

LESSON TOPIC 3.1**Classification Management****REFERENCES**

SECNAV M-5510.36, Chapters 4 and 5
EO 12958, As Amended, Classified National Security Information
OPNAVINST 5513 series, DON Classification Guides

LESSON**A. Limitations on Classifying or Reclassifying (ISP 4.1, 4.2 and 4.11)**

1. Purpose: Designate information for which unauthorized disclosure could be expected to result in a specific level of damage to national security
2. May NOT be used to: Conceal violations of law, inefficiency or administrative error; Prevent embarrassment to a person, organization or agency; Restrain competition; To prevent or delay the release of information that does not require protection in the interest of national security.
3. Classification Levels (and expected damage to national security of unauthorized disclosure): Top Secret (Exceptionally Grave); Secret (Serious); Confidential (Damage)

B. Original Classification (ISP 4.2 - 4.4)

1. Initial decision that information could be expected to cause damage to the national security if subjected to unauthorized disclosure
2. Authority rests with the Secretary of the Navy (SECNAV) and officials delegated the authority (Original Classification Authorities (OCAs))
 - Information classified by OCAs is codified in Security Classification Guides and shall be declassified as soon as it no longer meets standards for classification in interests of national security
 - OCA authority is not transferable or delegated (Exception: If OCA absent for extended periods time

and an emergent need requires OCA action, it may be judiciously exercised by individual officially designated to act in OCA's absence)

- Only the current incumbents of the positions listed in SECNAV M-5510.36 exhibit 4A have Original Classification Authority (See for updates - www.ncis.navy.mil/securitypolicy)

- OCAs are responsible for notifying holders of any classification changes involving their information

3. **OCA Training (ISP 4.4 and 4.6 and CNO ltr 5510 ser N09N2/9U223112 of 7 May 09, Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36)**

- OCAs must receive indoctrination training (prerequisite to exercising authority) and annual refresher OCA training

OCA training can be found on the website <https://stepp.dss.mil> under Information Security courses

4. **Security Classification Guide (SCG) - Approved personally by an OCA with program or supervisory responsibility (ISP 5-1 through 5-5)**

- Prepared for each DON system, plan, program, or project, in writing and specified OPNAVINST 5513.1 series format (OCAs - Provide DOD Security Classification Guide Data Elements (DD Form 2024) to DUSN(PPO&I) with each submission of new, revised or canceled SCGs

- Identify the security classification level and duration of classification for all information elements and reviewed for accuracy and completeness at least every 5 years

- Distributed to commands consistent with their command missions in OPNAVINST 5513.1 series

- Office of the Secretary of Defense (OSD) issues SCGs for systems, plans, programs, or projects involving more than one DoD component (**ISP 5-5**)

- Retrieval and Analysis of Navy Classified Information (RANKIN) Program - Provides standardization,

centralized management and issuance for all DON SCGs
(Managed by DUSN(PPO&I))

- f. Uniformly formatted SGCs are issued in the following major subject categories: **(ISP 5-3)**

OPNAVINST 5513.1 (DON SCGs (Responsibilities))
OPNAVINST C5513.2 (Air Warfare Programs)
OPNAVINST S5513.3 (Surface Warfare Programs)
OPNAVINST S5513.4 (General Intelligence, Cover and Deception, Security and Investigative Programs)
OPNAVINST S5513.5 (Undersea Warfare Programs)
OPNAVINST S5513.6 (Communication and Satellite Programs)
OPNAVINST S5513.7 (Mine Warfare Programs)
OPNAVINST S5513.8 (Electronic Warfare Programs)
OPNAVINST S5513.9 (Nuclear Warfare Programs)
OPNAVINST S5513.10 (Advanced Technology and Miscellaneous Programs)
OPNAVINST 5513.11 (Ground Combat Systems)
OPNAVINST S5513.12 (Intelligence Research Projects)
OPNAVINST 5513.13 (Non-Acoustic Anti-Submarine Warfare (NAASW) Programs)
OPNAVINST 5513.15 (Naval Special Warfare Programs)
OPNAVINST 5513.16 (Declassification of 25 Year Old DON Information)

5. Classification Criteria - OCAs must determine the information is under U.S. government control, concerns one of the following subjects and the threat of damage to national security: **(ISP 4-7, EO 12958, As Amended)**

- Military plans, weapon systems, or operations
- Foreign government information
- Intelligence activities, intelligence sources or methods or cryptology
- Foreign relations or foreign activities including confidential sources
- Scientific, technological or economic matters includes defense against transnational terrorism relating to national security
- Vulnerabilities or capabilities of systems, Installations Infrastructures, projects, plans or protection services, include transnational terrorism national security
- Weapons of mass destruction

- Safeguarding nuclear materials or facilities
- 6. Declassifying and Downgrading - Can eliminate or reduce costly control measures because it: Frees classified storage containers; Allows less expensive transmission; Requires less control; Allows easier destruction
- 7. Duration of Classification (**ISP 4-8**)
 - OCAs shall establish a date or event for declassification that is 25 years or less from the date of the original classification decision (The 10 year exemption from automatic declassification categories (X1 through X8) has been eliminated)
 - OCAs may specify duration of classification beyond 25 years only when originally classifying information: Could be expected to reveal the identity of a confidential human source or human intelligence source (50X1-Human), or that has been the subject of an Information Security Classification Appeals Panel (ISCAP) approved exemption
 - If OCA believes longer protection is required for information assigned a declassification date or event of less than 25 years - OCA may extend duration up to 25 years
- 8. Changing Classification Levels - Can only be done by an OCA with jurisdiction over the classified information and all holders shall be notified
- 9. Reclassification of Information (**ISP 4-11**)
 - Information released without proper authority may remain classified if cognizant OCA makes such determination
 - Information previously declassified and officially released can be reclassified by SECNAV and only under certain circumstances

C. Derivative Classification (ISP 4-9)

1. Definition: The incorporating, paraphrasing, restating, or generating, in new form, information that is already. (Over 99% of DON classified decisions are derivative)

2. When derivatively classify, may use a SGC, but will also use other sources such as: Correspondence; Messages; Publications; Operational Plans; Operational Orders; Naval Warfare Publications; Tactical Memos/Notices
3. A derivative classifier must:
 - Be trained (training is available on <https://stepp.dss.mil> (under Information Security Courses) **(ISP 3-3)** (If assigned a SIPRNET account need to receive derivative classifier training)
 - Observe and respect the original (source) classification determinations
 - Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification may have been changed in the process
 - Carry forward to a new document all applicable classification and associated markings
4. Original and derivative classifiers (along with those who exercise command signature authority) are accountable for accuracy of classification decisions and for applying proper classification markings **(ISP 4-10)**

D. Tentative Classification (ISP 4-14)

1. Avoid over classification - if there is a reasonable doubt about the need to classify, don't classify
2. If drafting a document and there is concern information may possibly be classified, but have no source document or SCG to verify it - contact the originator or OCA (See ISP Chapter 4 for guidance)

E. Classification Challenge (ISP 4-12)

1. Holders of classified information are encouraged and expected to challenge the classification of information which they, in good faith, believe to be improperly classified
2. Contact command security manager or classifier of the information to resolve the issue. Procedures to use:

Refer to a security classification guide; Safeguard information at the level specified or recommended, whichever is higher; Consult with originator or OCA informally to clarify the issue and resolve it if possible prior to submitting a formal challenge; Prepare a formal challenge per para 4-12.3, ISP

F. Foreign Government Information (FGI) (ISP 4-17)

1. Retains its classification level or is assigned a U.S. equivalent level (see ISP Exhibit 6C for equivalent foreign security classifications) (Authority to assign a U.S. classification equivalent does not require OCA)
2. Foreign Government Unclassified and RESTRICTED information provided with the expectation that it will be afforded a degree of protection at least equivalent to that required by that government

G. Automatic Declassification (ISP 4-20)

1. All 25 year old historically valuable classified records will be automatically declassified on 31 December 2006, whether or not the records have been reviewed
2. Subsequently all classified records shall be automatically declassified on 31 December of the year that is 25 years from the date of original classification, unless the records have been reviewed and exempted
3. Declassified documents will not be released to the public until a public release review is conducted

H. Mandatory Declassification Review (ISP 4-22)

1. Any individual or organization may request a review for declassification
2. The responsible DON organization upon receipt of such a request shall conduct a review if the information: Is described in the request with enough specificity to allow it to be located with a reasonable amount of Effort; Is not exempted from search and review, see para 4-22 ISP; Has not been reviewed within the past 2 years
3. If the information has been reviewed within 2 years or

is the subject of pending litigation, the requester shall be notified, and advised of their appeal rights