

## Student Guide

### Short: Requirements for OCAs

<b>Objective</b>	Identify the annual training requirements for original classification authorities (OCAs) as specified in E.O. 13526
<b>POC</b>	<a href="mailto:InformationSecurity.Training@dss.mil">InformationSecurity.Training@dss.mil</a>
<b>Estimated completion time</b>	10 minutes

#### Overview

On December 29, 2009, President Obama signed Executive Order 13526 – “Classified National Security Information.” This Executive Order calls for a uniform system for classification, safeguarding, and declassification of national security information. According to this Executive Order, as an Original Classification Authority, or OCA, you must receive training in these topics at least once per calendar year. This annual training is required; failure to complete it could result in suspension of your classification authority until you do so.

#### Refresher Training Topics

To complete your OCA annual training requirement, you must review the following topics: proper classification, including the avoidance of over classification; proper safeguarding of classified information; declassification; and sanctions.

##### 1. Classification

There are a few things to remember about classification. As you know, if there is any significant doubt about the need to classify information, the information should not be classified. Similarly, if there is any significant doubt about the appropriate level of classification, the information should be classified at the lower level. Even with this requirement to err on the side of a lower classification, remember that unauthorized disclosure of classified information does not mean it automatically becomes unclassified.

There are also a few things to remember about delegated classification authority. First, delegations of original classification authority must be limited to the minimum needed to administer the requirements in E.O. 13526. Delegated officials must have a demonstrable and continuing need for the authority and OCAs may not redelegate this authority to their subordinates. Once an OCA is authorized to classify information at a

specified level, however, he or she is also authorized to classify information at a lower level.

## **2. Safeguarding**

When it comes to safeguarding classified information, there are a few details to review. First, remember that individuals may access classified information only if a favorable determination of eligibility for access has been made, the individual has signed an approved nondisclosure agreement, and he or she has a need to know the information.

Once access is granted, individuals with access must protect classified information by securing it in approved storage containers or facilities when it is not in use, by meeting safeguarding requirements as prescribed in DoD 5200.1-R, and by ensuring that the classified information is not communicated in a manner that would allow it to be inappropriately disclosed. It should not be sent over unsecured voice or data circuits, discussed in public places, or transmitted in any other unsecured manner.

Finally, remember there are restrictions on removing and sharing classified information. Classified information may be shared with other government agencies, even without originating agency consent, as long as the criteria from E.O. 13526 are met. Individuals, however, must not take classified information from official agency premises without proper authorization. Finally, officials or employees leaving agency service may not remove classified information, or declassify the information in order to remove it.

## **3. Declassification**

As you know, at the time of original classification, OCAs must also establish a specific date or event for the declassification of information. Information will be automatically declassified when it reaches this date or event, except for information that might reveal the identity of a confidential human source or a human intelligence source, or key design concepts for weapons of mass destruction.

Review the options for declassification shown here:

- A date or event 10 years from original classification
- A date or event up to 25 years from original classification
- 25X1 through 25X9, with a date or event
- 50X1–HUM or 50X2–WMD, or Information Security Oversight Office (ISOO)-approved designator reflecting the Interagency Security Classification Appeals Panel (ISCAP) approval for classification beyond 50 years

For additional guidance on exemptions, please refer to Executive Order 13526 and Information Security Oversight Office, or ISOO, Directive 1.

## 4. Sanctions

As you know, government officers, employees, contractors, and others charged with the safeguarding of classified information, are subject to sanctions if they knowingly, willfully, or negligently disclose classified information to unauthorized individuals. Remember, however, that these individuals are also subject to sanctions if they classify information needlessly, if they create or continue special access programs that aren't required, or if they disregard any other provision of E.O. 13526 or its implementing directives.

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with laws and regulations. At the very least, supervisory officials must promptly remove the classification authority of any individual who shows reckless disregard for the classification standards, or a pattern of errors in the application of these standards.

### The Original Classification Process

You may already be familiar with the six-step process that OCAs follow when determining whether to classify information. If at any step the information does not meet the criteria for classification, the process will terminate and the OCA will not classify the information. You can refresh your knowledge of this process here.

#### Step 1: Is the information official?

Is it:

- Owned by the U.S. Government?

“Owned by” is information that belongs to the U.S. Government.

- Produced by or for the U.S. Government?

“Produced by” is government-developed information. “Produced for” is when the government enters into an agreement through purchase, lease, contract, or receipt of the information as a gift. It covers situations in which the government uses a contractor.

- Under the control of the U.S. Government?

“Under the control” is the authority of the originating agency to regulate access to the information. The contractor, inventor, etc., agrees to have the U.S. Government place it under their control so that the information is eligible for protection through classification. The contractor still retains ownership, but has entrusted the information to the U.S. Government.

**Step 2: Is the information eligible to be classified?**

- Perform an eligibility analysis

**Does the information fall within one of 8 eligible categories?**

1. Military plans, weapons systems, or operations
2. Foreign government information (FGI)
3. Intelligence activities (including covert action), intelligence sources or methods, or cryptology
4. Foreign relations or foreign activities of the United States, including confidential sources
5. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
6. U.S. Government programs for safeguarding nuclear materials or facilities
7. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security.
8. Development, production, or use of weapons of mass destruction

- Determine whether any prohibitions or limitations bar classification

**Information shall not be classified, continue 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 on classification apply to certain types of information:**

- Basic scientific research information not clearly related to national security shall not be classified
- Information may not be reclassified after declassification and release to the public under proper authority, except under certain conditions
- Information not previously disclosed to the public under proper authority may be classified or reclassified if it meets the requirements of E.O. 13526

**Step 3: What is the impact of classifying the information?**

Does unauthorized release create a risk of harm to the national security? **NO** → 

**YES**



Can the information reasonably be protected? **NO** → 

**YES**



What are the costs of classifying the information?

**Step 4: What level of classification is appropriate?**

- Determine how sensitive the information is
- Determine the potential for damage to the national security if the information is not protected
- Assign a classification level to the information:
  - Top Secret
  - Secret
  - Confidential
- Reassess classification assignment when appropriate

**Top Secret**

Top Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to the national security that the Original Classification Authority is able to identify or describe.

**Secret**

Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **serious damage** to the national security that the Original Classification Authority is able to identify or describe.

**Confidential**

Confidential information is information or material of which unauthorized disclosure could reasonably be expected to cause **damage** to the national security that the Original Classification Authority is able to identify or describe.

**Step 5: How long should the information remain classified?**

- Determine downgrading requirements:
  - Assign specific date/event when it will be appropriate to reduce the classification level of information to a lower level
- Determine declassification requirements:
  - Assign date/event within 10 years when potential for damage from compromise is no longer a concern, **OR**
  - Assign date that is exactly 10 years from original classification date, **OR**
  - Assign date up to 25 years from original classification date
  - No information may remain classified indefinitely
  - If information requires classification beyond 25 years, see guidance in E.O 13526, Section 3.3

**Step 6: How does the classification decision get disseminated?**

1. Security Classification Guide
2. Properly marked source document
3. DD Form 254 (For Contractors)

**Additional Resources**

The primary resource on classified national security information is E.O. 13526. You can find additional information and guidance in Information Security Oversight Office, or ISOO, Directive 1, Classified National Security Information, and DoD 5200.1-R, Information Security Program.