involve managing and overseeing classified information shall receive training that meets the requirements of DoDI 3305.13 (Reference (bi)) and addresses:

a. The original and derivative classification processes and the standards applicable to each.

b. The proper and complete classification markings to be applied to classified information,

c. The proper use of control markings to limit or expand distribution, including foreign disclosure and release markings (e.g., REL TO, NOFORN, and DISPLAY ONLY).

d. The authorities, methods, and processes for downgrading and declassifying information.

e. The methods for properly using, storing, reproducing, transmitting, disseminating, and destroying classified information.

f. The requirements for creating, maintaining, and issuing classification and declassification guides.

g. The requirements for controlling access to classified information.

h. The procedures for investigating and reporting instances of actual or potential compromise of classified information, including when in electronic form, and the penalties that may be associated with violating established security policies and procedures.

i. The requirements for creating, maintaining, and terminating SAPs, and the mechanisms for monitoring such programs.

j. The procedures for the secure use of information systems and networks that use, process, store, reproduce, or transmit classified information, and requirements for their certification and accreditation.

k. The provisions for automatic declassification and the need for systematic and mandatory reviews for declassification, and the DoD Component procedures for accomplishing each.

l. The requirements for overseeing the Information Security Program, including self-inspections.

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