

CHAPTER 4

SECURITY EDUCATION

4-1 BASIC POLICY

1. Each command handling classified information will establish and maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures.

2. The purpose of the security education program is to ensure that all personnel understand the need and procedures for protecting classified information. The goal is to develop fundamental security habits as a natural element of each task.

4-2 RESPONSIBILITY

1. CNO (N09N) is responsible for policy guidance, education requirements and support for the DON security education program. Development of security education materials for use throughout the DON must be coordinated with CNO (N09N2) for consistency with current policies and procedures. This requirement does not apply to materials that are prepared for use in command programs.

2. Recruit training commands are responsible for indoctrinating military personnel entering the Navy and Marine Corps, with a basic understanding of what "classified information" is and why and how it is protected. Civilians being employed by the DON for the first time (who will handle classified material) must also be given a basic security indoctrination by the employing activity.

3. Commanding officers are responsible for security education in their commands, ensuring time is dedicated for training and awareness. Supervisors, in coordination with the command security manager, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand the security requirements for their particular assignment. On-the-job training is an essential part of command security education and supervisors must ensure that such training is provided.

4-3 SCOPE

1. Security education must be provided to all personnel. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.

2. In formulating a command security education program, the security manager must provide the minimum briefing requirements of this regulation. Security managers must guard against allowing the program to become stagnant or simply comply with requirements without achieving the real goals.

3. The security education program should be developed based on the command mission and function and should:

a. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure of classified information and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control;

b. Advise personnel of their responsibility to adhere to the standards of conduct required of persons holding positions of trust and to avoid personal behavior that could render them ineligible for access to classified information or assignment to sensitive duties;

c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties;

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties;

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material and alert them to the strict prohibitions against improper use and abuse of the classification system;

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

g. Familiarize personnel with the security requirements for their particular assignments and identify restrictions;

h. Instruct personnel having knowledge, possession or control of classified information on how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her official duties, and can properly protect (store) the information;

i. Advise personnel of the strict prohibition against discussing classified information over an unsecured telephone, fax, IT system or in any other manner that may permit interception by unauthorized persons;

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information;

k. Inform personnel of their particular vulnerability to compromise during foreign travel;

l. Advise personnel that they are to report to their commanding officer, activity head or designee, contacts with any individual regardless of nationality, whether within or outside the scope of the individuals official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

m. Advise personnel of the penalties for engaging in espionage activities and for mishandling classified information or material.

4-4 MINIMUM REQUIREMENTS

1. The following are the minimum requirements for security education:

a. Indoctrination of personnel upon employment by the DON in the basic principles of security (paragraph 4-5 applies).

b. Orientation of personnel who will have access to classified information or assignment to sensitive duties

(including IT duties) at the time of assignment, regarding command security requirements (paragraph 4-6 applies).

c. On-the-job training in specific security requirements for the duties assigned (paragraph 4-7 applies).

d. Annual refresher briefings for personnel who have access to classified information (paragraph 4-8 applies).

e. Counterintelligence briefings annually for personnel who have access to information classified Secret or above (paragraph 4-9 applies).

f. Special briefings as circumstances dictate (paragraph 4-10 applies).

g. Debriefing upon termination of access (paragraph 4-11 applies).

4-5 INDOCTRINATION

1. All personnel entering employment with DON need to have a basic understanding of what classified information is, and the reasons(s) for its protection, as well as how to protect it.

2. A basic indoctrination for military members is done during training at the time of induction. Civilians will be indoctrinated by the employing command.

3. Through indoctrination, all personnel should know that:

a. Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;

b. Classified material will be marked to show the level of classification;

c. Only those who have been officially and specifically authorized may have access to classified information;

d. Personnel will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position.

e. Classified material must be stored and used in secure areas, must be protected during transfer from one area to another (including electronic transfer), and must be destroyed

by authorized means;

f. Any compromise or other security violation must be reported;

g. Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported.

4-6 ORIENTATION

1. Personnel who will have access to classified information or assignment to sensitive IT duties will be given a command security orientation briefing as soon as possible after reporting aboard or being assigned to duties involving access to classified information or assignment to sensitive IT duties.

2. A review of written command security manuals or material is not normally considered adequate for an orientation briefing.

3. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands, with irregular changes of personnel, individual policy manual may be necessary.

4. Through orientation, all personnel should know:

a. The command security structure (i.e., who the security manager is, who the TSCO is, SSO, etc.);

b. Any special security precautions within the command, (e.g., restrictions on access);

c. Command security procedures for badging, security checkpoints, destruction, visitors, etc.;

d. Their responsibility to protect classified information;

e. Their obligation to report suspected security violations;

f. Their obligation to report information that could impact on the security clearance eligibility of an individual who has access to classified information.

5. Additionally, commands must ensure that individuals assigned to DON IT positions receive the requisite information assurance, security awareness, and functional competency training as

required by their designated level of access and scope of duties, and that the training is documented in individual personnel files. Understanding the threats, system vulnerabilities, and protective measures required to counter such threats at each IT access level are key features of a core information assurance awareness program.

6. The security orientation should be tailored to the command and to the individual receiving it. More emphasis on security procedures will be needed when the individual has not had previous experience handling classified information.

4-7 ON-THE-JOB TRAINING

1. On-the-job training is the phase of security education when security procedures for the assigned position are learned. Security managers will assist supervisors in identifying appropriate security requirements.

2. Supervision of on-the-job training process is critical. Supervisors are ultimately responsible for procedural violations or for compromises that result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable.

4-8 REFRESHER BRIEFINGS

1. Once a year, all personnel who have access to classified information will receive a refresher briefing designed to enhance security awareness.

2. The refresher briefing may be addressed to the entire command or it could be tailored for particular groups in the command. It should cover general security matters but need not cover the whole subject of security.

3. Refresher briefings should cover:

- a. New security policies and procedures,
- b. Counterintelligence reminders regarding reporting contacts and exploitation attempts and foreign travel issues;
- c. Continuous evaluation; and
- d. Command specific security concerns or problem areas.

- e. Attestation of Nondisclosure Agreement requirements.
4. Results of self-inspections, inspector general reports, or security violation investigations provide valuable information for use in identifying command weaknesses;
 5. Every individual who is authorized Top Secret clearance eligibility, or who has access to SAP or SCI access, will make a verbal attestation confirming that they will conform to the conditions and responsibilities imposed by law and regulation on individuals granted such eligibility or access. The following applies to DON military and civilian personnel:
 - a. After reading the entire Classified Information Nondisclosure Agreement (Exhibit 4A) and/or the SCI/SAP Indoctrination Form, individuals initially authorized Top Secret clearance eligibility or access to a specially controlled category or compartmented information (SCI and SAP), shall verbally attest to fully understanding their responsibilities in protecting national security information and adhering to the provisions specifically stated in paragraph 1 of the forms to which they are agreeing.
 - b. The forms and verbal attestation must be witnessed by one individual in addition to the official presiding over the attestation.
 - c. Personnel with an existing Top Secret clearance eligibility or SCI/SAP access will verbally attest at the time the required periodic reinvestigation is requested or when granted access to another compartmented program, whichever is sooner.
 - d. During refresher training, commands will stress the provisions of the Nondisclosure Agreement and the responsibilities inherent for individuals with access to classified information. Security managers will be responsible for recording this training. Execution of the nondisclosure agreement forms will be recorded in JPAS.

4-9 COUNTERINTELLIGENCE BRIEFINGS

All personnel who have access to material classified Secret or above must receive periodic briefings, annually, on all threats posed by foreign intelligence and terrorist organizations. The security manager is responsible for arranging for the briefing with the local NCIS office.

4-10 SPECIAL BRIEFINGS

1. Special briefings include briefings that are not required as a matter of routine, but which may be required by unique circumstances or other program requirements including:

a. **Foreign Travel Briefing**

(1) Although foreign travel (personal or business) may be briefly discussed during annual refresher briefings, it may also be appropriate to require separate foreign travel briefings for personnel, especially for those who travel frequently. It is in the best interest of the command and the traveler to ensure travelers are fully prepared for any particular security or safety concerns that the foreign travel may introduce.

(2) A foreign travel briefing is usually only offered to those individuals who have access to classified information. However upon request, an unclassified version may be given to dependents, or others who do not have access, separately. (Individuals with SCI access should be referred to their SSO for foreign travel briefing requirements).

(3) Upon return of the traveler, they should be provided the opportunity to report any incident, no matter how insignificant it might have seemed, that could have security implications.

(4) Audiovisual material for a formal foreign travel briefings is stocked at servicing NCIS offices.

b. **New Requirement Briefings**. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

c. **Program Briefings**. Briefings that are specified or required by other program regulations (e.g., NATO, SIOP-ESI, SCI, etc.)

d. **NATO Security Briefing**. All personnel who have access to a SIPRNET terminal accredited to receive and process NATO information must receive a NATO security briefing.

2. Special briefings will be recorded in JPAS as functionality permits, or records may be maintained locally in the form of rosters or other automated format, until JPAS record keeping

functionality is fully deployed.

4-11 COMMAND DEBRIEFING

1. A debriefing will be given to individuals who no longer require access to classified information as a result of:

- a. Transfers from one command to another;
- b. Terminating active military service or civilian employment;
- c. Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or transfer to the Inactive Ready Reserves (IRR);
- d. Expiration of a Limited Access Authorization (LAA);
- e. Inadvertent substantive access to information that the individual is not eligible to receive;
- f. Security clearance eligibility revocation; or
- g. Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause. Refer to chapter 9 for additional information.

2. Debriefings must include the following:

- a. All classified material in individuals' possession must be returned;
- b. Individuals are no longer eligible for access to classified information;
- c. Reminder of the provisions of the Classified Nondisclosure Agreement (SF 312) (exhibit 4A) to never divulge classified information, verbally or in writing, to any unauthorized person or in judicial, quasi-judicial, or in administrative proceedings without first receiving written permission of CNO (N09N2);
- d. There are severe penalties for disclosure; and
- e. The individual must report to the NCIS (or to the FBI or nearest DoD component if no longer affiliated with the DON), without delay, any attempt by an unauthorized person to solicit classified information.

3. As part of a debriefing, individuals will be required to read the provisions of the Espionage Act and other criminal statutes. If individuals are retiring from active service and will be entitled to receive retirement pay, they must be advised that they remain subject to the Uniform Code of Military Justice (UCMJ).

4. As part of every debriefing (except when individuals transfer from one command to another command) a Security Termination Statement is required (paragraph 4-12 applies).

4-12 SECURITY TERMINATION STATEMENTS

1. Individuals must read and execute a Security Termination Statement (OPNAV 5511/14), exhibit 4B, at the time of debriefing, unless the debriefing is done simply because the individual is transferring from one command to another and will continue to require access to classified information.

2. A witness to the individual's signature must sign the Security Termination Statement.

3. The command, agency, or activity's name and mailing address will be annotated on the three lines at the top of the form.

4. The original signed and witnessed Security Termination Statement will be placed in the individual's official service record or the official personnel folder for permanent retention except:

a. When the security clearance eligibility of a Marine is revoked for cause, the original Security Termination Statement will be forwarded by the command to the Commandant of the Marine Corps (CMC) along with a copy of the revocation letter, for placement in the Master Service Record Book (MSRB).

b. When the Security Termination Statement is executed at the conclusion of a Limited Access Authorization, the original will be retained in command files for two years.

5. If an individual refuses to execute the Security Termination Statement, the individual will be debriefed, before a witness if possible, stressing the fact that refusal to sign the Security Termination Statement does not change the individual's obligation to protect classified information from unauthorized disclosure as stated on the Classified Information Nondisclosure

Agreement (SF 312). The Security Termination Statement will be annotated to show the identity and signature of the witness, if one was present, and that the individual was debriefed, but refused to sign the Security Termination Statement. Send a copy of only refusals to CNO (N09N2).

6. The SECDEF has specifically directed that Security Termination Statements will be executed by senior officials (flag and general officers, ES-1 and above, Senior Executive Service and equivalent positions). The immediate senior officials will ensure that the statement is executed and that failure to execute the statement is reported immediately to the (DASD(S&IO) via CNO (N09N2).

4-13 TRAINING FOR SECURITY PERSONNEL

1. The NCIS Security Training, Assistance, Assessment Team (STAAT) offers the Naval Security Manager Course, DON unique core training developed to train security managers, but also available to security specialists and assistants. For more information on this course, contact the Atlantic STAAT at NAB Little Creek, (757) 462-283 or DSN 253-2834 or the Pacific STAAT at NAS North Island, (619) 545-8934 or DSN 735-8934 or the CNO (N09N2) web page at www.navysecurity.navy.mil.

2. A Navy correspondence course entitled "Department of the Navy Introduction to the Information and Personnel Security Program," NAVEDTRA #14210, is available through the command education service officer (ESO).

3. For other security training available to DON personnel, contact the CNO (N09N2) security education specialist at (202) 433-8843 or DSN 288-8843. Security training opportunities are also posted on the CNO (N09N2) web page at www.navysecurity.navy.mil.

4. A listing of security disciplines and phone numbers is published periodically and posted on the web page to assist in routing telephone requests.

4-14 SECURITY AWARENESS

To enhance security, a security education program must include continuous and frequent exposure to current information and other awareness materials. Signs, posters, bulletin board notices, and Plan of the Day reminders are some of the media that should be used to promote security awareness.

SECURITY TERMINATION STATEMENT

(Enter the name and address of the Navy or Marine Corps activity obtaining this statement)

1. I HEREBY CERTIFY that I have returned to the Department of the Navy (DON) all classified material which I had in my possession in accordance with the directions contained in the DON Information and Personnel Security Program Regulations SECNAVINST 5510.36, the EKMS-1, CMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 and 3, and EKMS-1 Supplement 1, CMS Policy and Procedures for Navy Electronic Key management System Legacy Accounts/Tier 2S.

2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information to any person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and I agree to obtain the decision of the Chief of Naval Operations (CNO) or the CNO's authorized representative, on such matters prior to disclosing information which is or may be classified.

4. I will report to the Federal Bureau of Investigation or to the local Naval Criminal Investigative Service office without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I have been informed and am aware that Title 18 U.S.C. Sections 641, 793, 794, 798, 952 and 1924, as amended, and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial as provided by Title 18 U.S.C. 1001.

6. I have/have not received an oral debriefing.

Signature of Witness	Signature of employee or military member
Type or print name of witness	Type or print first, middle and last name of employee or service member. Include civilian grade or military rank/rate.
DATE	DATE

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER <i>(See Notice below)</i>
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) <i>(Type or print)</i>		

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS <i>(Type or print)</i>		NAME AND ADDRESS <i>(Type or print)</i>	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS <i>(Type or print)</i>	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.