

LESSON TOPIC 5.1**Control Measures for Classified Information****REFERENCES**

SECNAV M-5510.36, Chapters 2, 7, 9 and 10

SECNAV M-5510.30, Chapter 3

LESSON**A. Basic Policy (ISP 7-2)**

1. Classified information shall be afforded a level of control measures commensurate with its assigned security classification level
2. Includes all classified information that resides on classified IT systems
3. SECNAV M-5510.36 establishes baseline standards, but the Commanding Officer may impose more stringent requirements within the command or upon subordinates (if warranted) **(ISP 2-1)**
4. Applies to classified information introduced into your command by ensuring its proper dissemination and limiting reproduction
5. Classified information held shall be turned in by all military or civilian personnel upon resignation, separation, retirement or transfer **(ISP 7-1)**
6. Commanding Officers will ensure that all Controlled Unclassified Information (CUI) is safeguarded from unauthorized access by the public (to include that residing on IT systems)

B. Top Secret Control Measures (ISP 7-3)

1. All TS originated or received by a command shall be:
 - Accounted for continuously with signed receipts
 - Individually serialized at time of origination
 - Entered into a command Top Secret Register or

Log; format is command option (e.g., Log Book, computerized database, Control Form)

2. The Top Secret Control Officer (TSCO) shall:
 - a. Maintain a system of accountability (e.g., registry or log) to completely identify TS information to include:
 - Date originated/received
 - Individual serial number
 - Copy number
 - Title
 - Originator
 - Number of pages
 - Date of disposition action taken (e.g. transfer, downgrade, declassification, destruction)

(Maintain TS registers or logs for 5 years following disposition)
 - b. Mark command originated TS with copy number in specific format: "Copy no. ___ of ___ copies."

(Exceptions - publications containing distribution list by copy number and mass-produced reproductions where copy numbering would be prohibitive)
 - c. Obtain a record of receipt (typically a classified material receipt) from each recipient for TS information distributed internally and externally
3. Physical inventories - All TS shall be physically sighted or accounted for at least annually or when circumstances warrant, such as:
 - Change of command
 - Change of TSCO
 - Report of loss or compromise

Exception: Repositories, Libraries or activities which store large volumes of classified material (see ISP Chapter 7, paragraph 7-3 for guidance)

C. Secret Control Measures (ISP 7-4)

1. Commanding Officers shall establish administrative procedures for the control of Secret information appropriate to their local environment.
2. Controls based on assessment of the threat, location, and command mission.
3. Used to protect Secret information from unauthorized disclosure by access control and compliance with marking, storage, transmission and destruction requirements
4. Acknowledgement of receipt is required for all Secret information transmitted or transported in and out of the command

(Special types of classified information (i.e., NATO, NWPs) may require additional requirements)

D. Confidential Control Measures (ISP 7-5)

Administrative procedures will be put in place to protect Confidential information from unauthorized disclosure and ensure compliance with marking, storage, transmission and destruction requirements

E. Secret and Confidential Working Papers (ISP 7-6)

1. May be classified notes from a training course or conference, research notes, rough drafts, and similar items that are not finished documents
2. Accountability requirements:
 - Date when created
 - Conspicuously mark each page, top and bottom center with the highest classification level of any information they contain
 - Mark words "Working Paper" on top left of first page in letters larger than the text
 - Protect per assigned classification level
 - Destroy, by authorized means, when no longer needed

3. Requirements for a finished document apply when documents are retained more than 180 days from creation date or officially released outside the command by the originator

(A document transmitted over a classified IT system (e.g., SIPRNET) is considered a finished document)

4. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain Top Secret information

F. Risk Management Process (ISP 2.1)

1. Guiding philosophy of modern security programs

- Commands confront different environments and sets of changing operational requirements and therefore each Commanding Officer shall apply risk management principles to determine how best to attain the required levels of protection

- Risk Management is a rational and defensible method for making decisions about expenditures of scarce resources, and selection of cost-effective countermeasures to protect valued assets

- Risk management application results in command decisions to adopt specific security measures given the relative costs and available resources

2. Definitions

- Risk Management - The process of selecting and implementing proper countermeasures to achieve an acceptable level of risk at an acceptable cost (i.e., implementation of only those countermeasures which are justified as a result of a systematic assessment of the degree of risk in a situation)

- Risk - The potential damage or loss of an asset

- Level of risk - Combination of value placed on asset by its owner and the consequence, impact,

or adverse effect of loss or damage to that asset, *and* likelihood that a specific vulnerability will be exploited by a particular threat

- Impact - The amount of loss or damage that can be expected

- Adversary - Any organization, condition, or action which has capability of acting upon an asset in a detrimental manner

3. Risk Management Components: Analysis - determines the existing level of risk; Decision - determines what will be done about those risks.

4. Risk analysis consists of 5 steps:

- Identify and Prioritize Assets

- An asset can be any person, facility, material, information, or activity which has a positive value. Some examples of assets in the Information and Personnel Security Program are:

-Classified material-levels & amounts

-Classified equipment-computers

-Security Containers-Secure Rooms,
Vaults, Cruise Box Security

Padlocks, Built-in combination locks

-Restricted Areas-levels

-Badge System

-24 hour Watch

-Gate Guard-Security Patrols/guards

- Intrusion Detection Systems (IDS)

- Once assets have been identified they need to be prioritized based upon their value and the *impact* if they were damaged, lost or compromised

(This process determines value of what assets the command is trying to protect and the consequences of their loss to national security)

- Threat Assessment - Any indication, circumstance or event with the *potential* to cause the loss, compromise or damage to an asset. Certain things to consider: Who/what is the adversary; Intent/motivation of adversary; Frequency of threat; Type of threats; Magnitude of foreign intelligence threat (or other type of threat) at command's physical location
- Vulnerability Assessment - Vulnerability is any weakness that can be exploited by an adversary to gain access to an asset. Can result from:
 - Human vulnerabilities (Personal behavior attitudes, current awareness, e.g., lack of a continuous evaluation program); Building characteristics (Vulnerabilities such as weak door locks, absence of guards); Equipment/material properties; Locations of people, material, equipment; and buildings (Vulnerabilities such as being OCONUS or in an office off base); Operation of personnel practices
 - Some things to evaluate - Probability of inadvertent loss of sensitive information when command members lack sufficient knowledge of safeguarding rules and procedure. Some examples of vulnerabilities would be: Poor Security Education Program; Non effective procedures such as no handcarry procedures, no copy restrictions/controls
 - Other considerations: Types of vulnerabilities (i.e., physical/technical, manpower); Degree of vulnerability to each asset; and Existing countermeasures and effectiveness
- Identification of security countermeasures (i.e., procedures, control measures, physical protection, etc.,) that could eliminate or reduce the threat to (better protect) the asset and costs and benefits in terms of risk reduction
- Analysis of the cost and/or benefit of employing the countermeasures

- Analyze the benefits of the countermeasure vs. its cost (i.e., it would be hard to justify buying a \$10,000 IDS system where there is a minimal amount of classified material and no secure room)
- Once analysis is completed - prioritize options and prepare recommendation for decision maker
- Objective - Make decisions about security programs that can be justified in terms of the risk involved and the consequences of inaction

(In doing the risk management one option is to assign values and set up a matrix for the various areas you are analyzing in order to arrive at recommendations for decision maker)

5. Advantages to the risk management process

- Allows an educated evaluation of the probability of loss, compromise or damage and its *impact* as a guide to taking action
- Creates a *baseline* that can be built on or changed as the command's mission, manning, holdings and or/location may change
- Allows the decision maker to make an *informed* decision because of data provided to achieve the best security at a cost the command can afford

G. Special Types of Control Measures (ISP 7-8)

1. Naval Warfare Publications (NWPs)

- NWPs, both classified and unclassified, have their own system for administrative control under NTTP 1-01, Naval Warfare Library
- Classified NWPs will be safeguarded according to their classification level.
- Administrative requirements of NTTP 1-01 do not

replace the security controls required for classified information (i.e., classified NWP are considered classified documents first for control purposes and then NWP)

- NWP Custodian - Exercises control over receipt, correction, stowage, security, accounting, distribution and authorized destruction of all NWP

2. North Atlantic Treaty Organization (NATO)
 - a. Requires formally granted NATO access and briefing
 - b. Controlled and safeguarded per USSAN 1-69, Implementation of NATO Security Procedures
 - c. NATO Control Officer - Ensures that NATO information is correctly controlled and accounted for and that NATO procedures are observed
3. FGI Information (except NATO) - Control and safeguard in same manner as prescribed for U.S. classified information (Exceptions ISP 7-8)
4. Control and safeguard other types of classified information and material per the directives that are specific to that material as listed in ISP 7-8.

H. Recovery of Classified Information on Death or Desertion

1. Suicide or attempted suicide of personnel with access to classified information (**PSP 3-4**)
 - Commanding Officer will immediately forward all Available information to nearest NCIS office, with copy to DON CAF. NCIS will coordinate investigative action with Commanding Officer
 - Report to NCIS and DON CAF will describe nature and extent of classified information to which the individual had access and circumstances surrounding incident

2. Unauthorized Absentees With Access to Classified Information **(PSP 3-5)**
 - Commanding Officer will conduct inquiry to determine if there are any indications that absence contrary to interests of national security
 - If concerns developed, command will report all pertinent information to nearest NCIS office with copy to DON CAF; NCIS will advise whether or not they will conduct an investigation
3. Death or Desertion of Personnel with Access to Classified Information **(PSP 3-6)**
 - Commanding Officer must identify any unusual indications that may be contrary to interests of national security
 - If any unusual indications are developed, report all pertinent information to nearest NCIS office

I. Reproduction of Classified Information (ISP 7-15)

1. Reproduce classified information only to extent required by operational necessity unless restricted by originating agency or statutes/directives
2. Commanding Officers shall:
 - Designate specific equipment for classified reproduction (see figure 5.1-1)

COPIER WARNING

THIS MACHINE MAY BE USED FOR REPRODUCTION
OF CONFIDENTIAL AND SECRET INFORMATION

COPIER WARNING

THIS MACHINE IS NOT AUTHORIZED FOR THE
REPRODUCTION OF CLASSIFIED INFORMATION

Figure 5.1-1. Sample copier warnings.

- b. Ensure all copies are subject to same controls as the original information
 - c. Limit reproduction to that which is mission essential
 - d. Facilitate oversight and control of reproduction
3. Reproduction Equipment
- Select, if possible, reproduction equipment that does not have an internal hard drive or non-volatile memory
 - If equipment has memory then it must be protected at highest level of classified material reproduced
 - If networked to other IT systems or equipment, whole network must be provided security protection and approved to process classified material at highest level of classified material produced
 - Before permitting uncleared maintenance personnel access to or releasing reproduction equipment that has been used for processing classified material, inspect equipment to ensure that no classified material has been left in the equipment
- (The same guidance applies to printers and Scanners)
- Follow good clean-up procedures: Safeguard and promptly destroy classified waste; Check area to ensure all classified material removed and ensure original and copies have been removed; In event of any malfunctions, check for stuck copies; Do not place trash can at final copy end of copier; Check paper path and any hidden bins to ensure no residue remains in copier; Double sided copiers, ensure no residue remains in bin