CDSE

JOB AID

Original Classification Authority (OCA) Desktop Reference

NOVEMBER 2019

Table of Contents

Original Classification Authority (OCA) Decision Aid

The safety and security of the United States (U.S.) 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. CDSE packaged the standard process into six digestible steps 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 the Department of Defense (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 under their area of responsibility, such as a system, plan, program, project, or mission. For example, it would not be appropriate for an air wing commander to classify information about a Navy undersea warfare program.

Step 1: Determination of 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 United States Code 181, "Secrecy of Certain Inventions and Withholding of Patent.

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

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

The eight categories of information currently identified in Executive Order (E.O.) 13526 that can be considered for classification are:

- Military plans, weapons systems, or operations
- Foreign government information
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology
- Foreign relations or foreign activities of the U.S., including confidential sources
- Scientific, technological, or economic matters relating to national security
- U.S. Government programs for safeguarding nuclear materials or facilities
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
- Development, production, or use of weapons of mass destruction

Determine the information has not already been classified by another OCA.

Determine that classification guidance is not already available in the form of security classification guides, plans, or other memorandums. Within the DoD, the majority of existing classification guidance is indexed and promulgated via the Defense Technical Information Center (DTIC), available at www.dtic.mil.

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. In accordance with E.O. 13526, information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of national security

Limitations to classifications include:

- Basic scientific research information not clearly related to national security shall not be classified.
- Information that has been declassified and released to the public under proper authority may be reclassified only when the information may be reasonably recoverable without bringing undue attention to the information. This means that:

    1. Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from them.
    2. If the information has been made available to the public via means such as U.S. Government archives or reading rooms, it can be or has been withdrawn from public access without significant media or public attention or notice.

- DoD Component Heads other than the Secretaries of the Military Departments shall submit recommendations for reclassification of information under their jurisdiction to the Secretary of Defense through the Under Secretary of Defense (Intelligence). Recommendations for reclassification must include, on a document-by-document basis:

    1. A description of the information.
    2. All information necessary for the original classification decision in accordance with E.O. 13526, including classification level of the information and declassification instructions to be applied.
    3. When and how it was released to the public.
    4. An explanation as to why it should be reclassified. Include the applicable reason in accordance with E.O. 13526 and describe what damage could occur to national security. Also describe what damage may have already occurred as a result of the release.
    5. The number of recipients and/or holders and how they will be notified of the reclassification.
    6. How the information will be recovered.
    7. Whether the information is in the custody of the National Archives and Records Administration (NARA) and whether the Archivist of the U.S. must be notified of the reclassification.

Step 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 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 can be classified.

While it is not required to prepare a written description of the potential for damage to 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 the impact of classification itself, how over-classification could potentially impede the operational effectiveness of entities that 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 protected from unauthorized disclosure.

Step 4: Determine 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 national security:

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

Step 5: 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 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 can determine a date within ten (10) years where the potential for damage from compromise is no longer a concern to 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 (10) years where the potential for damage from compromise is no longer a concern to 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 (25) years from the date of the original decision.
- Human intelligence exemption – An OCA shall apply the "50X1-HUM" exemption with no date of declassification when classifying information that could be clearly and demonstrably 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.
- Weapons of Mass Destruction exemption – An OCA shall apply the "50X2-WMD" exemption with no date of declassification when classifying information that could be clearly and demonstrably expected to reveal the development, production, or use of weapons of mass destruction. Only OCAs having jurisdiction over such information may use this designation.
- Guides containing RD or FRD topics must be coordinated with DoE. Note also that RD and FRD are never automatically declassified and such information must not include declassification instructions.

Step 6: Providing & 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 two methods for communicating the decision.

- Security classification guides
- Properly marked source documents

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

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.