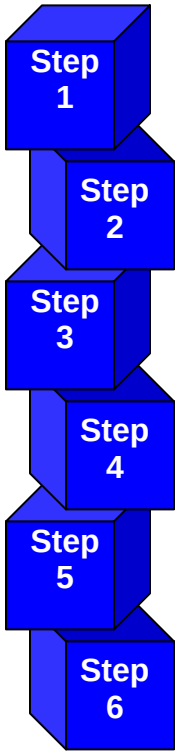
Defense Security Service Academy

OCA Desk Reference Guide



May 2007

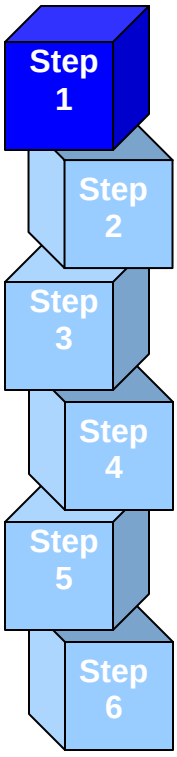
OCA Decision Aid

The safety and security of the United States depend upon the protection of sensitive information. Classification is one way to accomplish this protection. Original classification is the initial decision that particular information requires protection in the interest of national security and could be expected to cause damage if subjected to unauthorized disclosure. It is a six-step process in which the classifier must answer specific questions at each step and make considerations and decisions before classifying information. This desk reference guide is designed to provide individuals with the six-step decision process to enable the OCA to make quality classification decisions.

OCAs, also called original classifiers, include the President, Vice President, Secretary of Defense, the Secretaries of the Military Departments, and other officials within DoD who have been specifically delegated this authority in writing.

When Original Classification Authority is granted, OCAs are delegated classification authority specific to a level of classification and cumulative downwards. For example, an OCA appointed with Top Secret classification authority may classify information at the Top Secret, Secret, and Confidential levels. An OCA appointed with Confidential classification authority may only classify information at the Confidential level.

OCAs may only classify information that is under their area of responsibility such as a specific project, program, or type of operation. For example, it would not be appropriate for an air wing commander to classify information about a Navy undersea warfare program.



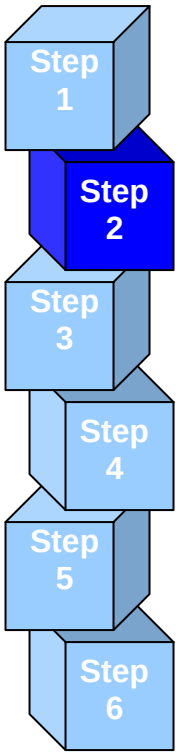
1. Determination If Official Government Information

The OCA must determine if the information being considered for classification is official. “Official” in this context is defined as information owned by, produced by or for, or under the control of the U.S. Government. Without the government having some proprietary interest in the information, classification is not an option. If the information is not official, the process stops at Step 1, as the information would not be eligible for classification. The government would have to acquire proprietary interest before information could be classified.

Defining information as "official" is not always clear. Some information may fall within the criteria of the Patent Secrecy Act of 1952 and/or may require guidance from your Government legal counsel.

For additional information on secrecy of certain inventions and withholding of patents you may refer to 35 U.S.C. 181 Secrecy of certain inventions and withholding of patent, located on the Original Classification Multimedia Overview under "Resources".

If the information is official, the OCA would move to Step 2 in the decision process.



2. Determination Of Eligibility For Classification

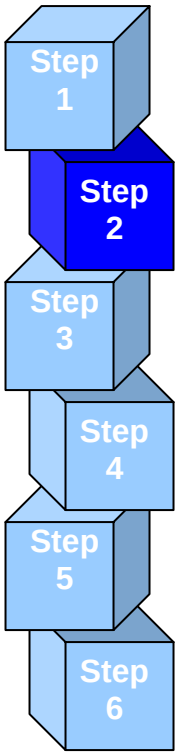
The OCA must consider if the information is eligible for classification, and if eligible, determine if the information is limited or prohibited from being classified.

a. Eligibility for classification

The OCA must determine if the government information is eligible for classification. Eight categories of information currently identified in the E.O. 12958, as amended, can be considered for classification:

- Military plans, weapons systems, or operations
- Foreign government information
- Intelligence activities (including special activities), intelligence sources or methods, or cryptology
- Foreign relations or foreign activities of the United States, including confidential sources
- Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
- U.S. Government programs for safeguarding nuclear materials or facilities
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
- Weapons of mass destruction

If the information under consideration for classification cannot be placed in one or more of the eight categories, it cannot be classified.



Determination Of Eligibility For Classification

(continued)

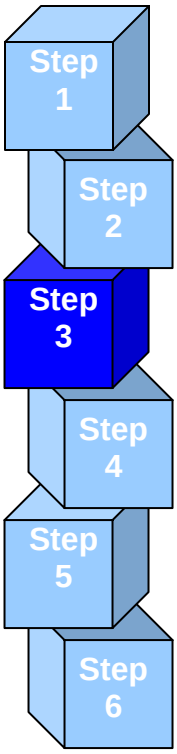
b. Classification prohibitions and limitations

Once information has been determined eligible for classification, the OCA must determine if the information is limited or prohibited from being classified. E.O. 12958, as amended, specifically prohibits classification of information for the purposes of:

- Concealing violations of law, inefficiency, or administrative error
- Preventing embarrassment to a person, organization, or agency
- Restraining competition
- Preventing or delaying the release of information that does not require protection in the interest of the national security

Limitations to classifications include:

- Basic scientific research information not clearly related to the national security shall not be classified
- Information may be reclassified after declassification and released to the public under proper authority only in accordance with the following conditions:
  - The reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security
  - The information may be reasonably recovered
  - The reclassification action is reported promptly to the Director of the Information Security Oversight Office
- Information not previously disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 442a), or the mandatory review provisions described in sections 3.5 and 5.4 of E.O. 12958, as amended.

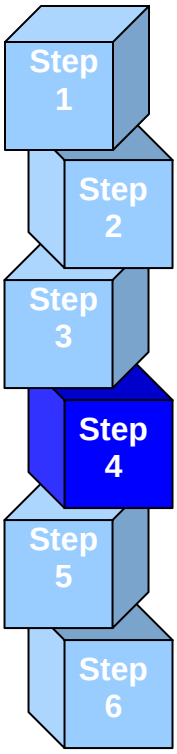


3. Determination Of The Impact On National Security

Another essential decision the OCA must make before they can say, “The information has been classified,” is to determine the potential for damage to national security if unauthorized release occurs. If it is determined that there is no potential for damage to the national security, the information will not be classified. If there is potential for damage to national security and the information is determined eligible for classification as defined in Step 2, the information is then determined classified.

While it is not required to prepare a written description of the potential for damage to the national security before the information can be classified, the OCA must be able to defend their decision and identify or describe the potential damage if their decision is questioned or challenged. It is recommended that the OCA put this justification in writing at the time the decision is made so when another person assumes their OCA responsibilities, that person will have proper information.

The OCA must also consider both the impact of classification itself; overclassification could potentially impede the operational effectiveness of entities which need the information to complete their mission, and the possibility of protection. If classification is applied or reapplied, there must be a reasonable possibility that the information can be provided protection from unauthorized disclosure.

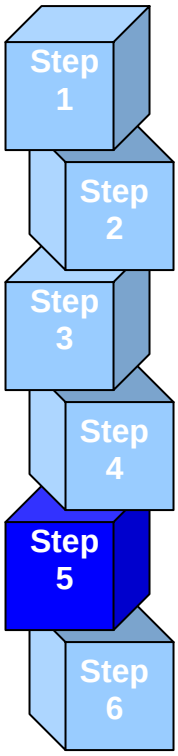


4. Designation Of Appropriate Classification Level

The OCA must evaluate the impact of classification in order to identify the appropriate classification level. The OCA must determine how sensitive the information is, what the potential damage to national security would be if the information was not protected, and assign a classification level based on that determination. The OCA must use reasoned judgment to consider the extent of potential damage.

The classification levels are defined in relation to their potential damage to the national security.

- If unauthorized disclosure of the information could reasonably be expected to cause exceptionally grave damage to the national security, it should be classified as TOP SECRET.
- If unauthorized disclosure of the information could reasonably be expected to cause serious damage to the national security, it should be classified as SECRET.
- If unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, it should be classified as CONFIDENTIAL.



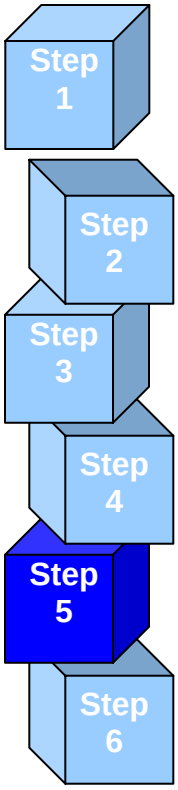
Determination of Classification Duration

After determining the level of classification, the OCA must determine the duration of classification. This involves reviewing the level of classification to determine downgrading requirements and declassification, where it is determined that information no longer requires classification.

Downgrading: The OCA must evaluate the information to determine if there is a specific date or event in the future where the potential for damage to the national security diminishes to a point that will enable the classification level to be lowered. If the sensitivity of the information changes, the OCA will need to assign a date or event when downgrading can take place. If the OCA determines that sensitivity will not decrease or cannot make a determination on decreased sensitivity, then the OCA will proceed to determine the declassification instructions.

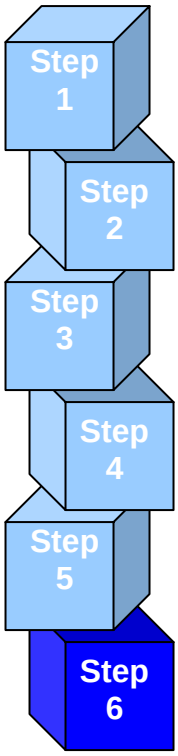
Declassification: The OCA must make declassification determinations for all classification decisions. When considering the duration of classification, the OCA must follow these guidelines:

- If the OCA knows of a date within ten years where the potential for damage from compromise is no longer a concern to the national security, then that date is assigned as the declassification date.
- If the OCA cannot determine a date, but can identify an event that is expected to occur within the next ten years where the potential for damage from compromise is no longer a concern to the national security, then that event is assigned as the declassification instruction.
- If the OCA determines that information requires protection beyond ten years of the original classification, the OCA may assign a date or event up to but not exceeding twenty-five years from the date of the original decision.
- Human intelligence exemption – An OCA shall apply the “25X1-human” exemption with no date of declassification when classifying information that could be expected to reveal the identity of a confidential human source or human intelligence source. Only OCAs having jurisdiction over such information may use this designation.



Determination of Classification Duration (continued)

- In rare cases, other 25X exemptions may apply. Such exemptions must be approved through the Interagency Security Classification Appeals Panel (ISCAP). ISCAP approval for 25X exemptions must be requested via the chain of command.
- The 25X markings other than "25X1-human" are applied when information is exempt from 25-year automatic declassification, and cannot be used unless the specific information has been approved through the ISCAP, generally in the form of a declassification guide. Such information must be incorporated into classification guides. The classification guide would include the specific element of information and the level of classification. (Two examples of how to do this would be "25X4, October 10, 2040" or "25X4, 20401010.") When the 25X marking is applied, the "Declassify on" line would include the symbol "25X" plus a brief reference to that category or categories in section 3.3(b) of E.O. 12958, as amended, and the new date or event for declassification. For a complete list of the exemptions, refer to E.O. 12958, as amended.
- Information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data [RD] and Formerly Restricted Data [FRD]) is exempt from declassification requirements. For RD, classification decisions are codified in Department of Energy (DoE) Classification Guides. For FRD, classification decisions are documented in Joint DoE/DoD Classification Guides.



6. Providing and Communicating Guidance for Derivative Classification

The OCA's final step in the original classification decision process is to designate the information as classified and communicate the decision. There are three methods for communicating the decision.

- Security classification guides
- Properly marked source documents
- Outline classification instructions on a DD Form 254, DoD Contract Security Classification Specification

The preferred method for communicating classification decisions is to communicate it through a security classification guide.

The least common method for communicating the decision is to outline classification instructions on a DD Form 254. The DD Form 254 identifies all security requirements and guidance. This is rarely used and may occur when a contract must be put into place and needs classification instructions, but a classification guide is not available.

Once the decision is communicated, the decisions will be used by others who must work with the information to make proper derivative classification decisions and assure the information is properly protected from unauthorized disclosure. It is vital that OCAs communicate their decisions effectively.