

LESSON TOPIC 1.1**Command Security Program****REFERENCES**

EO 13526, Classified National Security Information (NSI)
EO 12968, Access to Classified Information
EO 10450, Security Requirements for Government Employees
EO 12829, National Industrial Security Program
DOD 5200.01, Volume 1, DOD Information Security Program:
Overview, Classification and Declassification
DOD 5200.01, Volume 2, DOD Information Security Program:
Marking of Classified Information
DOD 5200.01, Volume 3, DOD Information Security Program:
Protection of Classified Information
DOD 5200.01, Volume 4, DOD Information Security Program:
Controlled Unclassified Information
DOD 5200.2-R, DOD Personnel Security Program Regulation
SECNAVINST 5510.36A, DON Information Security Program (ISP)
Instruction
SECNAV M-5510.36, DON Information Security Program (ISP)
Manual, Chapters 1 and 2
SECNAVINST 5510.30B, DON Personnel Security Program (PSP)
Instruction
SECNAV M-5510.30, DON Personnel Security Program (PSP)
Manual, Chapters 1, 2 and Appendix C
OPNAVINST 5530.14E, Navy Physical Security and Law
Enforcement Program

LESSON

- A. National Security Organization (ISP 1-1 thru 1-5,
PSP 1-1 thru 1-3)**
1. Presidential Executive Orders (EOs) 13526, 12968 and 10450 set standards for classifying information and granting access to classified information; 12829 sets standards for safeguarding classified information released to industry
 2. Structure operates at different levels: President; National Security Council; Department of Defense; Department of the Navy; and individual USN/USMC commands

3. DON level (Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration) - Responsible to SECNAV for effective program compliance and implementation; Guidance issued under DUSN(PPO&I); Responsible for maintaining a world wide web page at www.ncis.navy.mil/securitypolicy for policy guidance

B. Command Security Management

1. Controlling regulations for the DON's Information and Personnel Security Program: SECNAV M-5510.36 and M-5510.30 respectively (**ISP 1-1, PSP 1-1**)
2. Commanding Officer's responsibilities (**ISP 2-1, PSP 1-5 and 2-2**)
 - Safeguard classified material and ensure personnel security oversight through an effective Program (Commanding Officers can impose more stringent requirements than SECNAV M-5510.36 and M-5510.30 if situation warrants and if they do not impact other commands nor contradict the ISP and PSP)
 - Designate Security Manager (designation letter) and other key personnel and assistants in writing
 - Implement a security education, training and awareness program for all assigned personnel
 - Issue written command security instruction and emergency plans
 - Conduct command self inspections and review/inspect subordinate commands for program effectiveness
 - Set up an Industrial Security Program when command engages in classified procurement and or cleared DOD contractors operate within areas under their direct control
 - Apply risk management, as appropriate, for safeguarding of classified information, including

use of personal electronic devices in areas where classified information is processed or stored

- Ensure Security Manager receives formal training (Naval Security Manager Course (S-3C-0001)) and other security personnel receive training, as required, to support command security education program
- Ensure implementation Joint Personnel Adjudication System (JPAS)
- Ensure Security Manager has direct access
- Ensure performance rating systems of all DON military and civilian personnel whose duties significantly involve the creation, handling, or management of classified information include a critical security element on which to be evaluated

3. Components that make up a command security program: Organization; Procedures, Transmission of classified material; Education and Training; Controls; Information Security Measures; Inspections; Continuous Evaluation; Personnel Security

C. Security Manager (ISP 2-2, PSP 2-3 and 2-4)

1. Submit copy of designation letter to DUSN(PPO&I). Preferred method, scan letter and send to W_DONAA_CYGN_DON_SECURITY_INFO_PERS_US@NAVY.MIL With UIC/RUC and return email.
2. Identify to all members of command on POD/POW, organization charts, telephone listings, rosters,
3. Obtain formal training
4. Following is a list of Security Manager duties (not all duties apply to every Security Manager):
 - Advise Commanding Officer
 - Develop written command security procedures and Emergency Plan(s)

- Coordinate Awareness and Education Program
- Coordinate with other security personnel (e.g., Security Officer, Legal Officer, Information Assurance Manager, Public Affairs Officer,)
- Ensure personnel execute Classified Information Nondisclosure Agreement (SF 312)
- Deal with threats, compromises, and violations, to include those involving IT systems (coordinate with IAM on after-incident responses involving classified information processed on IT systems)
- Manage the Joint Clearance and Access Verification System (JCAVS) (a subset up the Joint Personnel Adjudication System (JPAS)), ensure personnel security investigations, clearances and access are properly documented
- Manage command information security program to include: Accounting and control measures; Classification management/Marking; Safeguarding and storage; Release of classified information; Coordinating access for visitors, if authorized
- Manage other requirements of the personnel security program to include: Ensuring personnel are appropriately cleared prior to being assigned access; assigning access based on need-to-know; Requesting personnel security investigations (PSIs), when required; Coordinating command's continuous evaluation program; Verifying clearance/access for visitors who require access

D. Security Organization (PSP 2-5 to 2-9, ISP 2-3 to 2-9)

1. Needs directed by command size and complexity
2. Personnel in the following positions (collateral or full-time) work for the Security Manager: Top Secret Control Officer (TSCO); Assistant Security Manager; Security Assistants and/or Clerks; Contracting Officer's Representative (COR)

3. Personnel in the following positions (collateral or full-time) may either work *with* or *for* the Security Manager: Security Officer; Information Assurance Manager (IAM); Operations Security (OPSEC) Officer; Electronic Key Management System (EKMS) Manager (In performance of EKMS duties - works directly for CO); Special Security Officer (SSO), Foreign Disclosure Officer, Knowledge Management Officer, Communication Officer, Research Officer
4. Security position requirements (see figure 1.1-1)

SECURITY POSITION REQUIREMENTS						
POSITION	MINIMUM GRADE		CIT	PSI	CLEARANCE	WRITTEN DESIG
	MILITARY	CIVILIAN				
SECURITY MANAGER	OFFICER	GS-11	↑ U.S. citizen ↓	SSBI	= ACCESS	↑ YES ↓
TSCO	E-7	GS-7		SSBI	FINAL TS	
IAM				SSBI	= ACCESS	
SSO*	OFFICER	GS-9		SSBI	FINAL TS	
COR					= ACCESS	
<u>SECURITY ASSTS</u>						
ASST SEC MGR	E-6	GS-6		**	= ACCESS	
TS CONTROL ASST	E-5	GS-5		SSBI	FINAL TS	
SECURITY CLERK				= ACCESS	NO	

* SECURITY MANAGER MAY ALSO BE SSO (SSO NAVY MUST APPROVE)

** ASST SEC MGR - SSBI REQUIRED IF DESIGNATED TO GRANT TEMPORARY ACCESS (INTERIM CLERANCE)

Figure 1.1-1. Security position requirements

E. Command Security Instruction (ISP Exhibit 2A, PSP Appendix C)

1. Form and content depend on command mission, demographic considerations, and classified information held. Commanding Officer should sign instruction.
2. Elements of written procedures required of each command that handles classified information (see figure 1.1-2)

Figure 1.1-2. Command Written Procedures

COMMAND SECURITY PROCEDURES	
Table of Contents	
Section	Page
1. Security Organization...	...
2. Control Measures...	...
3. Physical Security...	...
4. Reproduction Control...	...
5. Destruction...	...
6. Access...	...
7. Classified Receipts...	...
8. Safeguarding/Storage	...
9. Security Education...	...
10. Classification Management/ Marking...	...
11. Visit Procedures...	...
12. Personnel Security Procedures	...
13. Security Reviews/Inspections	...
14. Reporting Requirements...	...
15. Procedures for loss/compromise	...
16. Processing classified information on IT systems	...

3. Points to remember in writing security procedures (ISP, Exhibit 2A and PSP, Appendix C provide guidance):
 - Command procedures *supplement* (don't repeat) ISP and PSP. Avoid general statements - Be specific as to what is to be done and who is to do it

- Include, when appropriate: Controls on special types of classified and controlled unclassified information (CUI); Processing classified information on IT systems and any Security Servicing Agreements (SSAs)

F. Emergency Plans (ISP Exhibit 2B, Part One and Two)

1. Commands that handle classified information must develop an Emergency Plan to protect the information in the event of a natural disaster or civil disturbance (**Part One**)
2. Deployable commands and commands located outside the U.S. and its territories must also include an Emergency Destruction Supplement (**Part Two**) (The requirements for this will be covered in the Lesson Topic 5.2, Destruction)
3. Variables to consider: Command's risk posture; Local situation (e.g., command mission, capabilities, and environmental, political, and physical conditions); Classified holdings: (e.g., amount; disposition and sensitivity; command command/control considerations; and impact of any)
4. Factors to include: Designate persons authorized to implement; Use of security personnel and equipment; Coordination with other commands/agencies; Means to transport classified material; Assessment of integrity of classified information after the emergency
5. Accommodate most sensitive material first
6. Critical aspects: Minimize risk to personnel and ensure access not denied to uncleared fire and emergency personnel
7. Ensure personnel are trained on the Emergency Plan

G. Security Servicing Agreements (SSAs) (ISP 2-10, PSP 2-11)

1. One activity performs specified security functions for another when a command is not set up to perform certain security functions, or when it is more economical
2. Typical situations: Host-tenant, senior-subordinate, contractor located on Navy/Marine Corps installation, inter-service agreement, or when one command has greater capability or is tasked by its common support mission
3. Conditions: Clearly define functions to be accomplished; Include in command security procedures; Include procedure to notify command Commanding Officer on command security matters

H. Combat Operations (ISP 1-5, PSP 1-9)

Commanding Officers may modify the safeguarding requirements of the ISP, as necessary, to meet local conditions during combat or combat-related operations. Even under these circumstances, the provisions of the ISP shall be followed as closely as possible. This exception does not apply to regularly scheduled training exercises and operations.

I. Waivers and Exceptions (ISP 1-5, PSP 1-10)

1. Waivers or exceptions can be given to certain aspects of the regulations when circumstances warrant. Possible waivers or exceptions: TSCO grade requirements; Classified storage requirements; Completed SSBI for Security Managers (however, waiver of grade requirements rarely granted); Portion marking requirements
2. Definition:
 - *Waiver* - Granted to provide temporary relief from a specific requirement pending completion of action
 - *Exception* - Granted to accommodate a long term or permanent inability to meet a specific requirement

3. Submit requests, via admin chain of command to DUSN(PPO&I), when conditions exist that prevent compliance with a specific standard or cost of compliance exceeds available resources. If request is for a requirement set by the PSP (e.g., an administrative issue) - Submit waiver in letter format stating why requirement cannot be met and alternative procedures.
4. If request is for a requirement set by the ISP (e.g., a physical security/equipment issue) - Submit waiver or exception request as follows: (Each request requires an identifier) (See figure 1.1-3)

<i>WAIVERS</i>	<i>EXCEPTIONS</i>
N01234-W(I)-01-13	N24467-E(I)-02-13
N=Navy	N=Navy
01234=UIC	24467=UIC
W=Waiver	E=Exception
(I)=Information Security	(I)=Information Security
01=Number of Waiver requests this CY	02=Number of Exception requests this CY
13=Calendar Year (CY)	13=Calendar Year (CY)

Figure 1.1-3. Waivers and Exceptions Format

- Include a complete description of problem and describe compensatory procedures, as appropriate, and POC information (name, rank/grade, DSN and commercial phone numbers). (For waiver requests include a Plan of Action and Milestones (POA&M) on when command plans fixing issue that waiver is being requested for to include start and completion dates)

NOTE: Waivers and exceptions are self-cancelling at the end of the specified period, unless a renewal request is approved by DUSN(PPO&I)

J. Security Inspection and Reviews (ISP 2-11, PSP 2-10)

1. Important part of command security programs which includes review/inspection of subordinate units and self-inspections

2. Commanding Officers are responsible for evaluating and documenting the overall security posture of the command and subordinate commands by conducting inspections, assist visits, and reviews. (May be conducted during other scheduled inspections with the results identified as such)
 3. Self-inspections are an important technique to:
Identify and resolve possible security weaknesses; Train personnel in security functions; Identify future security programs and resource requirements. (Exhibit 2C (ISP) and Appendix D (PSP) are comprehensive self-inspection checklist guides.)
- K. Echelon I and II Commands (CNO ltr 5510, ser N09N2/9U223112 of 7 May 09, Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36)**
1. Submit results of command reviews (i.e., assist visits, program reviews of specific focus area(s), or self inspection) to DUSN(PPO&I) NLT 30 working days after the end of each fiscal year.
 2. Reports will include: Total number of inspections conducted (including subordinate commands); Significant trends (positive and negative); Corrective action(s) and anticipated completion, if significant weaknesses identified; Challenges (i.e., policy constraints, resource issues, etc.); Total number of security violations (i.e., PIs/JAGMANs to include total resulting from Electronic Spillages); Results of random sampling of originally (if applicable) and derivatively classified (if commands have significant (100 or more) classification activity; Confirm that specialized training (as required by ISP 3-3.1.a-d) has been met; confirm required review and update/cancellation Security Classification Guides (OCAs only)
- L. Security Standdown** (DODM 5200.01-V3 specifies that each activity with classified holdings shall establish at least 1 day each year when specific attention and effort is focused on disposing of unneeded classified material ("clean-out day).

1. A means to do an intensive review of all aspects of a command security program; done on a periodic basis or one-time
2. Can include: Total or partial security self-inspections; Review adequacy of command security procedures; Clean-out of non-mission essential classified information; Inventory accountable TS information; Security briefings and training