

LESSON TOPIC 5.5**Safeguarding****REFERENCES**

SECNAV M-5510.36, Chapters 7 and 10
OPNAVINST 5530.14E, Physical Security and Loss Prevention
SECNAVINST 5430.107, Mission and Functions of the Naval Criminal
Investigative Service
SECNAVINST 3850.4, DON Technical Surveillance Countermeasures
(TSCM) Program

LESSON**A. Basic Policy (ISP 7-1)**

1. Classified information will be processed: In secure facilities; on accredited IT systems; and under conditions which prevent unauthorized persons from gaining access to it - to include properly security it when not under direct control of cleared individual
2. Commands must carefully balance need for operational efficiency and cost of exceeding minimum security requirements (see figure 5.5-1)

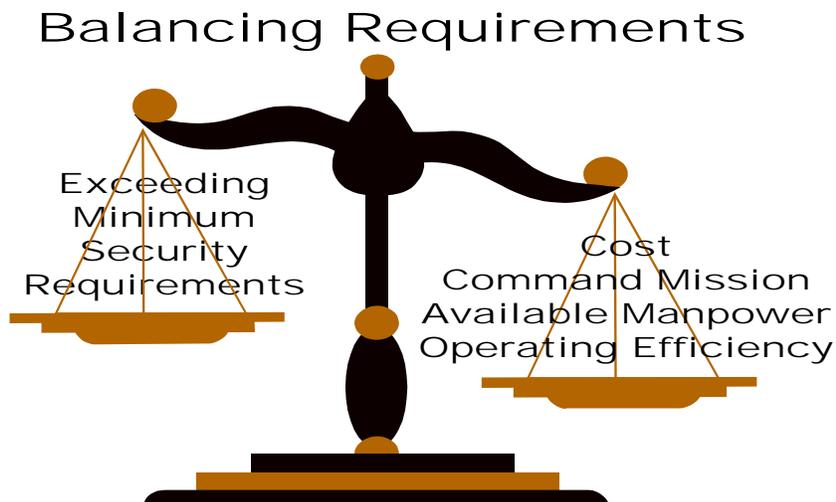


Figure 5.5-1 Balancing requirements

3. Ensure that controlled unclassified information (CUI) is safeguarded from unauthorized access by the public. Take measures to protect IT systems which store, process, and transmit such information from unauthorized access
4. Classified information is the property of the U.S. government and not personal property
5. Responsibilities for safeguarding
 - Anyone in possession of classified information must safeguard it at all times and secure it when not in use or under direct supervision of authorized persons
 - Custodian Responsibilities: Ensure no unauthorized persons gain access, need-to-know established before releasing, obtain command approval before removing from designated area, and ensure removal is in performance of official duties and under conditions providing required protection
6. Safeguarding U.S. classified information in foreign countries - Safeguard at a U.S.: **(ISP 7-14)**
 - a. Military installation or where U.S. enjoys extraterritorial status (e.g. embassy/consulate)
 - b. Government activity located in a building:
 - Used exclusively by U.S. government tenants, provided it is under 24-hour control by U.S. government personnel, or
 - Not used exclusively by U.S. government tenants nor under host government control, provided classified information is stored in GSA-approved security containers and under 24 hour control by U.S. government personnel, or
 - Not used exclusively by U.S. government tenants but which is under host government control, provided classified information is secured in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access

NOTE: To extent possible separate U.S. classified information determined releasable to the host government from that not authorized for release.

Foreign personnel shall be escorted in areas where U.S. non-releasable classified information is handled or stored

B. Care of Working Spaces

1. Buildings and spaces - Must have the security measures necessary to prevent unauthorized persons from viewing or hearing classified information
2. Measures which can be used for buildings: Trim shrubbery outside ground-floor offices; Install grills/bars/screens on ground-floor (below 18') windows and other openings; Use window coverings (opaque windows)
3. Conference rooms and other areas designated for classified discussions
 - a. For Top Secret and other designated classified discussion areas, request Technical Surveillance Countermeasures (TSCM) support from NCIS. Once TSCM is complete: **(SECNAVINST 3850.4)**
 - Ensure continuous access control to space once it has been surveyed
 - Require escorts for uncleared personnel who need admission
 - Monitor telephones, office intercommunications, public address systems, or other equipment, which has not been checked by a TSCM technician in the space.
 - b. TSCMs are not normally supplied to ships or aircraft due to the low technical security vulnerability and threat
 - c. Because most commands do not have TSCMs, the security manager needs to:
 - Check room periodically for listening devices
 - Allow no cell phones, personal radios, TVs, or recording devices in classified discussion areas
 - Monitor activities of uncleared personnel (e.g., maintenance people)
 - Report any attempts or suspected attempts of penetration to NCIS
 - d. Keep extraneous information (e.g., unclassified

papers, printouts, publications) off the top of security containers to prevent inadvertent intermingling with classified information

C. Restricted Areas (OPNAVINST 5530.14E, Chapter 2)

1. A command with areas of varying security importance may require different protective measures, depending on: Mission; Volume of material; Type of equipment used to process classified information; Sensitivity of information used; Environment
2. Purpose - An effective method to restrict access and control movement. Requirement for all levels:
(OPNAVINST 5530.14E)
 - a. Designated in writing by Commanding Officer
 - b. Post Restricted Area warning signs at normal points of ingress/egress (If located in a foreign country, the warning signs will be in English and the local language)
 - c. Clearly defined perimeter
 - d. Admission only to people with appropriate authorization and others controlled by escort
 - e. A personnel identification and control system
 - f. Entry and departure controlled
 - An electronic control system may be used
 - Use of access controls (e.g., mechanical push-button combination locks) allows authorized movement, while detecting and delaying unauthorized movement of personnel and information
 - If a computer access control or logging system is used, it must be safeguarded against tampering.
 - g. Secured during non-working hours and checks made for signs of unauthorized entry
3. Level 2 additional requirements
 - After duty hours all personnel must be logged in and out

- When secured check at least twice per 8-hour shift or if adequately equipped with an operational IDS, check once per 8-hour shift

4. Level 3 additional requirements:

a. Access list

b. Entry and departure log:

- During normal hours - Visitors logged in/out
- After hours - All personnel logged in/out

D. ID Cards and Badges (OPNAVINST 5530.14E)

1. Purpose

a. Control physical access to an area for security purposes.

- Color or symbol coding can help identify level of holder's security access, or indicate special nature of his authorization to enter a Restricted Area
- Do not use the words Top Secret, Secret, or Confidential or their abbreviations

b. Alert other personnel in the area to the presence of unauthorized persons, because such persons are not wearing a badge or are wearing a questionable badge.

2. NCIS Special Agent credentials are acceptable ID for purposes of controlling access through Top Secret.

NOTE: NCIS agents cannot surrender credentials; if surrender is required for badging purposes, other acceptable ID will be exchanged (**SECNAVINST 5430.107**)

3. Rules for coded ID cards or badges

- Echelon 2 commands will approve adequacy of security badges and their manner of use by their subordinate activities.

- Badges should have expiration dates and serial numbers; strict control and accountability required (All new acquisitions of security badge-related components will comply with OPNAVINST 5530.14E)

- Design to minimize tampering or unauthorized use

E. Personnel Administrative Inspections (OPNAVINST 5530.14E)

1. Required in Restricted Areas
2. Purpose - To deter and detect unauthorized introduction or removal of government material
3. Method and frequency at Commanding Officer's discretion. To be effective inspections should be conducted frequently.
(Better to frequently conduct random inspections of a few people at any one time than to inspect a lot of people only infrequently)
 - Not interfere unduly with performance of duties or ingress/egress of employees/visitors
4. Persons should be advised in advance (Properly worded sign to this effect prominently displayed in front of entry point will suffice).
5. Instruct inspection personnel:
 - To inspect only what is necessary and what to do when it appears classified information is being removed or brought in without authorization
 - Command authorization (e.g., authorization letter, visit request, DD 2501, Courier authorization Card, travel order) is required for the removal of classified material

F. Care During Working Hours (ISP 7-9)

1. Protect classified information when removed from storage - Keep under constant surveillance by an authorized person and use a coversheet, Standard Forms 703 (TS), 704 (Secret), 705 (Confidential) when removed from secure storage
2. Removable computer media
 - In a mixed working environment (classified and unclassified) mark removable media with a SF 706 (TS), 707 (Secret), 708 (Confidential), 709, 710 (Unclassified), 711, or 712 (SCI), as applicable (If unable to use SF stickers can write on the classification)

- In a totally unclassified working environment, SF labels are not required

3. Do not discuss classified information in unauthorized areas or when unauthorized persons can overhear
4. Protect drafts, notes, CDs etc.

G. Security Checks at End of Working Day (ISP 7-10)

1. Commanding Officers shall establish procedures for end of the day security checks
2. Use the SF 701, Activity Security Checklist (see Student CD for form), to ensure all areas which process classified information are properly secured. Post the SF 701 near exit. (Can be annotated to add additional command check off items (e.g., coffee pot off))
3. Use the 702, Security Container Check Sheet to record that vaults, secure rooms, and security containers have been properly secured

- Each time a container, vault, or secure room is opened and closed
- At the end of the day (second check)
(Attach SF 702 to the container)

(When securing, rotate dial of mechanical combination locks at least 4 times in same direction; check each drawer by depressing latch and pulling on drawer. Rotate the dial of the XO series locks at least one turn in each direction. (If the dial is only a quick twist, it is possible to open most locks merely by turning the dial back to its opening position) **(ISP 10-14)**

4. Ensure the SF 701 and 702 reflect after hours, weekend or holiday activity in secure areas (Security managers should check records regularly to ensure proper use)
5. The SF 701 and 702 may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation.