Original Classification

Lesson: Course Introduction

Course Information

Welcome to the Original Classification Course.

Purpose: Define original classification and identify the process for determining classification levels in the Department of Defense

Audience: Security professionals, Original Classification Authorities staff

Course Overview

The safety and security of the United States depends on our ability to protect sensitive information.

Original classification is the initial government decision about what information needs to be classified and protected as such. These decisions are important, because they have implications for how that information must be handled and for who may access and use it.

In this course, you will learn about what original classification is, who makes those decisions, and the process those individuals follow in making those determinations.

Course Objectives

Here are the course objectives. Take a moment to review them.

Course Objectives
- Define original classification
- Identify Original Classification Authority requirements and qualifications
- Identify the six steps in the original classification decision process
- Identify limitations and prohibitions on original classification
- Identify the basis for determining classification levels
- Identify the process for determining duration of classification
- Identify authorized sources of classification guidance

Course Structure

This course is organized into the lessons listed here.

Lessons
- Course Introduction

- Original Classification Basics
- Original Classification Authority
- Original Classification Decision Process
- Course Conclusion

Lesson: Original Classification Basics

Introduction

It is in the best interest of national security to legally control the dissemination of very sensitive information.

Executive Order or E.O. 13526 establishes the legal authority for certain officials within the Executive Branch of the Federal government to designate classified national security information.

Original classification is the first step in providing protection to this information. All other classification decisions and safeguarding requirements are based on original classification decisions.

In this lesson, you will learn what original classification is, and will learn some key terms used in the classification process.

Here is the lesson objective. Take a moment to review it.

Lesson Objective:
- Define original classification
    - Distinguish between original classification and derivative classification

Classification Process Overview

Classification is the determination that information requires protection in the interest of national security. The individuals who perform classification are referred to as *classifiers*. When information is classified, it is assigned one of three levels of classification — TOP SECRET, SECRET, or CONFIDENTIAL.

There are two ways information is determined to be classified. One is through original classification, and the other is through derivative classification. Let's look at these two types of classification in greater detail.

Classification rollover: Classification is the act or process by which information is determined to be classified. It is the determination that information requires protection in the interest of national security. When the information is identified, it is assigned one of three levels of classification: TOP SECRET, SECRET, or CONFIDENTIAL.

Classifier rollover: An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an Original Classification Authority (OCA) or a person who derivatively assigns a

security classification based on a properly classified source or a classification guide.

Derivative Classification rollover: Derivative classification is the process of extracting, paraphrasing, restating, or generating in another form, information that is already classified and marking the information to show its classification.

Information rollover: Information is the knowledge that can be communicated, and documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

Original Classification rollover: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification

Original classification is the initial government determination that information needs protection because its disclosure could reasonably be expected to cause identifiable or describable damage to national security.

Classifying information incurs costs for things like security clearances, physical security measures, and countermeasures. Therefore, original classifiers must be careful and consistent in their decision-making in order to minimize cost impact, while ensuring the proper level of classification. If there is significant doubt about the need to classify information, the Original Classification Authority shall not classify the information. In fact, only a limited number of officials are authorized to perform original classification.

These officials must follow a specific process when doing so to ensure the classification is appropriate and reasonable. The officials who perform original classification are referred to as Original Classification Authorities, or OCAs.

Original Classification
What is it?

- Initial determination that information requires protection against unauthorized disclosure in the interest of national security

Who does it?

- ONLY government officials with authority to make original classification decisions

National security rollover: National security is information relating to the national defense or foreign relations of the United

States.

Original Classification rollover: Original classification is an initial determination by an authorized Original Classification Authority (OCAs) that information requires protection because unauthorized disclosure of the information could reasonably be expected to cause damage to national security.

Derivative Classification

Derivative classification is quite different. It is the process of using existing classified information to create new material and marking that newly developed material consistent with the classification markings that apply to the source information.

The individuals who perform derivative classification are known as derivative classifiers. In contrast to original classification, there are a great many individuals who derivatively classify information.

What is it?

- Developing new materials from existing classified information
- Marking the newly developed materials consistent with the classification markings that apply to the source information

Who does it?

- All cleared DoD and authorized contractor personnel who generate or create material from classified sources

Derivative Classification rollover: Derivative classification is the process of extracting, paraphrasing, restating, or generating in another form, information that is already classified and marking the information to show its classification.

Review Activity 1

Try answering this question.

Which statement best defines original classification?

- o The act or process by which information is determined to be declassified
- o The change in status of information from classified to unclassified
- o The process of generating in another form, information that has been classified and marking it to show its classification
- o The initial government determination that information requires protection in the interest of national security

Answer: The initial government determination that information requires protection in the interest of national security

Review Activity 2

Try answering this question.

Question 1 of 2:
A classifier uses information in a TOP SECRET document to general a new document for use in the DoD. The classifier marks the new document "TOP SECRET." What process did this individual just complete?

- Original Classification
- Top Secret Classification
- Derivative Classification
- National Security Classification

Answer: Derivative Classification

Question 2 of 2:
A classifier determines that a report containing certain chemical formulas associated with bio-chemical defense could cause exceptionally grave damage to the national security of the United States if revealed. The classifier classifies the information TOP SECRET. What process did this individual just complete?

- Original Classification
- Top Secret Classification
- Derivative Classification
- National Security Classification

Answer: Original Classification

Lesson Conclusion

In this lesson, you learned some key terms used to describe the classification process. You also learned what original classification is, who performs it, and how it is different from derivative classification.

Original Classification
What is it?

- Initial determination that information requires protection against unauthorized disclosure in the interest of national security

Who does it?

- ONLY government officials with authority to make original classification decisions

Classification rollover: Classification is the act or process by which information is

	determined to be classified. It is the determination that information requires protection in the interest of national security. When the information is identified, it is assigned one of three levels of classification: TOP SECRET, SECRET, or CONFIDENTIAL.
Classifier rollover:	An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an Original Classification Authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.
Derivative Classification rollover:	Derivative classification is the process of extracting, paraphrasing, restating, or generating in another form, information that is already classified and marking the information to show its classification.
Information rollover:	Information is the knowledge that can be communicated, and documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.
National security rollover:	National security is information relating to the national defense or foreign relations of the United States.
Original Classification rollover:	An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.
OCA rollover:	Original Classification Authority An individual authorized in writing, either by the President, the Vice-President, or by agency heads or other officials designated by the President, to originally classify information in the first instance.

Lesson: Original Classification Authority

Introduction

Because the initial decision to classify information is so important, the government grants the authority to perform original classification to only a limited number of officials.

In this lesson, you will learn how they are appointed, the required training before exercising their authority, the level and scope of authority they have, and when and how other individuals may assume their classification duties.

Here is the lesson objective. Take a moment to review it.

Lesson Objective:

- Identify original classification authority requirements and qualifications

OCA Responsibilities

Original Classification Authorities, or OCAs, are responsible for determining when and if information should be classified, the level of that classification, and for determining how long it requires protection.

OCAs are also responsible for communicating those decisions to other individuals who will need to use or store the information.

OCA Requirements

Because their decisions have such an impact, OCAs are senior government officials.

The government grants the authority to originally classify information only when there is a "demonstrable and continuing need" for such authority. That is, there must be a justifiable requirement to perform original classification, and that need must be expected to last over time. As a general rule, classification authority must be exercised an average of twice a year to qualify for retention of the OCA designation if an OCA does not issue and maintain a security classification guide.

In addition, in order for an individual to exercise original classification authority, he or she must have the appropriate level of security clearance and must have received training in the fundamentals of proper security classification to include the avoidance of over-classification.

The individual should also have sufficient expertise and information available to permit effective classification decision-making.

OCA are senior government officials.

Positions with OCA

Original classification authority is not granted to particular individuals in the government, but rather to specific positions.

The positions that have original classification authority include the President of the United States, the Vice President, the Secretary of Defense, and the Secretaries of the Military Departments.

Original classification authority is also granted to certain other officials within the Office of Secretary of Defense, or OSD, and the Department of Defense (DoD). Let's look at how these appointments are made.

Appointing OCAs

The decision to confer original classification authority onto a position in the DoD is based on a specific request for such authority. Requests for original classification authority within the military components need to be submitted based on component guidance. All other DoD activities shall request original classification authority through their activity to the office of the Under Secretary of Defense for Intelligence.

Requests must specify the position title for which the authority is requested, provide a brief mission specific justification for the request, and be submitted through established organizational channels.

When authority is granted to a position, that authority is documented by an appointment letter. The government will grant requests for original classification authority under a specific set of circumstances.

Circumstances popup:	A request for original classification authority will be granted when there is a demonstrable and continuing need to exercise OCA during the normal course of operations and he or she has adequate information and expertise available to make the classification decisions. Requests will be granted only when any existing Security Classification Guides (or SCGs) are insufficient to address the information in question, and when it is impractical to refer decisions to another OCA.

Required Training

OCAs must be trained extensively before they can start exercising their authority to originally

classify information.

All original classification authorities must receive training in proper classification, including the avoidance of over-classification, and declassification at least once a calendar year. The training shall address OCA responsibilities and classification principles, proper safeguarding of classified information, and the criminal, civil, and administrative sanctions that may be brought against an individual.

OCAs must know the answers to these questions:

Classifying Information:
- What is the difference between original and derivative classification?
- Who can classify information originally?
- What are the standards and training requirements that an original classifier must meet to classify information?
- What are the prohibitions and limitations on classifying information?
- Has the information already been classified by another OCA?
- Is classification guidance already available in the form of security classification guides (SCGs), plans or other memorandums?

Duration/Declassification:
- What is the process for determining duration of classification?
- What are the declassification options available to OCAs?
- What are the general standards and procedures for applying declassification instructions?

Marking Classified Information:
- What are the basic portion, banner and classification authority box markings that must appear on classified information?

Communicating Classification Decisions:
- What are the requirements and standards for creating, maintaining, and publishing SCGs?

Safeguarding Classified Information:
- What are the procedures for properly safeguarding classified information?
- What are the criminal, civil, and administrative sanctions that can be imposed for failure to protect classified information from unauthorized disclosure?

SCGs rollover: Security Classification Guides are documentary forms of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

unauthorized disclosure rollover: Unauthorized disclosure is a communication or physical transfer of

classified information to an unauthorized recipient.

OCA Requirements

Once appointed, OCAs are granted classification authority at a specific level of classification and cumulative downwards. For example, an OCA that has TOP SECRET classification authority may classify information at the TOP SECRET, SECRET, and CONFIDENTIAL levels. However, an OCA that has been granted SECRET classification authority may classify information only at the SECRET and CONFIDENTIAL levels.

Jurisdiction

When OCAs are appointed, they are given a specific area of jurisdiction. That is, a specific realm in which they are qualified to make original classification decisions. This may be a particular type of information, such as design information for a new military aircraft. Or it may involve information relating only to a specific project, program, or type of operation.

This jurisdictional limit on authority helps ensure that OCAs are working in their realm of expertise and experience. For example, an air wing commander would not be granted original classification jurisdiction for an undersea warfare program.

Circumstances for Assignment

When an official occupies a position designated as an original classification authority, it does not include the ability to grant that authority to other officials. For example, an official with SECRET original classification authority may not name another official as a SECRET, or even a CONFIDENTIAL, OCA. The reason for this is to reduce the likelihood of conflicting classification guidance caused by unclear or overlapping jurisdiction.

If, however, a person in a position designated as an original classification authority will be unable to perform his or her duties for an extended period, the authority to perform original classification may be assumed by another official. For example, deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to exercise authority when they officially assume the OCA position in an "acting" capacity and have certified in writing that they have received the required OCA training.

Training Certification

Before a subordinate acting in the capacity of an OCA can perform original classification, he or she must certify in writing that he or she has been trained in several key areas. These include OCA responsibilities, classification principles, to include avoidance of over-classification, proper safeguarding of classified information, and the criminal, civil, and administrative penalties for failing to protect classified information from unauthorized disclosure. These records of delegation and training must be maintained by the activity Security Manager.

unauthorized disclosure	
rollover:	Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.

Review Activity 1

Try answering these questions.

An OCA appointed with TOP SECRET classification authority may not delegate SECRET and CONFIDENTIAL classification authority to a subordinate.
Answer: False

If a Security Classification Guide exists to address a specific classification need, an OCA request will be denied.
Answer: True

An OCA request will not be granted if there is another OCA in the chain of comment to which decisions can be referred.
Answer: True

All OCAs must be trained in how to properly mark classified information.
Answer: True

Review Activity 2

How about this question?

An OCA appointed with Secret classification authority may classify information at which of the following levels?

- TOP SECRET, SECRET, and CONFIDENTIAL
- SECRET and CONFIDENTIAL
- TOP SECRET and SECRET
- CONFIDENTIAL

Answer: SECRET and CONFIDENTIAL

Review Activity 3

What must OCA requests contain?

Which of the following must appear in a request for original classification authority?

- □ Brief mission specific justification for the request
- □ Level of security clearance held by the requested OCA
- □ Position title for which the authority is requested
- □ Name of the requested OCA's immediate subordinate

Answer: Brief mission specific justification for the request, Position title for which the authority is requested

Summary

In this lesson, you learned about the responsibilities of an OCA, who they are, how they are appointed, and the training they must undergo. You also learned about the scope of their original classification authority, and the circumstances when it may be assigned to a subordinate.

Original Classification Authority:

- Responsibilities
- Positions
- Appointment criteria
- Training requirements
- Scope of authority
- Assignment to subordinates

Responsibilities rollover:

OCA Responsibilities:

- Determine whether information needs to be classified
- Determine level of classification
- Determine duration of classification
- Disseminate classification decisions to others

Positions rollover:

Positions with OCA:

- President of the United States
- Vice President
- Secretary of Defense
- Secretaries of the Military Departments
  - Secretary of the Army
  - Secretary of the Navy
  - Secretary of the Air Force
- Certain other senior agency officials within DoD

Appointment criteria rollover:

Requests for OCA must:

- Specify the position title
- Present a mission specific justification for the request
- Submit through established organizational channels

Circumstances for granting OCA:

- Demonstrable and continuing need to exercise OCA
- Sufficient expertise and information is available
- Existing Security Classification Guides are not sufficient to address classification needs
- Referral of decisions to existing OCAs is not practical

Training requirements rollover:

Classifying Information:

- What is the difference between original and derivative classification?
- Who can classify information originally?
- What are the standards and training requirements that an original classifier must meet to classify information?
- What are the prohibitions and limitations on classifying information?
- Has the information already been classified by another OCA?
- Is classification guidance already available in the form of security classification guides (SCGs), plans or other memorandums?

Duration/Declassification:

- What is the process for determining duration of classification?
- What are the declassification options available to OCAs?
- What are the general standards and procedures for applying declassification instructions?

Marking Classified Information:

- What are the basic portion, banner and classification authority box markings that must appear on classified information?

Communicating Classification Decisions:

- What are the requirements and standards for creating, maintaining, and publishing SCGs?

Safeguarding Classified Information:

- What are the procedures for properly safeguarding classified information?

- What are the criminal, civil, and administrative sanctions that can be imposed for failure to protect classified information from unauthorized disclosure?

Scope of authority rollover text:

Scope of authority:
- Classification level
- Specific area of jurisdiction

Assignment to subordinates rollover text:

Assignment to subordinates:
- OCA may be assumed by a subordinate only when "acting in the capacity" of the OCA
- Subordinates must provide written certification of required training

Lesson: Original Classification Decision Process

Introduction

Original Classification Authorities, or OCAs, have an important responsibility. To ensure they make effective classification decisions, they must follow a standard process. CDSE packaged the standard process into six digestible steps. The six-step process takes different elements into account at different stages of the process.

In this lesson you will learn how OCAs reach their classification decisions. Here are the lesson objectives. Take a moment to review them.

Original Classification Authority Lesson Objectives:

- Identify the six steps in the original classification decision process
- Identify limitations and prohibitions on original classification
- Identify the basis for determining classification levels
- Identify the process for determining duration of classification
- Identify authorized sources of classification guidance

Overview

Before considering original classification, an OCA must determine whether decisions have already been made about classification of the information. If another OCA has already made an original classification determination, then the information cannot be originally classified again. If the information has not been classified, however, OCAs can proceed with the decision-making process.

The process OCAs follow when determining whether to classify information involves six distinct steps. At each step, if the information does not meet the criteria for becoming classified, the process terminates, and the OCA will not classify the information.

Each step asks a question. First, is the information in question official government information? Next, is the information even eligible to be classified? If so, what harm could be done to national security if the information were revealed?

If the risk of harm to national security is sufficient, the OCA can decide to classify the information. Given the degree of potential damage, what level of classification is appropriate for the information? How long should the information stay protected? And finally, how should the decision to classify the information get communicated to others?

Now let's look at each of these steps in more detail.

Six-Step Process for Original Classification
Step 6 – Guidance
Step 5 – Duration

Step 4 – Designate Classification Level
Step 3 – Impact
Step 2 – Eligibility
Step 1 – Government Information

Step 1: Government Information

Since the OCA must be the one to classify the information, the OCA must first determine whether the information is official. This means the information must be owned by, produced by or for, or under the control of the U.S. Government.

If the government does not have any ownership interest in the information, it cannot be classified, regardless of how sensitive it might be. If the information in question is not official, the classification process stops at Step 1.

Determining if information is "official" is not always simple. In some cases, advice from government legal counsel may be necessary. For example, the Patent Secrecy Act of 1952 allows the Secretary of Defense to determine that disclosure of an invention by granting a patent would be detrimental to national security. DoDM 5200.01, Volumes 1 through 3, the DoD Information Security Program, contain more detail.

Once you determine that the information is "official," you can move to the next step in the decision process.

Owned by rollover:	"Owned by" is information that belongs to the U.S. Government
Produced by or for rollover:	"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 rollover:	"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: Eligibility

Next, the OCA must determine whether the information is eligible to be classified.

This determination actually involves four parts. First, the OCA has to analyze whether the information is eligible for classification. Second, the OCA needs to assess whether there are any prohibitions or limitations on classifying it. Third, the OCA must determine if the information has already been classified by another OCA. And finally, the OCA must determine if classification guidance is already available in the form of security classification guides, plans or other memorandums.

Eligibility popup: The OCA must determine whether the information under consideration is eligible for classification. Executive Order 13526 identifies eight categories of information that are eligible for classification. These categories are fairly broad and general in scope.

If information does not fall into one of these categories, it cannot be classified. However, the fact that information does fit into one or more of the categories does not automatically mean it can be classified. There is more to the analysis. Executive Order 13526 identifies some prohibitions and limitations on the information that can be classified.

Does the information fall within one of 8 categories?

MORE popup: These are the eight categories of information eligible for classification:

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 national security
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. The development, production or use of weapons of mass destruction (WMD)

Prohibitions popup: Once an OCA determines that information is eligible for classification, the next step is to check whether the information is prohibited from being classified. Executive Order 13526 prohibits classification of information for four

specific reasons. In no case shall information 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, restrict competition, or prevent or delay the release of information that does not require protection.

If classifying the information is not prohibited, the OCA may continue with the analysis.

Limitations popup: Even if information is eligible to be classified and there are no prohibitions on classification, the OCA also has to check whether there are any other limitations on classifying it.

Executive Order 13526 identifies some limitations on the types of information that can be classified. An OCA may not classify basic scientific research information that is not clearly related to national security. If information has been declassified and released to the public, it may be reclassified only under certain conditions.

Information not previously released to the public may be classified or reclassified in response to a request for release of that information only in certain cases. If there are no limitations on classifying the information, the information has met all of the criteria required in Step 2 - Eligibility.

MORE popup: Information that has been declassified and released to the public may be reclassified only when:

- The reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security
- The information may be reasonably recovered
- The reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and Director of the Information Security Oversight Office (ISOO)

Notify the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action for documents in the physical and legal custody of the National Archives and Records Administration (National

Archives) that have been available for public use

Classification or reclassification may be considered after an agency has received a request for the information under:

- The Freedom of Information Act (5 U.S.G. 552)
- The Presidential Records Act, 44 U.S.C. 2204(c)(1)
- The Privacy Act of 1974 (5 U.S.C. 552a)
- The mandatory review provisions of Section 3.5 of Executive Order 13526

Classification or reclassification may ONLY be considered if such classification meets the requirements of Executive Order 13526 and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the designated senior agency official.

Step 3: Impact

In Step 3, the OCA has to assess the impact to national security if unauthorized release occurs.

The first part of this assessment is to evaluate the potential for damage to national security if unauthorized release of the information occurs. If there is no potential for damage to national security the information will not be classified. If, however, releasing it could cause harm to national security, the information meets the technical requirements to be designated as classified information.

Although OCAs are not required to document the potential for damage to national security, because they may be asked to defend their decision should it be questioned or challenged, it is recommended they record their justification in writing. This is not the end of Step 3, however. The OCA still needs to evaluate some practical factors related to classifying the information. First, the OCA needs to look at whether there is a reasonable possibility of protecting the information from unauthorized disclosure. If the probability of protection is small, the OCA must consider foregoing classifying the information, even though the information is sensitive. Finally, the OCA must also consider other costs of classifying the information, including operational and technological factors, and how it would impact resources. The OCA may decide at this point that the cost of protecting the information far exceeds the need for protecting it.

Once an OCA determines that the need to protect the information justifies the effort and cost of protecting it, he or she can decide to classify the information.

EXAMPLE popup:

Scenario:
An OCA wants to classify all observable aspects of a particular facility. The facility sits along major highways, along flight paths of commercial airlines, and is surrounded by commercial buildings that are not under U.S. Government

control.

What is the possibility of protecting information about the size, shape and layout of this facility?

MORE popup:

Operational factors:

- Classifying information impacts mission operations and the availability of information needed to accomplish mission objectives

For example, imagine the impact on combat operations if personnel with a SECRET security clearance require access to TOP SECRET maps in order to call in artillery support.

Technological factors:

- Classifying certain types of information will have an impact on the information assurance systems in which it resides. This in turn, causes the systems to be classified, limits their connectivity and functionality, and limits the availability of the information
- Classifying weapons systems affects their availability for use, access to the system, and use of the system in various platforms

For example, imagine the impact on combat support if personnel with a SECRET security clearance require access to information about a weapon system that is stored on a TOP SECRET authorized system.

Impact on resources (personnel and money):

- Classifying information has an impact on organizational resources:
    - Impacts personnel staffing based on security clearance requirements and the need for security staff
    - Requires use of security countermeasures, such as alarms, locks, vaults, etc.
    - Requires personnel be cleared to access this information and limits the availability to other individuals who are not cleared

For example, when an OCA classifies information as TOP SECRET, the organization holding this information must ensure that it is safeguarded appropriately with alarms, security containers, guards, security oversight personnel, and similar security countermeasures. Additionally, all personnel must be appropriately cleared to access the information.

Lesson 4: Designate Classification Level

Once the OCA has decided to classify the information, the next step is to determine the appropriate level of classification. This involves determining how sensitive the information is, and what the potential damage to national security is if the information were not protected. In doing this, the OCA must use his or her reasoned judgment.

Based on the sensitivity of the information, and the potential harm to national security, the OCA will proceed to assign a classification level to the information. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

The United States uses three classification levels: TOP SECRET, SECRET, and CONFIDENTIAL. Each level is defined in relation to the potential for damage to the national security. The OCA must look at the damage criteria and decide the appropriate level of classification.

If, in the future, the situation changes, and the risk of harm is greater or lesser, the OCA is responsible for reconsidering his or her initial decision about the level of classification that was assigned.

There are two special cases that OCAs need to consider when classifying information.

CONFIDENTIAL
rollover: 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 (OCA) is able to identify or describe.

SECRET
rollover: 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 (OCA) is able to identify or describe.

TOP SECRET
rollover: 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 (OCA) is able to identify or describe.

Compilation
popup: Sometimes combining two or more pieces of unclassified

information can result in an aggregate that warrants protection. Or combining elements of information classified at one level may require protection of the aggregate at a higher level.

This occurrence is called compilation. In making decisions about whether information should be classified by compilation, an OCA needs to consider the same criteria for classification eligibility and potential for impact on national security as other original classification actions. Although classification by compilation may be uncommon, some types of information are more likely to be subject to it.

Compilation rollover: Compilation: also known as aggregation involves combining or associating individually, unclassified information that reveals an additional association or relationship that warrants protection as classified information. This concept also applies to elements of information classified at a lower level that become classified at a higher level when combined.

The information must be located where one could realistically Assume that the elements of information could be associated to derive classified meaning. Since most information is no longer solely paper-based, the interpretation of this requirement to mean in the same section of the document or on the same page is inadequate. User queries of data in electronic formats (e.g., databases, spreadsheets) lead to new aggregations, and posting of information on the internet makes the use of data mining and other data correlation tools easy and widespread. OCAs should consider the possibility that such tools and methods will be used to compile information and should, when appropriate, identify classified compilations when issuing classification guidance.

Budget and tables of distribution EXAMPLE

	Unclassified	CONFIDENTIAL	SECRET	TOP SECRET
3.3.3.7 Budget	X			
3.3.3.8 Tables of Distribution	X			
3.3.3.9 Compilation of both budget and tables of distribution within the same document		X		

Staffing and equipment allowances EXAMPLE

	Unclassified	CONFIDENTIAL	SECRET	TOP SECRET
3.3.4.7 Staffing		X		

3.3.4.8 Equipment allowances		X		
3.3.4.9 Compilation of both staffing and equipment allowances within the same document			X	

Mission and Geographic Location EXAMPLE

	Unclassified	CONFIDENTIAL	SECRET	TOP SECRET
3.3.2.7 Mission	X			
3.3.2.8 Geographic Location	X			
3.3.2.9 Compilation of both mission and geographic location within the same document			X	

Reclassification popup:

Sometimes it is necessary to reclassify information that has been declassified and released to the public. This decision must be made based on proper authority and must meet certain requirements. Only the Secretary of Defense or, for information under his or her jurisdiction, the Secretary of a Military Department or the Deputy agency head or senior agency official to whom such authority has been delegated may decide to reclassify such information.

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 OUSD(I). Requests for reclassification must include specific information.

Reclassification requires a written determination of necessity in the interest of national security.

Requests for reclassification must include:

- A description of information
- The classification level of the information
- When and how it was released to the public
- An explanation as to why it should remain classified
- The number of recipients/holders and how they will be notified of the reclassification
- How the information will be recovered

Step 5: Duration

After determining the level of classification, the OCA must decide how long the information will remain classified, and at what level.

Step 5 involves two considerations. The first is downgrading. The OCA must review the information and its classification level to assess whether it can be lowered in the future. The second is declassification. This is a determination made by the OCA of how long the classification of the information will remain in effect.

Downgrading popup:

Downgrading is a determination that information classified at one level will have its classification reduced to a lower level on a specific date or event. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level.

In making a downgrading determination, an OCA must evaluate the information to assess whether there is a date or event in the future when the potential for damage to national security diminishes to a point that will enable the classification level to be lowered. For example, the sensitivity of certain information during the design phase of an effort may change once the effort has moved to manufacturing, or a phase of operations has passed. If the OCA can determine a date or event that will trigger this decrease in sensitivity, he or she can assign a downgrading date and the lower classification level to take effect on that date.

Downgrading: a determination that information classified at one level will have its classification reduced to a lower level on a specific date or event.

Declassification popup:

Declassification is an authorized change in status of information from classified to unclassified. The OCA must make declassification determinations for all classification decisions, with a few special exceptions. The OCA should select, to the greatest extent possible, the declassification instruction that will result in the shortest duration of classification. Here are the guidelines an OCA must follow when making declassification determinations.

If the OCA knows of a date within ten years when the potential for damage from compromise is no longer a concern to the national security, then he or she assigns that date as the declassification date. If the OCA cannot identify a date, but rather an event that is expected to occur within the next ten years after which the potential for damage from compromise is no longer a concern, then that event is assigned as the declassification date. Absent a date or event within that ten-year period, the OCA assigns the declassification date as the date that is exactly ten years after the

date of original classification.

If, however, the OCA determines the information requires protection beyond ten years of its original classification, he or she may assign a date up to 25 years from the date of the original classification decision. Several 25X and 50X exemptions to this are detailed in Executive Order 13526, for special cases in which information needs to remain classified longer than 25 years.

Requests for reclassification must include:

- 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 between 10 and 25 years from original classification date
- Unless a 25X exemption applies

MORE popup:

25X Exemption Applications
Executive Order 13526 (Section 3.3(b)) contains the following exemptions from the requirement to declassify information at 25 years of the date of its original classification:

- 25X1: reveals the identify of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use or under development;
  Interagency Security Classification Appeals Panel (ISCAP) approval for 25X exemptions must be requested via the chain of command and must have an ISCAP-approved date or event for declassification:
- 25X2: reveals information that would assist in the development, production, or use of weapons of mass destruction;
- 25X3: reveals information that would impair U.S. cryptologic systems or activities;
- 25X4: reveals information that would impair the application of state-of-the-art technology within a U.S. weapon system;
- 25X5: reveals formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

- 25X6: reveals information including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- 25X7: reveals information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of national security, are authorized;
- 25X8: reveals information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- 25X9: violates a statute, treaty, or international agreement

CAUTION

"25X1-human" may not be used for information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source.

50X1 – HUM shall be used for information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source (do not include a declassification date or event).

50X2 – WMD shall be used for information that is clearly and demonstrably expected to reveal key design concepts of weapons of mass destruction (do not include a declassification date or event).

Follow guidance provided in this course, Executive Order 13526, 32 CFR Parts 2002 and 2003 Classified National Security Information; Final Rule, and DoDM 5200.01, Volume 2.

DO NOT USE X1 through X8.

Compromise rollover: A compromise is an unauthorized disclosure of classified Information.

50X1-HUM rollover: An OCA shall apply the 50X-HUM, 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 originally classify it.

50X2-WMD rollover: WMD shall be used for information that is clearly and demonstrably expected to reveal key design concepts of weapons of mass destruction (do not include a declassification date or event).

Exemptions popup: In the following areas, classification is based on statute, rather than Executive order 13526:

- Information classified in accordance with the Atomic Energy Act of 1954, as amended, which includes restricted data and formerly restricted data (RD)
- Restricted data (RD) classification decisions are noted in Department of Energy (DoE) Classification Guides
- Formerly restricted data (FRD) classification decisions are documented in the Joint DoE/DoD Classification Guides

Step 6: Guidance

The final step in the original classification decision process is to designate the information as classified and communicate that decision to individuals who use the information. Because the decisions of OCAs are used by others who must make derivative classification determinations and protect the information from unauthorized disclosure, it is vital for OCAs to communicate their decisions effectively.

There are two methods for communicating original classification decisions. In order of preference, they are through a security classification guide, or SCG, or in a properly marked source document.

Security Classification Guide (SCG) popup: The preferred method for communicating an original classification decision is through a security classification guide. An SCG is topic-specific, covering a specific system, plan, program, project, or mission. Security classification guides allow the OCA to identify the exact classification, downgrading, and declassification instructions, and any special handling caveats for all aspects of the system, plan, program, project, or mission. DoDM 5200.45, Instructions for Developing Security Classification Guides, lists the minimum information SCGs must contain.

MORE popup: DoDM 5200.45, Instructions for Developing Security Classification Guides requires SCGs to contain at a minimum:

- Name of the system, plan, program, project, or mission
- Name and address of issuing office
- Identify the OCA by name and title or personal identifier
- Identify an agency point of contact for question about the guide
- Provide the date of issuance or last review
- General guidelines, per DoDM 5200.45, Enclosure 4, Figure 4
- State precisely the items or elements of information to be protected
- Specify a level of classification for each item or element or that is unclassified
- State a concise reason for classification of the information and cite the applicable classification category
- Give notice of any special handling caveats
- State the declassification instructions for each item or element of classified information, including citation of the approved automatic declassification exemption category, if any

Properly marked source document popup: The second preferred method of disseminating an original classification decision is through a properly marked source document. Using this method, OCAs may provide guidance in the form of a memorandum, plan, message document, letter, or publication. This type of guidance must contain minimum classification markings.

Document rollover: Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage material

MORE popup: A properly marked document includes:

- Appropriate portion markings
- Overall classification
- Date of decision/guidance
- Agency and office of origin
- Subject
- Name or personal identifier and position of the OCA
- Declassification instructions

- A concise reason for classification, which at a minimum cites one of the categories in paragraph 1.4, E.O. 13526
- Applicable special control or warning notices

Review Activity 1

Can you identify the correct order of the steps in the original classification process?

_____ Step 1
_____ Step 2
_____ Step 3
_____ Step 4
_____ Step 5
_____ Step 6

A. Determine the impact of classifying the information.
B. Determine the duration of the classification.
C. Determine if the information is eligible for classification.
D. Determine how to communicate the classification.
E. Determine if the information is official government information.
F. Designate the classification level of the information.

Answer: E, C, A, F, B, D

Review Activity 2

Read each scenario and answer the question.

Question 1 of 2
An OCA has reviewed information. After a thorough review, the OCA determines that the information does not require protection, but that its release should be delayed for a couple of months in the interest of national security. What determination should the OCA make?

- o Classify the information
- o Derivatively classify the information
- o Do not classify the information
- o Declassify the information

Answer: Do not classify the information

Question 2 of 2
As part of a school research project, university students developed a technology that might one day be applicable in defending the U.S. against biological weapons, but it is not clearly related to national security. What determination should the OCA make?

- o Classify the information
- o Derivatively classify the information
- o Do not classify the information

- Declassify the information

Answer: Do not classify the information

Review Activity 3

Can you answer this question?

An OCA has examined information and has determined it needs to be classified at the SECRET level. If this information were disclosed without authorization, what type of damage could reasonably be expected to occur to national security?

- Exceptionally grave damage
- Damage
- Severe damage
- Serious damage

Answer: Serious damage

Review Activity 4

Try answering these questions.

How well do you know the process for determining the duration of classification?

OCAs must always assign a downgrading date when they originally classify information.
Answer: False

OCAs must always make a declassification determination when they originally classify information.
Answer: True

OCAs first seek to identify a declassification date within 10 years of the date of original classification, after which revealing the information no longer poses a threat to national security.
Answer: True

If there is no specific date or event within 10 years, OCAs may assign a date that is exactly 10 years after the original classification.
Answer: True

If the information needs protection for longer than 10 years, OCAs may assign a declassification date up to 15 years after original classification of the information.
Answer: False

Several special exemptions apply that allow information to remain classified beyond the maximum duration.
Answer: True

Review Activity 5

Can you answer this question?

Which of the following are authorized methods for communicating original classification decisions?

- □ Security Classification Guide (SCG)
- □ Security Declassification Guide (SDG)
- □ Distribution Statements
- □ Properly marked source documents

Answer: Security Classification Guide (SCG), Properly marked source document

Summary

In this lesson, you learned about the six-step process that OCAs follow when determining whether to originally classify information. Select each step to see a brief review.

Six-Step Process for Original Classification
Step 6 – Guidance
Step 5 – Duration
Step 4 – Designate Classification Level
Step 3 – Impact
Step 2 – Eligibility
Step 1 – Government Information

Step 1: Government Information

Since the OCA is a classifier, he/she must determine if the information is:

- Owned by
- Produced by or for, or
- Under the control of the U.S. Government?

Owned by rollover: "Owned by" is information that belongs to the U.S. Government

Produced by or for rollover: "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

rollover: "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: Eligibility

Step 2: Is the information eligible to be classified?

- Perform an eligibility analysis
- Determine whether any prohibitions or limitations bar classification
- Has the information already been classified by another OCA?
- Is classification guidance already available in the form of security classification guides, plans or other memorandums?

eligibility analysis popup: 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 national security
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. The development, production or use of weapons of mass destruction (WMD)

prohibitions popup: In no case shall information 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 popup: Limitations on classification apply to the following types of

information:

- Basic scientific research information not clearly related to national security
- Information that has been declassified and released to the public may be reclassified only under specific conditions
- Information not previously disclosed to the public may be classified or reclassified only in certain cases

Step 3: Impact

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

- Does unauthorized release create a risk of harm to the national security?
- Can the information reasonably be protected?
- What are the costs of classifying the information?

Step 4: Designation

Step 4: What level of classification is appropriate?

- Determine how sensitive the information is
- Determine the potential 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

CONFIDENTIAL
rollover: 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 (OCA) is able to identify or describe.

SECRET
rollover: 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 (OCA) is able to identify or describe.

TOP SECRET
rollover: 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 (OCA) is able to identify or describe.

Step 5: Duration

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 between 10 and 25 years from original classification date
  - Unless a 25, 50, or 75X exemption applies

Step 6: Guidance

Step 6: How does the classification decision get disseminated?

1. Security Classification Guide (SCG)
2. Properly marked source document

Lesson: Course Conclusion

Course Summary

The national security of the United States depends on the protection of sensitive information. The initial determination that information needs to be protected as classified is known as original classification.

Only certain officials - - known as original classification authorities - have the authority to make these decisions.

In this course you learned about their role and responsibilities, the requirements they must meet, as well as the process they follow in making these important determinations.

Lesson Review

Here is a list of the lessons in the course.

Lessons:

- Course Introduction
- Original Classification Basics
- Original Classification Authority
- Original Classification Decision Process
- Course Conclusion

Original Classification Basics

Review popup:

Original Classification
What is it?

- Initial determination that information requires protection against unauthorized disclosure in the interest of national security

Who does it?

- ONLY government officials with authority to make original classification decisions

Classification rollover:

Classification is the act or process by which information is determined to be classified. It is the determination that information requires protection in the interest of national security. When the information is identified, it is assigned one of three levels of classification: TOP SECRET, SECRET, or CONFIDENTIAL.

Classifier rollover: A classifier is an individual who makes a classification determination and applies a security classification to information or material. A classifier may be an Original Classification Authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

Information rollover: Information is the knowledge that can be communicated, and documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

national security rollover: National security is information relating to the national defense or foreign relations of the United States.

Original Classification rollover: Original classification is an initial determination by an authorized Original Classification Authority (OCAs) that information requires protection because unauthorized disclosure of the information could reasonably be expected to cause damage to national security.

OCA rollover: An original classification authority is an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance).

Original Classification Authority Review popup:

Original Classification Authority:

- Responsibilities
- Positions
- Appointment criteria
- Training requirements
- Scope of authority
- Assignment to subordinates

Responsibilities rollover: OCA Responsibilities:

- Determine whether information needs to be classified
- Determine level of classification
- Determine duration of classification
- Disseminate classification decisions to others

Positions rollover:

Positions with OCA:

- President of the United States
- Vice President
- Secretary of Defense
- Secretaries of the Military Departments
  - Secretary of the Army
  - Secretary of the Navy
  - Secretary of the Air Force
- Certain other senior agency officials within DoD

Appointment criteria rollover:

Requests for OCA must:

- Specify the position title
- Present a mission specific justification for the request
- Submit through established organizational channels

Circumstances for granting OCA:

- Demonstrable and continuing need to exercise OCA
- Sufficient expertise and information is available
- Existing Security Classification Guides are not sufficient to address classification needs
- Referral of decisions to existing OCAs is not practical

Training requirements rollover:

OCAs must be trained in the following:

Classifying Information:

- What is the difference between original and derivative classification?
- Who can classify information originally?
- What are the standards and training requirements that an original classifier must meet to classify information?
- What are the prohibitions and limitations on classifying information?

- Has the information already been classified by another OCA?
- Is classification guidance already available in the form of security classification guides (SCGs), plans or other memorandums?

Duration/Declassification:

- What is the process for determining duration of classification?
- What are the declassification options available to OCAs?
- What are the general standards and procedures for applying declassification instructions?

Marking Classified Information:

- What are the basic portion, banner and classification authority box markings that must appear on classified information?

Communicating Classification Decisions:

- What are the requirements and standards for creating, maintaining, and publishing SCGs?

Safeguarding Classified Information:

- What are the procedures for properly safeguarding classified information?
- What are the criminal, civil, and administrative sanctions that can be imposed for failure to protect classified information from unauthorized disclosure?

Scope of authority rollover:

Scope of authority:

- Classification level
- Specific area of jurisdiction

Assignment to subordinates rollover:

Assignment to subordinates:

- OCAs may be assumed by a subordinate only when "acting in the capacity" of the OCA
- Subordinates must provide written certification of training

Original Classification Decision Process popup:

Six-Step Process for Original Classification
- Step 6 – Guidance
- Step 5 – Duration
- Step 4 – Designate Classification Level
- Step 3 – Impact
- Step 2 – Eligibility
- Step 1 – Government Information

Step 1 – Government Information rollover:

Since an OCA is a classifier, he/she must determine if the information is:
- Owned by
- Produced by or for
- Under the control of the U.S. Government

Step 2 – Eligibility rollover:

Step 2: Is the information eligible to be classified?
- Perform an eligibility analysis
- Determine whether any prohibitions or limitations bar classification
- Determine if the information has already been classified by another OCA
- Determine if classification guidance is already available in the form of security classification guides, plan or other memorandums

Step 3 – Impact rollover:

Step 3: What is the impact of classifying the information?
- Does unauthorized release create a risk of damage to national security?
- Can the information reasonably be protected?
- What are the costs of classifying the information?
  - Operational factors
  - Technological factors
  - Impact on resources

Step 4 – Designate Classification Level rollover:

Step 4: What level of classification is appropriate?
- Determine how sensitive the information is

- Determine the potential damage to national security if the information is not protected
- Assign a classification level to the information:
  - TOP SECRET
  - SECRET
  - CONFIDENTIAL
- Reassess classification assignment when appropriate

Step 5 – Duration rollover:

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, OR
  - Assign date between 10 and 25 years from original classification
  - Unless a 25, 50, or 75X exemption applies

Step 6 – Guidance rollover:

Step 6: How does the classification decision get disseminated?

1. Security Classification Guide (SCG)
2. Properly marked source document

Course Objectives

You should now be able to perform all of the listed activities. Congratulations. You have completed the Original Classification Course.

You should now be able to:

- ✓ Define original classification
- ✓ Identify Original Classification Authority requirements and qualifications
- ✓ Identify the six steps in the original classification decision process
- ✓ Identify limitations and prohibitions on original classification
- ✓ Identify the basis for determining classification levels
- ✓ Identify the process for determining duration of classification
- √ Identify authorized sources of classification guidance