OUTLINE SHEET 2.1

Security Education Program

REFERENCE

SECNAV M-5510.30, Chapters 2, 3, and 4
SECNAV M-5510.36, Chapter 3

OUTLINE

A. PROGRAM PURPOSES (PSP 4.1, ISP 3-1)

1. Required for all DON commands handling classified information with goal to instruct all personnel in security policy and procedures and foster awareness (Not limited to those with clearance/access)

2. Integrate security awareness into duty performance

3. Essential for a successful security program

B. Responsibility for Security Education (PSP 4.2)

1. CNO (N09N2) - Policy guidance, education requirements, and source support

2. Entry-level Training Commands - Indoctrinating new recruits/officers in what classified information is and why and how it is protected

3. USN/USMC Commands:

   a. COs (through Security Managers)- Ensure sufficient time dedicated to security education

   b. Supervisors - OJT security requirements

C. Program Scope (PSP 4.3)

1. Should be broad, centered on classified information held by the command, and tailored to specific job needs

2. Includes personnel with or without clearance/access, but greatest emphasis is on cleared personnel

3. Need to advise personnel of:

   - Denial of unauthorized access
   - Importance of personal behavior

- Reporting security-relevant derogatory behavior
- Continuous evaluation of personnel
- Requirements for classified information
- Challenges to improper classification
- Security requirements of job
- Access and need-to-know concepts
- Hostile threat to communications, IT systems
- Foreign intelligence techniques
- Vulnerabilities during foreign travel
- Penalties for espionage and mishandling information
- Personal security reporting responsibilities

NOTE: Each item above is more fully explained in paragraph 4-3.3, PSP

D. Minimum Security Education Requirements (PSP 4-4) (see figure 2.1-1)

BRIEFING	NEWLY ENTERING PERSONNEL	PERSONNEL WITH CONFIDENTIAL Access	PERSONNEL WITH SECRET AND ABOVE Access	PERSONNEL WITHOUT CLEARANCES
Indoctrination	■			
Orientation		■	■	○
On-the-Job		■	■	
Annual Refresher		■	■	○
Counter-Intelligence		○	■	○
Special Briefings		■	■	○
Debriefings		■	■	
Legend: ■ **REQUIRED** ○ **OPTIONAL**				

Figure 2.1-1. Minimum briefing requirements.

1. Indoctrination briefing - basic security principles **(PSP 4.2, 4.4, 4-5)**

a. Given to recruits/officers during entry training and to new hire civilians (who will be handling classified material) by employing command

b. Topics (basic security principles):

- Need to safeguard
- Classification markings
- Access requirements
- Continuous evaluation
- Use, storage, transmission, destruction
- Reporting any compromise or other security violations
- Reporting any attempt by unauthorized person(s) to solicit classified information

2. Orientation briefing **(PSP 4-6)**

a. Required for all personnel who will have access and/or assignment to sensitive IT duties – Given as soon as possible after personnel report aboard or being assigned duties involving classified access or assignment to sensitive IT duties

b. Depending on command size, may be scheduled group session or done with individual

c. DO NOT rely on "read and sign" or on their maturity and past experience; DO NOT fail to specify responsibility for orientation

d. Given on topics specific to the command, such as:

- Command security structure
- Special security precautions
- Command security procedures
- Classified information control procedures
- Physical security measures
- Local counterintelligence situation
- Reporting information which could impact security clearance eligibility
- Reporting suspected security violations
- Processing classified information on command information (computer) systems and the name of the Information Assurance Manager (IAM)

(See Student CD for sample Orientation Briefing)

3. On-the-Job training **(PSP 4-7)**

a. Critical training - Supervisor's responsibility

NOTE: Supervisors are ultimately responsible for procedural violations or for compromises resulting from improperly trained personnel

b. Cover security procedures that apply to a member's specific duties, to include topics such as:

- Use, handling, storage
- Clearance/Access of co-workers/visitors
- Accessing information - visitors
- Opening/securing containers and spaces
- Control procedures
- Destruction procedures/responsibilities
- Key security personnel

4. Annual refresher briefings **(PSP 4-8)**

a. Required for all personnel with access to classified information; need not cover all aspects of security

b. Topics/focus:

- Changes in security policies/situations
- Review of command security situation, vulnerabilities, violations, areas of concern
- Anticipated changes that could affect command security posture
- Review of key security practices
- Reiteration of individual’s responsibility and trust in being given access to classified national security information
- Obligation to protect classified information through proper safeguarding and limiting access to those with clearance, access and need-to-know
- Counterintelligence reminders about reporting contacts and exploitation attempts **(PSP 3-3)**
- Continuous evaluation/Reporting requirements
- Focus on recent security issues (not a repeat of other briefings)

5. Counterintelligence briefings **(PSP 4-9)**

a. Required annually if have access to Secret or above (separate brief from Annual Refresher)

b. Request from servicing NCIS Office

6. Special briefings – Provided for such areas as: **(PSP 4-10)**

- Foreign travel (May be part of Annual Refresher Brief or a separate briefing)
- New requirements
- Program briefings (e.g., NATO, NC2-ESI, SCI)- Record in JPAS

  NOTE: Conduct NATO briefings for USN personnel who have access to a SIPRNET terminal accredited to receive and process NATO information. Conduct NATO briefings for **ALL** USMC personnel who have access to SIPRNET (MARADMIN 136/04)

- Command discretion (e.g., STU III briefing, CDO briefings, JPAS Usage)

7. Command debriefings **(PSP 4-11)**

a. Required on following occasions, for all personnel who no longer need access:

- Command to command transfer
- Termination of service
- Temporary separation for 60 days or more
- Expiration of Limited Access Authorization (LAA)
- Inadvertent substantive access to ineligible individual(s)
- Revocation of clearance eligibility for cause
- Administrative withdrawal or suspension for cause of clearance and SCI access

b. Required debriefing topics: **(PSP 4-11.2)**

- Return of classified information
- No longer eligible for access
- Reminder of the provisions against unauthorized disclosure
- Penalties for unauthorized disclosure
- Reporting of unauthorized solicitations

(See Student CD for sample Debriefing)

c. Required to read provisions of Espionage Act and other criminal statutes

d. Must read and execute Security Termination Statement (OPNAV Form 5511/14) **(PSP 4-12, Exhibit 4A)** (See Student CD for OPNAV Form 5511/14)

NOTE: Exception – do not execute upon command to command transfer debriefing

(1) Administrative requirements:

- Witness signature
- Command name/mailing address at top
- USN - Place original signed/witnessed form in service record
- USMC – Place original signed/witnessed form in service record book; Submit original to MMSB-20 if clearance revoked for cause – forward with revocation letter to CMC
- Civilians – Place in official personnel folder
- Completion of LAA – retain original in command files for 2 years

(2) Actions in case of refusal to execute form:

- Debrief, before a witness, if possible
- Annotate termination form to reflect identity and signature of witness (if present) and individual debriefed but refused to sign
- Send a copy of the termination form to CNO (N09N2) immediately

(3) Required of senior officials – Flag/Senior Executive Service (SES) done by immediate senior (report refusal to Deputy Assistant Secretary of Defense (S&IO) via CNO (N09N2)

e. Record date and reason for debrief in JPAS

E. Special Training Requirements (ISP 3-3) (PSP 4-6 and 4-10)

1. Specific job training required for incumbents in following designated positions:

- Security Manager
- Original classifier
- Derivative classifier
- Security Specialist
- Classified courier

- Declassifier (other than original classifier)
- Personnel assigned DON IT positions (Must receive requisite information assurance, security awareness, and functional competency training as required by their designated level of access and scope of duties)

2. Additional training may be required for personnel:

- Traveling to foreign countries with special concerns about exploitation or at meetings with foreign attendance
- Involved with international programs
- Involved with certain acquisition programs

F. Documentation (PSP 4-5 thru 4-11)

1. COs will maintain a personnel security record on all personnel, including security briefings received

2. Essential to a successful security program

3. Means to indicate:

   a. Dates and type of briefings conducted

   b. Who attended

   c. Security awareness program initiatives

G. Continuing Security Awareness (PSP 4-14)

In addition to the mandatory security briefings, commands should conduct continuing security awareness programs through:

- POD/POW notes (see Student CD for some POD/POW notes)
- Signs and posters
- Bulletin board notices
- GMT
- SOPs
- Drills
- Special events (e.g., security standdowns, security cleanouts, special briefings)
- Recognition of personal and organizational security achievements