Student Guide

Course: Derivative Classification

Lesson 1: Course Introduction

Course Information

Purpose	Provide a thorough understanding of the responsibilities associated with derivative classification and the procedures to follow to correctly derivatively classify documents
Audience	Military, civilian, and contractor personnel responsible for oversight or application of derivative classification.
Pass/Fail %	75%
Estimated completion time	90 minutes

Course Overview

In the course of working with classified information, individuals sometimes generate or create new documents and materials based on that information. These individuals are called derivative classifiers. These derivative classifiers are responsible for maintaining the protection of that classified information. These individuals are called derivative classifiers. In addition, they must carefully analyze their work product to determine what classified information it contains or reveals, and evaluate that information against official classification guidance.

Based on that evaluation, derivative classifiers must ensure that the information in the new material is identified as classified by applying the appropriate markings to the document. This process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material is called derivative classification.

Derivative classifiers need to understand what their responsibilities are, what processes to follow, and what resources to consult to safeguard information that, if revealed, could cause damage to national security.

Course Objectives

- Identify the responsibilities associated with derivatively classifying information
- Identify the processes and methods for derivatively classifying information
- Identify authorized sources to use when derivatively classifying information
- Applying authorized sources, derivatively classify information based on the concepts of “contained in,” “revealed by,” and "compilation"
- Explain the limitations and prohibitions of classifying information and ways to promote information sharing through classification
- Identify the process for managing classification challenges, security incidents, and sanctions

Lessons in the Course

- Course Introduction
- Derivative Classification Basics
- Classification Concepts
- Limitations, Prohibitions and Challenges
- Practical Exercise
- Course Conclusion

Student Guide

Course: Derivative Classification

Lesson 2: Derivative Classification Basics

Introduction

Because protecting classified information from improper disclosure is so critical, there are responsibilities and procedures to follow when using classified information to create new documentation. You must be familiar with these responsibilities and procedures as well as where to go for guidance so you can successfully implement and execute them at your activity or facility.

Lesson Objectives

- Define derivative classification
- Identify the requirement for and importance of derivative classification
- Identify who will have derivative classification responsibilities and the requirements he or she must meet
- Identify the steps involved in the derivative classification process
- Identify authorized sources to use when derivatively classifying information

Derivative Classification Overview

1. **What is Derivative Classification?**

The initial decision about what information should be classified is called original classification. Because this is a very important, sensitive decision, the Government has granted only a limited number of government officials the authority to perform original classification.

Derivative classification is different. It is the process of using existing classified information to create new documents or material, and marking the newly-developed document or material consistent with the classification markings that apply to the source information. Copying or duplicating existing classified information, such as photocopying a document, is not derivative classification.

Whereas delegation of authority to perform original classification is appointed to specific government officials by position, no specific delegation of authority is required to be a derivative classifier. In fact, all cleared DoD and authorized contractor personnel who generate or create documents or material from classified sources are derivative classifiers.

Like original classification, derivative classification has far-reaching effects on the Department of Defense and industry. Classifying information helps protect our national security. It limits access to only those individuals with the appropriate clearance level and a legitimate need to know the information. Classification also impacts resources; it imposes costs for things like security clearances, physical security measures, and countermeasures. Because of the importance of classification, but also its inherent limitations and costs, it is crucial that derivative classifiers follow appropriate procedures and observe all requirements.

2. Derivative Classification Responsibilities

In general, derivative classifiers are responsible for ensuring that they apply the highest possible standards when derivatively classifying information. Derivative classifiers who generate new products bear the principal responsibility for the accuracy of the derivative classification. For this reason, it is important to follow DoD policy requirements.

Derivative classifiers have a variety of responsibilities they must meet in order to properly perform derivative classification. First, they must understand derivative classification policies and procedures. Before derivative classification can be accomplished, the classifier must have received the required training in the proper application of the derivative classification principles as specified in E. O. 13526, as well as emphasizing the avoidance of over-classification. At a minimum, the training must cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. Personnel shall receive this training prior to derivatively classifying information.

In addition to this preparatory training, derivative classifiers must receive training at least once every two years. Derivative classifiers who do not receive mandatory training at least once every two years will have their authority to apply derivative classification markings suspended until they have received such training.

They must also possess expertise in the subject matter on which they are creating documentation, as well as on classification management and marking techniques. Derivative classifiers must also have access to classification guidance. This helps meet the responsibility of analyzing and evaluating information to identify elements that require classification.

The most important responsibilities derivative classifiers have is to observe and respect the original classification authority’s decision and to use only authorized sources to determine derivative classification.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

To understand derivative classification policies and procedures:

- Complete the eLearning course: Derivative Classification
- Complete the Marking Classified Information eLearning course offered by the DSS CDSE
- Consult DoDM 5200.01, Volumes 1-4 and/or DoD 5220.22-M
- Contact your Security Manager or Facility Security Officer (FSO)

3. Policy Guidance

There are two primary sources of policy guidance for derivative classification.

Within the Department of Defense, DoD Manual 5200.01, Volumes 1-4, the Information Security Program, provides the basic guidance and regulatory requirements for the DoD Information Security Program. Volume 1, Enclosure 4, discusses derivative classifier responsibilities.

For industry, DoD 5220.22-M, the National Industrial Security Program Operating Manual, or NISPOM, contains information on the derivative classification responsibilities.

How Does Derivative Classification Work?

1. Derivative Classification Concepts

So how do you determine whether the information contained in a new product is classified? As a derivative classifier, you are responsible for checking whether the content of the information already exists in one of the acceptable forms of classification guidance. If the guidance tells you the information in your new product is classified, you must classify and treat it as such. Note that for derivative classification purposes, the term "document" refers to any physical medium in or on which information is recorded or stored. This includes written or printed matter, audiovisual materials, and electronic storage media. Let's take a closer look at these authorized sources for derivative classification.

2. Authorized Sources for Derivative Classification

To ensure that the original classification of information is maintained, derivative classifiers must use *only* authorized sources of classification guidance to derivatively classify information. While it might be tempting, derivative classifiers must *not* rely on their memories or general rules about classification.

There are only three authorized sources for derivative classification. The first source is a Security Classification Guide (SCG). An SCG is a collection of precise, comprehensive guidance about a specific program, system, operation, or weapon system telling what elements of information are classified. For each element of information, the SCG includes its classification level, the reasons for that classification, and when the information can be downgraded or declassified. For this reason, SCGs are the primary source for derivative classification.

A second authorized source is an existing, properly marked source document from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document. You must carry the classification of that existing material forward into your new end product.

The third authorized source is the DD Form 254, the Department of Defense Contract Security Classification Specification which is used by contractors. The NISPOM states the Government Contracting Activity, or GCA, is responsible for providing the contractor proper classification guidance needed during the performance of the contract. This guidance is provided by the Contract Security Classification Specification, in this case, the DD Form 254. The DD Form 254 also informs the contractor of the level of information they will need to access, the required level of security clearance for access, and the performance requirements; for example, safeguarding and special security requirements. Security classification guidance required for derivative classification is identified in block 13 of the DD Form 254. However, source documents such as the security classification guide itself sometimes are attached to the DD Form 254. This is usually done when there is not enough space in block 13 to include all the classification guidance the contractor will need to perform derivative classification.

These three sources are the *only* authorized sources for derivative classification. Any other source is *unauthorized*, and must *not* be used as the basis for derivative classification. Some examples of such unauthorized sources appear in the box below:

Examples of unauthorized sources of classification:

- ∅ Memory: "I remember that project was classified Secret 5 years ago, so it must be Secret now."
- ∅ Unconfirmed source: "Someone told me this document can be declassified."
- ∅ Just because: "I am going to classify this technology Top Secret because I think it might give the U.S. a superior tactical advantage."
- ∅ Media/Internet: "I saw it while browsing the internet so it must be declassified."

3. Process Overview

Derivative classifiers must carefully analyze the material they are classifying to determine what information it contains or reveals, and evaluate that information against the instructions provided by the classification guidance or the markings on source documents.

To perform that evaluation, derivative classifiers may use only authorized sources of guidance to classify the information in question. Authorized sources of classification guidance are a Security Classification Guide, a properly marked source document, and the DD Form 254. If the authorized sources do not provide sufficient guidance, you may need to refer to other officials for assistance, such as the Security Manager or Original Classification Authority (OCA) with jurisdiction for DoD personnel, or the Facility Security Officer (FSO) or Government Contracting Activity (GCA) for contractors. Your chain-of-command or appropriate reporting channels will provide specific guidance about who you should consult.

In addition to assigning the appropriate classification level to information, derivative classifiers are also responsible for carrying forward guidance about when the classification of that information may be downgraded, and when it may be declassified altogether. This is an important part of the derivative classification task. Downgrading information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Executive Order 13526 provides that "information shall be declassified as soon as it no longer meets the standards for classification" established by the Order.

Every time information is classified, a determination must be made regarding how long the information will be protected. This is an essential part of the classification and declassification process.

For derivatively classified information, the classifier must specify one of the following on the "Declassify On" line:

1. A specific date or event for declassification, within 25 years of the document's origin
2. Absent a declassification instruction or other declassification guidance from the OCA, a calculated date 25 years from the date of the document's origin
3. An approved 25-year exemption (i.e., 25X1 through 25X9) with a date or event for declassification
4. 50X1-HUM or 50X2-WMD
5. An approved 50-year exemption (i.e., 50X1 through 50X9) with date or event for declassification
6. An approved 75-year exemption (i.e., 75X1 through 75X9) with date or event for declassification

Finally, once you have determined the derivative classification of the new material and its downgrading and/or declassification dates, you are responsible for marking it appropriately. Proper marking practices include:

- Applying portion markings
- Documenting or attaching the list of sources to the new document or material (especially when multiple sources are used)

- Providing source of derivative classification, i.e., “Derived From”
- Identifying on the “Classified By” line, the person performing derivative classification by name and position or personal identifier

For information on marking, refer to DoD Manual 5200.01,Volume 2, Information Security Program, and the Marking Classified Information eLearning course offered by the DSS CDSE.

Review Activity

Question 1

Which of the following is NOT a function of derivative classification? Select the best answer.

○ Creating new classified materials from properly marked, existing classified source materials and marking them accordingly
○ Making an initial determination that information requires protection against unauthorized disclosure in the interest of national security
○ The process of extracting, paraphrasing, restating, or generating in a new form, information that is already classified
○ Carrying forward the correct classification level for classified information used to generate new materials or documents

Question 2

Which of the following are authorized sources for derivative classification? Select all that apply.

☐ Security Classification Guide (SCG)
☐ DoD 5220.22-M (NISPOM)
☐ Your level of expertise with the content
☐ DoDM 5200.01, Vol. 1-4 (DoD Information Security Program)
☐ A properly marked classified source document
☐ DD Form 254 (Department of Defense Contract Security Classification Specification)
☐ The Facility Security Officer (Industry) or Security Manager (DoD)

Question 3

Select True or False for each statement.

		True	**False**
Photocopying a Secret document and marking the photocopy Secret is derivative classification.		○	○
Only government officials may perform derivative classification.		○	○
Consulting your FSO or security manager is always the first step in the derivative classification process.		○	○
Derivative classifiers are responsible for analyzing and evaluating information to identify elements that require classification.		○	○

Lesson Conclusion

In this lesson, you learned about the importance of derivative classification and how it is different from original classification. You also learned about the responsibilities of derivative classifiers. You learned about the three authorized sources for derivatively classifying information, and you learned the basic process for derivatively classifying information.

Answer Key

Question 1

Which of the following is NOT a function of derivative classification? Select the best answer.

- ○ Creating new classified materials from properly marked, existing classified source materials and marking them accordingly
- ⦿ Making an initial determination that information requires protection against unauthorized disclosure in the interest of national security
- ○ The process of extracting, paraphrasing, restating, or generating in a new form, information that is already classified
- ○ Carrying forward the correct classification level for classified information used to generate new materials or documents

Feedback: *"Making an initial determination that information requires protection against unauthorized disclosure in the interest of national security" describes original classification, not derivative classification.*

Question 2

Which of the following are authorized sources for derivative classification?

- ☑ Security Classification Guide (SCG)
- ☐ DoD 5220.22-M (NISPOM)
- ☐ Your level of expertise with the content
- ☐ DoDM 5200.01, Vol. 1-4 (DoD Information Security Program)
- ☑ A properly marked classified source document
- ☑ DD Form 254 (Department of Defense Contract Security Classification Specification)
- ☐ The Facility Security Officer (Industry) or Security Manager (DoD)Question 3

Feedback: *The only authorized sources for derivative classification are SCGs, properly marked classified source documents, and DD Form 254.*

Question 3

		True	False
Photocopying a Secret document and marking the photocopy Secret is derivative classification.		○	●
Feedback: *Derivative classification does not include copying or duplicating existing classified information.*			
Only government officials may perform derivative classification.		○	●
Feedback: *Derivative classification is not limited to government personnel. All cleared DoD and contractor personnel who are authorized by DD Form 254 to generate or create material from classified sources are derivative classifiers.*			
Consulting your FSO or security manager is always the first step in the derivative classification process.		○	●
Feedback: *Consulting your FSO or security manager in derivative classification determinations is authorized but it may not be necessary if you are knowledgeable in your derivative classification responsibilities. Consult your FSO or security manager for additional training, guidance, and/or clarification during the derivative classification process.*			
Derivative classifiers are responsible for analyzing and evaluating information to identify elements that require classification.		●	○
Feedback: *As a derivative classifier, one of your responsibilities is to analyze and evaluate information to identify elements that require classification.*			

Student Guide

Course: Derivative Classification

Lesson: Classification Concepts

Introduction

Government and contractor personnel who extract, paraphrase, restate, or generate classified information in a new form are derivatively classifying the new content. When information is clearly identified as classified, it is marked as Top Secret, Secret, or Confidential. However, there are times in the derivative classification process when the classification of information is not clearly stated or obvious. This does not mean that the information is unclassified. Derivative classifiers must carefully analyze the material they are classifying to determine what information it contains or reveals, and evaluate that information against authorized classification guidance.

Lesson Objectives

- Define and distinguish the differences between the concepts of “extracting,” “paraphrasing,” and “generating”
- Define and distinguish the differences between the concepts of “contained in,” “revealed by,” and "compilation"
- Recognize examples of derivative classification based on the concept of “contained in,” based on various authorized sources
- Recognize examples of derivative classification based on the concept of “revealed by,” based on various authorized sources
- Recognize examples of derivative classification based on the compilation of information, guided by authorized sources

Derivative Classification Terms and Concepts

1. **Key Terms**

There are different ways in which derivative classifiers can create new content from authorized sources. They can extract information, paraphrase or restate it, or generate that information in a new form.

As part of their derivative classification responsibilities, they must correctly identify the classification level of the new material and mark it accordingly. It is important, therefore, to understand what each of these terms means.

- Extracting occurs when information is taken directly from an authorized classification guidance source and is stated verbatim in a new or different document.

- Paraphrasing or restating occurs when information is taken from an authorized source and is re-worded in a new or different document. Derivative classifiers must be careful when paraphrasing or restating information to ensure that the classification has not been changed in the process.

- Generating is when information is taken from an authorized source and generated into in another form or medium, such as a video, DVD, or CD.

Understanding the different ways of incorporating existing classified information into new material is only part of the picture. However, there are three key classification concepts you will need to apply in order to correctly classify your newly created materials.

2. Concepts Overview

There are three key concepts that you can use to determine the classification level of the material you create. Your new material may include classified information that is *contained in* the classification guidance. Or, because of the way it is organized or structured, your new material may *reveal* classified information that did not specifically appear in the classification guidance used to create it. Finally, your new material may aggregate, or bring together, pieces of information that are unclassified, or have one classification level, but when you present them together it either renders the new information classified, or increases its classification level. This is called *compilation*. Let's take a closer look at each of these concepts.

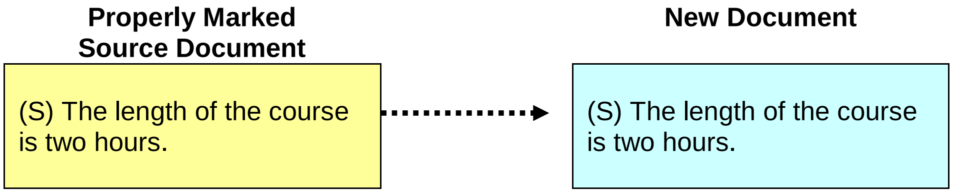
"Contained In"

1. Definition

The concept of "contained in" applies when derivative classifiers incorporate classified information from an authorized source into a new document, and *no* additional interpretation or analysis is needed to determine the classification of that information. In other words, when classified information in a new document is *contained in* the authorized source, the new document's classification is derived directly from the classification of that source. The concept of "contained in" can apply when the information is extracted word-for-word, or when the information is *paraphrased* or *restated* from the existing content.

2. Examples

Let's review some examples of how the "contained in" concept determines the derivative classification of a new document.



Properly Marked Source Document

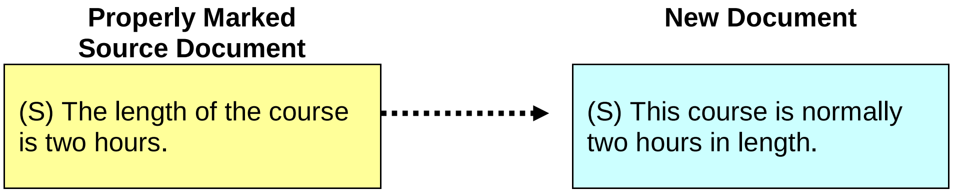
(S) The length of the course is two hours.

New Document

(S) The length of the course is two hours.

In this example, the classification guidance is a properly marked source document. It contains classified information that has been extracted word for word into the new document. Because the information contained in the classification source was Secret, you must classify the new document Secret.

Let's look at another example:



Properly Marked Source Document

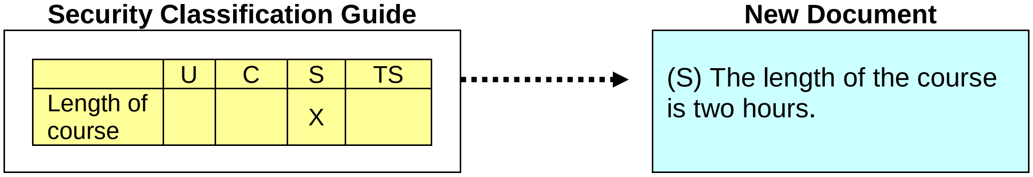
(S) The length of the course is two hours.

New Document

(S) This course is normally two hours in length.

Here, the information from the classified source is paraphrased and incorporated in the new document. Even though it is worded differently, the information in the new document is contained in the classified source, where it is Secret. Therefore, you must classify the new document Secret.

The "contained in" concept also applies to the use of a Security Classification Guide (SCG). Sometimes, the guidance in an SCG may explicitly apply to the content you incorporate into a new document:



Security Classification Guide

	U	C	S	TS
Length of course			X	

New Document

(S) The length of the course is two hours.

This SCG provides that the information about the length of the course is classified Secret. Because you have stated this exact information in your new document, you must apply this Secret classification as dictated by the SCG.

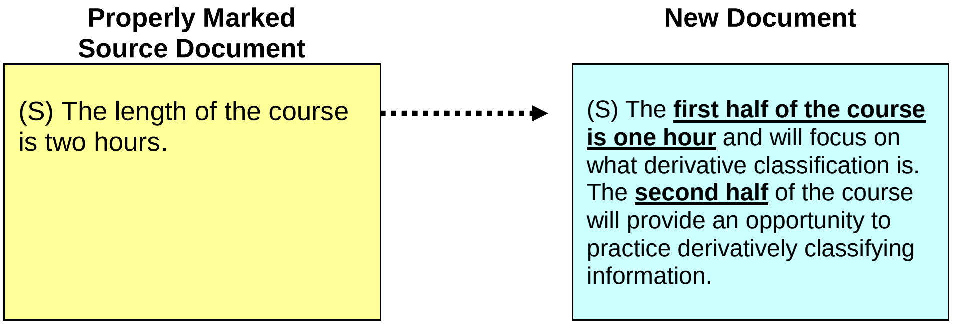
"Revealed by"

1. Definition

The concept of "revealed by" applies when derivative classifiers incorporate classified information from an authorized source into a new document that is *not* clearly or explicitly stated in the source document. However, a reader can *deduce* the classified information from the new document by performing some level of additional interpretation or analysis. In this sense, the classified nature of the information in the new document is *revealed by* analysis of its contents, so it will need to be marked in accordance with that classification.

2. Example

Let's look at some examples of how the classification of information can be revealed through analysis.



Properly Marked Source Document

(S) The length of the course is two hours.

New Document

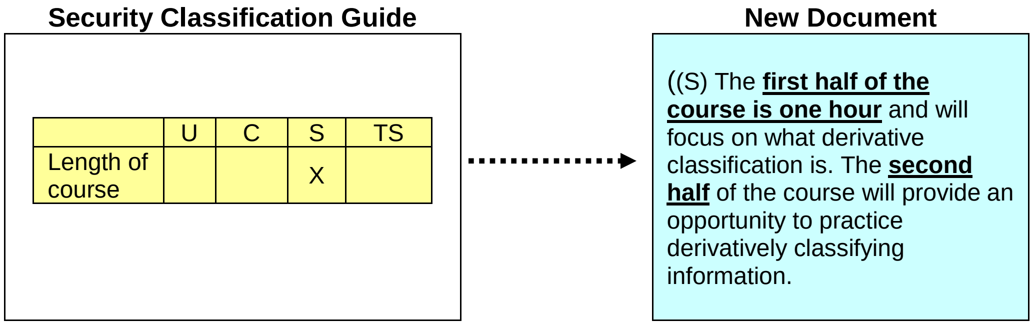
(S) The **first half of the course is one hour** and will focus on what derivative classification is. The **second half** of the course will provide an opportunity to practice derivatively classifying information.

The properly marked source document contains some Secret information. Your new document does not contain that same information. However, the information in your new document will allow a reader to *deduce* the classified information.

If the *first* half of the course is one hour long, it follows that the *second* half would be the same length -- one hour. Since the course has two one-hour halves, it must be two hours long. That information is classified Secret according to the properly marked source document, so you must apply the same classification markings to the information in your new document.

The concept of "revealed by" also applies when you are using an SCG as classification guidance. You need to look at what information can be deduced from what you have included in your new material and check whether that information is *itself* listed as classified in an SCG:

	U	C	S	TS
Length of course			X	



Security Classification Guide

	U	C	S	TS
Length of course			X	

New Document

((S) The **first half of the course is one hour** and will focus on what derivative classification is. The **second half** of the course will provide an opportunity to practice derivatively classifying information.

"Classification by Compilation"

1. Definition

Sometimes combining two or more pieces of unclassified information can result in an aggregate that is classified. This occurrence is called compilation, or aggregation.

Classification by compilation involves combining or associating unclassified individual elements of information to reveal an additional association or relationship that warrants a classified level of protection. Classification by compilation is not the norm when derivatively classifying information. However, because of the risks involved, it is critical to refer to classification guidance, such as SCGs, to ensure otherwise unclassified information does not become classified when you use it in a new document.

There are some special procedures to follow whenever you classify information by compilation. First, you must place a clearly worded explanation of the basis for classification by compilation on the face of the new document or include it in the text. You must also mark each element of information individually, according to its classified content. This will allow subsequent derivative classifiers to use the individual elements at their original classification level.

2. Examples

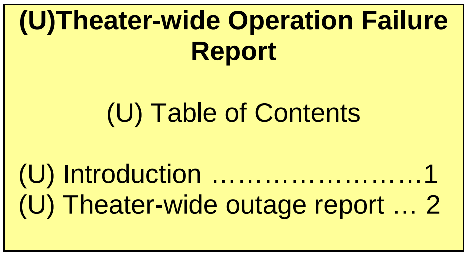
Let's look at an example of classification by compilation. You have two Theater-Wide Operation Failure Reports, both of which are unclassified. When you refer to the SCG below, you can verify this fact in row 3.3.2.8:

Security Classification Guide

	U	C	S	TS
3.3.2.8 Single theater-wide operation failure report, outage report, problem report, or investigation report	X			
3.3.2.9 Compilation of 2 or more theater-wide operation failure reports, outage reports, problem reports, or investigation reports within the same document			X	

Therefore, if you create a new document that mentions either report alone, that new document will also be unclassified. But the *next* row in the SCG indicates that if you compile two or more of the listed report types into a single document, it is a different situation entirely.

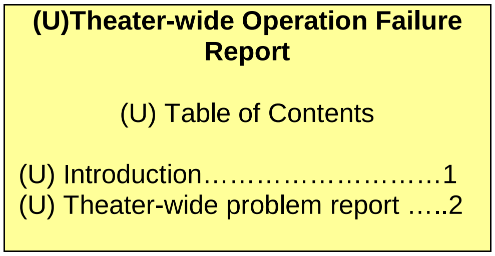
Imagine you need to create an Investigation Report that summarizes the contents of two Theater-Wide Operation Failure Reports:



(U)Theater-wide Operation Failure Report

(U) Table of Contents

(U) Introduction ……………………1
(U) Theater-wide outage report … 2

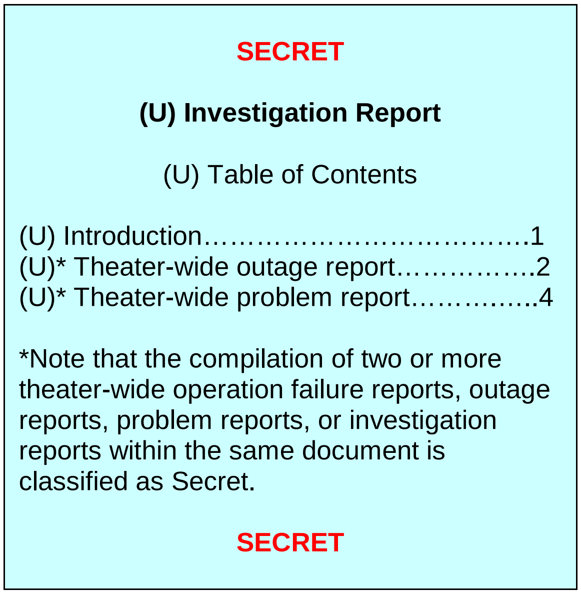


(U)Theater-wide Operation Failure Report

(U) Table of Contents

(U) Introduction……………………….1
(U) Theater-wide problem report …..2

When you aggregate these unclassified pieces of information in a new document, the SCG indicates that the information taken *together* should be classified as Secret.



SECRET

(U) Investigation Report

(U) Table of Contents

(U) Introduction……………………………….1
(U)* Theater-wide outage report…………….2
(U)* Theater-wide problem report…………..4

*Note that the compilation of two or more theater-wide operation failure reports, outage reports, problem reports, or investigation reports within the same document is classified as Secret.

SECRET

Note that the individual pieces of information should still be marked unclassified, consistent with their original classification. You are also required to explain the basis for your classification by compilation. The Note on the report above is one example of how you might do so. If you think classification by compilation applies to your situation, refer to your classification guidance. Although classification by compilation may be rare, some types of information are more likely to be subject to it. Here are some examples:

Example: Budget and Schedule of Distribution

	U	C	S	TS
3.3.3.7 Budget	X			
3.3.3.8 Schedule of Distribution	X			
3.3.3.9 Compilation of both budget and schedule of distribution within the same document		X		

Example: Staffing and Equipment Allowances

	U	C	S	TS
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	

Example: Mission and Geographic Location

	U	C	S	TS
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	

Seeking Further Guidance

1. When and Where to Seek Guidance

An important aspect of your responsibilities as a derivative classifier is to use your subject matter and classification expertise to analyze the information you are working with. If the classification in the existing content seems incorrect, or there is conflicting guidance from authorized sources, you are required to seek further guidance.

Remember, as a derivative classifier, you are not authorized to make original classification decisions. Only the cognizant original classification authority has that authority. Rather, your duty is to responsibly derivatively classify new documents based on classification guidance, and to seek clarification or further direction when the classification guidance is in question.

Examples of issues that may lead you to believe that an existing document is incorrectly marked include: the level of classification; the duration of the classification; special control requirements; and outdated classification guidance.

When there is a conflict between an existing source document and an SCG, the SCG takes precedence.

When you are unsure of how to mark the new document, DoD employees should contact their security manager or OCA, and contractor employees should contact their FSO or Government Contracting Authority. Your community will define the appropriate chain-of-command or channels for resolving such issues.

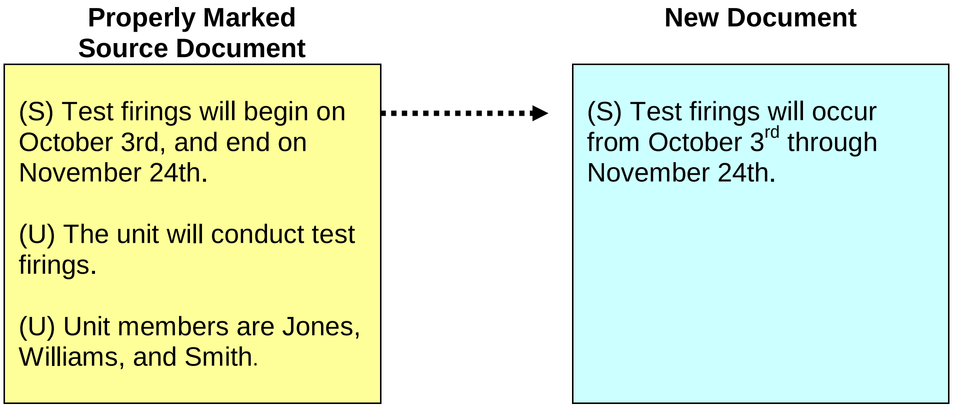
When in doubt, you should always seek additional guidance, rather than guess or speculate how to mark the new document. Remember, your derivative classification determinations may have far-reaching effects on national security and the efficient use of resources.

Review Activity

Question 1

Using the source document and the SCG, identify the concept used to determine the derivative classification of the new document.

○ Contained in
○ Revealed by
○ Classification by compilation



Properly Marked Source Document

(S) Test firings will begin on October 3rd, and end on November 24th.

(U) The unit will conduct test firings.

(U) Unit members are Jones, Williams, and Smith.

New Document

(S) Test firings will occur from October 3rd through November 24th.

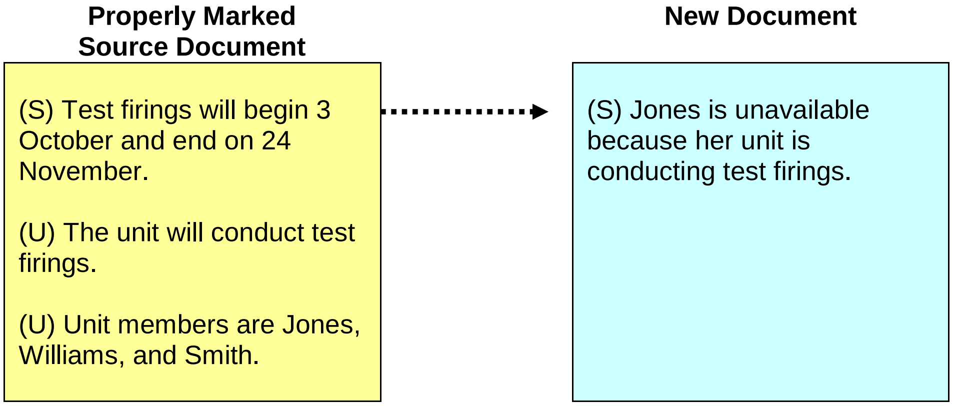
Security Classification Guide

	U	C	S	TS
The unit will conduct test firings.	X			
Test firing dates			X	
Unit members are Jones, Williams, and Smith.	X			
Compilation of unit member names and fact that the unit will conduct test firings			X	

Question 2

Using the SCG, identify the concept used to determine the derivative classification of the new document.

○ Contained in
○ Revealed by
○ Classification by compilation



Properly Marked Source Document

(S) Test firings will begin 3 October and end on 24 November.

(U) The unit will conduct test firings.

(U) Unit members are Jones, Williams, and Smith.

New Document

(S) Jones is unavailable because her unit is conducting test firings.

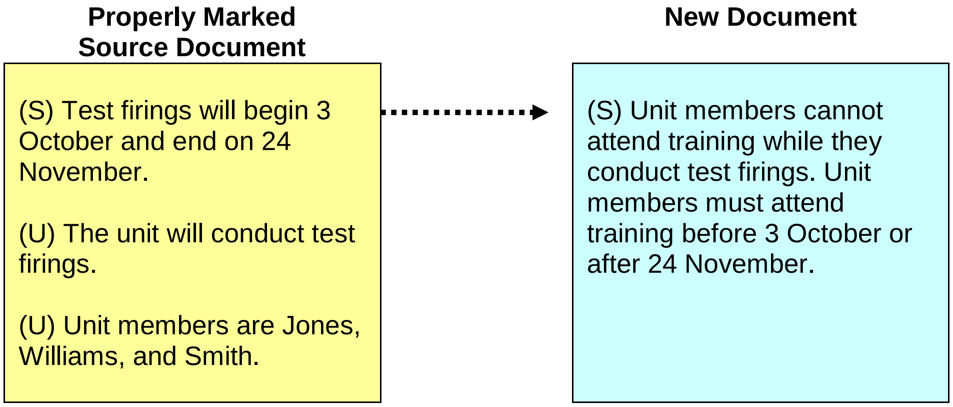
Security Classification Guide

	U	C	S	TS
The unit will conduct test firings.	X			
Test firing dates			X	
Unit members are Jones, Williams, and Smith.	X			
Compilation of unit member names and fact that the unit will conduct test firings			X	

Question 3

Using the SCG, identify the concept used to determine the derivative classification of the new document.

○ Contained in
○ Revealed by
○ Classification by compilation



Properly Marked Source Document

(S) Test firings will begin 3 October and end on 24 November.

(U) The unit will conduct test firings.

(U) Unit members are Jones, Williams, and Smith.

New Document

(S) Unit members cannot attend training while they conduct test firings. Unit members must attend training before 3 October or after 24 November.

Security Classification Guide

	U	C	S	TS
The unit will conduct test firings.	X			
Test firing dates			X	
Unit members are Jones, Williams, and Smith.	X			
Compilation of unit member names and fact that the unit will conduct test firings			X	

Lesson Conclusion

In this lesson you learned about the key concepts in derivative classification: contained in, revealed by, and classification by compilation.

Contained in:	**Definition:** Incorporating classified information from an authorized source of classification guidance into a new document • No additional interpretation/analysis needed to deduce classification
Revealed by:	**Definition:** Incorporating classified information into a new document that is *NOT* clearly stated in an authorized source of classification guidance • Additional interpretation or analysis is needed to deduce the classification
Compilation:	**Definition:** Combining or associating individual pieces of information with one classification level to reveal information that is classified at a higher level **Requirements:** • Explain the basis for classification by compilation on the face of the document or in the text • Mark each portion individually according to its classified content

You also learned about when and where to seek additional guidance when performing derivative classification.

Answer Key

Question 1

The classified information is **contained in** the existing document and has been paraphrased in the new document. The SCG identifies the test firing dates as Secret information. No additional interpretation was needed to identify this information's classification.

Question 2

Both pieces of information are unclassified on their own, but together, they are **classified by compilation**. The SCG identifies the compilation of the unit members' names and the fact that the unit is conducting test firing as Secret information.

Question 3

The classification is **revealed by** analyzing the information. The SCG identifies the test firing dates as Secret information. By analyzing the information in the new content, the reader is able to deduce that test firing will occur between 3 October and 24 November.

Student Guide

Course: Derivative Classification

Lesson: Limitations, Prohibitions and Challenges

Introduction

As a derivative classifier, you must be aware of the limitations and prohibitions of classifying information, including how classification and marking of information affect the sharing of information within the government and with the public. You must also be aware of management actions and sanctions that could result if you improperly classify information or compromise classified information. And you must know when and how to challenge the improper classification of information.

Lesson Objectives

- Explain limitations and prohibitions of classifying information
- Explain how information should be classified and marked to promote information sharing
- Identify actions that may result in sanctions
- Recognize that knowing, willful, or negligent unauthorized disclosure results in sanctions
- Recognize the range of possible sanctions for information security incidents
- Explain the reasons and procedure for challenging improper classification of information

Limitations and Prohibitions

1. Limitations

Only certain types of information may be classified or maintained as classified. Here are the three criteria information must meet in order to be classified. First, the information must be owned by, produced by or for, or be under the control of the U.S. Government. Second, the unauthorized disclosure of the information must be reasonably expected to cause damage, serious damage, or exceptionally grave damage to national security. And third, the information must concern at least one of the eight categories specified in section 1.4 of Executive Order 13526, Classified National Security Information. The categories are as follows:

- Military plans, weapon systems, or operations
- Foreign government information (FGI)

- Intelligence activities (including covert action), intelligence sources or methods, or cryptology
- Foreign relations or foreign activities of the United States, including confidential sources
- Scientific, technological, or economic matters relating to 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
- The development, production, or use of weapons of mass destruction

2. Prohibitions

As you know, the only lawful reason to classify information is to protect national security. And that information must be declassified as soon as it no longer qualifies for classification. Information must not be classified, continue to be maintained as classified, or fail to be declassified for any other reason. Information is prohibited from being classified to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, organization, or agency, to restrain competition, or to prevent or delay the release of information that does not require protection in the interests of national security. In addition, basic scientific research and its results cannot be classified unless that information is clearly related to national security.

3. Information Sharing

The purpose of properly classifying only what is necessary to be classified and only for as long as necessary is to promote the sharing of information within the Federal government, across state, local, and tribal governments, with coalition partners, with law enforcement agencies, and with the general public. To promote information sharing, certain guidelines must be followed in DoD Manual 5200.01, Volumes 1 and 2, when classifying and marking information. Not only does an original classification authority have to understand these guidelines when making an original classification decision, but you, as a derivative classifier must understand them as well.

First, avoid unnecessary classification or over-classification. For example, when classified information constitutes only a small portion of an otherwise unclassified document, prepare a classified attachment, addendum, annex, or enclosure so that only the necessary information is marked as classified rather than marking the whole document as classified. And information should not be classified if there is significant doubt that it should be classified. Information should be classified at the lower level if there is doubt about its level of classification. Finally, dissemination markings should only be used when absolutely necessary. For example, the ORCON dissemination marking is used to mark information that requires the originator’s consent for further dissemination or extraction of information when the classification level and other controls alone are insufficient to control dissemination. However, the ORCON marking must be applied carefully as it can impede efficient information sharing.

4. Actions Resulting in Sanctions

As a Department of Defense (DoD) military or civilian employee, you may be subject to sanctions if you violate any of these policies in DoD Manual 5200.01, Volumes 1 to 4. If you intentionally or inadvertently disclose classified information to unauthorized individuals, you may be subject to sanctions. If you classify or continue classification of information in violation of the Manual, you may be subject to sanctions. If you create or continue a special access program (SAP) contrary to requirements in the Manual, you may be subject to sanctions. Cleared contractor employees are subject to sanctions for violating any policies in the NISPOM.

5. Types of Sanctions

Sanctions vary depending on the violation and they range from administrative sanctions to the Uniform Code of Military Justice (UCMJ) sanctions to criminal sanctions. Administrative sanctions include suspension without pay, revocation of your security clearance, termination of employment, and loss of DoD contracts. UCMJ sanctions for military personnel include loss of rank, loss of pay, dishonorable discharge and incarceration. Criminal sanctions include incarceration, fines, and loss of Federal retirement benefits.

Challenges

1. How to Challenge Classification Decisions

As a derivative classifier, what should you do if you come across information that you think was improperly or unnecessarily classified?

If you have substantial cause for doubt, you are expected to challenge the classification. Before you create a formal challenge, you should first challenge the information informally. First ask your security manager or supervisor about your concerns. Then, if necessary, you may contact the original classification authority (OCA) for clarification regarding the classification. He or she may be able to address your concerns.

If informally questioning the information does not resolve the issue, initiate a formal challenge. Once initiated, the classifying agency must provide a written response within 60 days. If they are unable to respond fully, the agency must acknowledge your challenge and provide an estimated date for their response. As this acknowledgement will indicate, if they can't provide a response within 120 days, you as the challenger have the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP). Note that the classifying agency does not need to process the challenge if the information has been challenged in the last two years, or if it is currently under review. Also note that information which is being challenged must remain classified and be safeguarded appropriately until a decision is made to declassify it.

Review Activity

Question 1

Select True or False for each statement.

		True	**False**
You should first contact your security manager or supervisor if you have concerns or suspect information may be improperly classified.		○	○
You are subject to sanctions if you improperly classify information.		○	○
Information may be classified to prevent embarrassment to the U.S. Government.		○	○
Information may be classified if it is foreign government information (FGI).		○	○

Lesson Conclusion

In this lesson you learned about limitations and prohibitions in classifying information. You also learned what actions are subject to sanctions and what types of sanctions may apply. You learned how to challenge information that is improperly classified as well as some guidelines for classification and markings to promote information sharing.

Answer Key

Question 1

		True	False
You should first contact your security manager or supervisor if you have concerns or suspect information may be improperly classified.		●	○
Feedback: *When you suspect improper classification or over-classification, first contact your security manager or supervisor and then the OCA if necessary.*			
You are subject to sanctions if you improperly classify information.		●	○
Feedback: *You are subject to sanctions if you improperly classify information, disclose classified information or controlled unclassified information to unauthorized individuals, or create or continue a special access program contrary to DoD policy requirements.*			
Information may be classified to prevent embarrassment to the U.S. Government.		○	●
Feedback: *Information may not be classified to prevent embarrassment to the U.S. Government.*			
Information may be classified if it is foreign government information (FGI).		●	○
Feedback: *Foreign government information (FGI) may be classified as long as its disclosure could be expected to cause damage to national security and as long as that information is under the control of the U.S. Government.*			

Student Guide

Course: Derivative Classification

Lesson: Practical Exercise

Introduction

In this lesson, you will practice how to derivatively classify a document. As you go through the practical exercise, use what you have learned about classification concepts, authorized sources, and the process to follow when derivatively classifying documents.

As you complete each activity, you can check your answers in the Answer Key at the end of this Student Guide.

Lesson Objectives

- Practice derivatively classifying a document
- Apply classification concepts
- Identify authorized sources
- Follow the derivative classification process

Scenario 1

Your office is tasked with recording meeting minutes for a new series of planning meetings. You must prepare and forward the minutes, along with the Commander's comments, to staff Department Heads and Special Assistants. Below you will see a series of questions about the classification of the new document you are creating.

There are two sources of classification guidance for you to use to determine the classification of your new document, the source document that you received at the first planning meeting and the Security Classification Guide (SCG).

Properly Marked Source Document:

SECRET

1. (S) This is to announce the intent to hold a series of internal planning meetings in support of exercise OBSCURE NIMBUS XX, which is being hosted by Pandora Naval Station (PNS) and scheduled to take place from 15-25 March 20XX. The first planning meeting will be held on 14 August 20XX in the Rocky Oaks Conference Center. LT Herman Lukowicz, Administration Officer will serve as point of contact.

2. (C) Attendance at this initial planning meeting will be limited to PNS Administration, Operations, Training, Maintenance, and Supply Department Heads. The next meeting will be held at the PNS Training Facility, Bldg. 112. Attendance will include all Department Heads, their key personnel, and Special Assistants.

SECRET

Security Classification Guide:

	U	C	S	TS
Intent to hold series of internal planning meetings			X	
Name of exercise is OBSCURE NIMBUS			X	
PNS is hosting meetings	X			
Exercise dates	X			
Attendance limited to PNS Administration, Operations, Training, Maintenance, Supply Department Heads		X		
Future meeting location		X		
Future meeting attendees		X		
Compilation of future meeting attendees and meeting dates				X
Point of contact's name	X			

1. Activity 1

Derivative Document:

> 1. (__) The planning meeting for exercise OBSCURE NIMBUS XX was held on 14 August 20XX. Target audience was present, participative, resourceful, and enthusiastic. The groundwork for this year's exercise scheduled for 15-25 March 20XX has been positively established, and meeting minutes are forwarded as enclosure (1).
>
> 2. (__) My point of contact in this matter is LT Herman Lukowicz, Administration Officer.
>
> 3. (__) The next meeting will be held at the PNS Training Facility, Bldg. 112 to continue planning for the exercise.

Question 1

What is the correct portion marking for Paragraph 1 in the derivative document?

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

Question 2

What is the correct portion marking for Paragraph 2 in the derivative document?

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

Question 3

What is the correct portion marking for Paragraph 3 in the derivative document?

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

2. Activity 2

Refer to the source document and the SCG above to answer the following questions:

Your SCG and your properly marked source document both indicate that the exercise name is classified as Secret. LT Lukowicz, however, tells you that the exercise name has been recently declassified. Which source(s) should you use to derivatively classify the material?

○ LT Lukowicz
○ SCG and properly marked source document

3. Activity 3

Now use these sources of classification guidance to answer the question below.

Properly Marked Source Document:

SECRET

1. (S) This is to announce the intent to hold a series of internal planning meetings in support of exercise OBSCURE NIMBUS XX, which is being hosted by Pandora Naval Station (PNS) and scheduled to take place from 15-25 March 20XX. The first planning meeting will be held on 14 August 20XX in the Rocky Oaks Conference Center. LT Herman Lukowicz, Administration Officer will serve as point of contact.

2. (C) Attendance at this initial planning meeting will be limited to PNS Administration, Operations, Training, Maintenance, and Supply Department Heads. The next meeting will be held at the PNS Training Facility, Bldg. 112. Attendance will include all Department Heads, their key personnel, and Special Assistants.

SECRET

Security Classification Guide:

	U	**C**	**S**	**TS**
Intent to hold series of internal planning meetings			X	
Name of exercise is OBSCURE NIMBUS			X	
PNS is hosting meetings	X			
Exercise dates	X			
Attendance limited to PNS Administration, Operations, Training, Maintenance, Supply Department Heads		X		
Future meeting location		X		
Future meeting attendees		X		
Compilation of future meeting attendees and meeting dates				X
Point of contact's name	X			

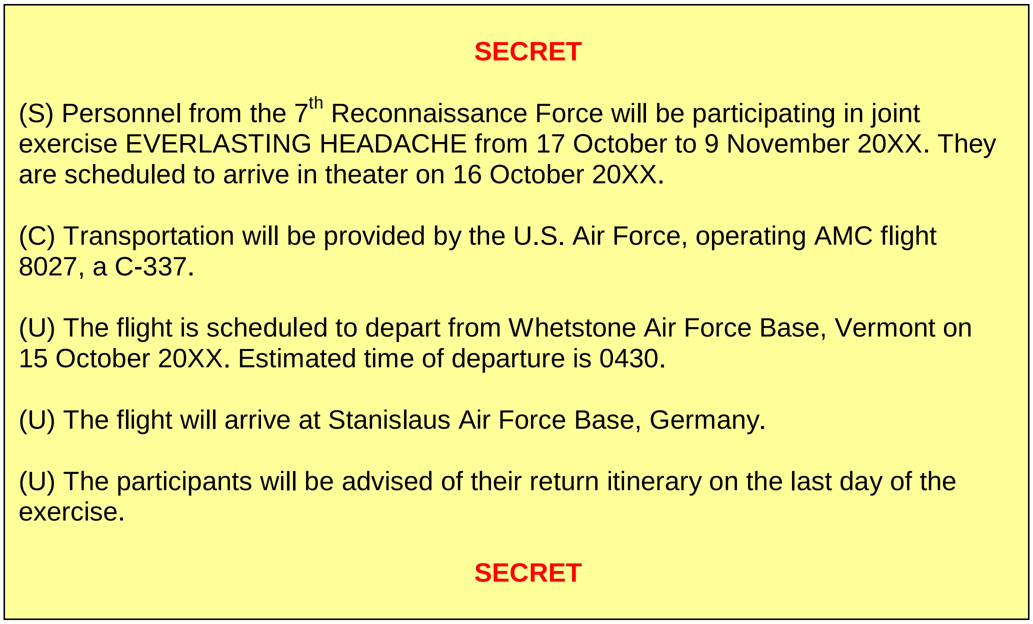
If your SCG says the exercise name is Secret, but your properly marked source document says the exercise name is unclassified, which source should you use to derivatively classify the material?

○ Properly marked source document
○ SCG

Scenario 2

After receiving a classified document, your office is required to issue a letter outlining personnel movement information. In the following activities, you will see a series of questions about the classification of the new document you are creating. You will have two authorized sources of classification guidance available to you. You will, of course, have the properly marked source document, and you will also have a Security Classification Guide. Use both of these authorized sources to help you answer the questions.

Properly Marked Source Document:



SECRET

(S) Personnel from the 7th Reconnaissance Force will be participating in joint exercise EVERLASTING HEADACHE from 17 October to 9 November 20XX. They are scheduled to arrive in theater on 16 October 20XX.

(C) Transportation will be provided by the U.S. Air Force, operating AMC flight 8027, a C-337.

(U) The flight is scheduled to depart from Whetstone Air Force Base, Vermont on 15 October 20XX. Estimated time of departure is 0430.

(U) The flight will arrive at Stanislaus Air Force Base, Germany.

(U) The participants will be advised of their return itinerary on the last day of the exercise.

SECRET

Security Classification Guide:

	U	C	S	TS
In theater arrival dates			X	
Joint exercise name			X	
Joint exercise dates			X	
Name of departure Air Force Base	X			
Name of arrival Air Force Base	X			
Compilation of departure and arrival Air Force Bases		X		
Flight number		X		
Exercise participants		X		
Compilation of flight number and exercise participants			X	
Type of aircraft used for flight	X			

Here is your draft letter. The following activities will let you analyze and classify each paragraph.

Derivative Document:

(__) Request transportation assistance for a joint exercise from Whetstone Air Force Base, Vermont to Stanislaus Air Force Base, Germany.

(__) Personnel from the 7th Reconnaissance Force must arrive in theater on 16 October 20XX.

(__) The 7th Reconnaissance Force must arrive on AMC scheduled flight 8027, a C-337.

(__) The exercise begins on 17 October 20XX and will continue for twenty-four days. Request assistance for return transportation on the day following exercise completion.

1. Activity 1

What classification concept would you use to determine the correct marking for the first paragraph of your derivatively classified letter?

(__) Request transportation assistance for a joint exercise from Whetstone Air Force Base, Vermont to Stanislaus Air Force Base, Germany.

○ Compilation
○ Revealed by
○ Contained in

2. Activity 2

What is the classification for the first paragraph of your derivatively classified letter?

> (__) Request transportation assistance for a joint exercise from Whetstone Air Force Base, Vermont to Stanislaus Air Force Base, Germany.

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

3. Activity 3

What classification concept would you use to determine the correct marking for the second paragraph of your derivatively classified letter?

> (__) Personnel from the 7th Reconnaissance Force must arrive in theater on 16 October 20XX.

○ Compilation
○ Revealed by
○ Contained in

4. Activity 4

What is the classification for the second paragraph of your derivatively classified letter?

> (__) Personnel from the 7th Reconnaissance Force must arrive in theater on 16 October 20XX.

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

5. Activity 5

What classification concept would you use to determine the correct marking for the third paragraph of your derivatively classified letter?

> (__) The 7th Reconnaissance Force must arrive on AMC scheduled flight 8027, a C-337.

○ Compilation
○ Revealed by
○ Contained in

6. Activity 6

What is the classification for the third paragraph of your derivatively classified letter?

> (__) The 7th Reconnaissance Force must arrive on AMC scheduled flight 8027, a C-337.

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

7. Activity 7

What classification concept would you use to determine the correct marking for the last paragraph of your derivatively classified letter?

> (__) The exercise begins on 17 October 20XX and will continue for twenty-four days. Request assistance for return transportation on the day following exercise completion.

○ Compilation
○ Revealed by
○ Contained in

8. Activity 8

What is the classification for the last paragraph of your derivatively classified letter?

> (__) The exercise begins on 17 October 20XX and will continue for twenty-four days. Request assistance for return transportation on the day following exercise completion.

○ Unclassified
○ Confidential
○ Secret
○ Top Secret

9. Activity 9

Which of the following methods would you use to determine classification of this paragraph?

> (__) Personnel from the 7th Reconnaissance Force will be participating in joint exercise EVERLASTING HEADACHE from 17 October to 9 November 20XX. They are scheduled to arrive in theater on 16 October 20XX.

○ Seek guidance from an appropriate authority (e.g., Security Manager, OCA, FSO, or GCA)
○ Ask LT Lukowicz to mark the document
○ Use the Security Classification Guide
○ Use your subject matter expertise and experience to create the original classification

10. Activity 10

If the SCG was not available, how would you determine classification? Select the best response.

> (__) Personnel from the 7th Reconnaissance Force will be participating in joint exercise EVERLASTING HEADACHE from 17 October to 9 November 20XX. They are scheduled to arrive in theater on 16 October 20XX.

○ Seek guidance from an appropriate authority (e.g., Security Manager, OCA, FSO, or GCA)

○ Ask LT Lukowicz to mark the document

○ Use the properly marked source document

○ Use your subject matter expertise and experience to create the original classification

Summary

Congratulations! You have completed the Practical Exercise for the Derivative Classification course.

Answer Key

Scenario 1

1. **Activity 1**

Question 1

The information in this paragraph is **contained in** the properly marked source document, where it is marked Secret. The SCG confirms this classification, so it should be marked **Secret** in the derivative document.

Question 2

The SCG indicates the point of contact's name is **unclassified**.

Question 3

The information in this paragraph is restating information classified as **Confidential** in the existing document and the SCG.

2. **Activity 2**

The available sources of classification guidance (**SCG and source document**) classify the exercise name as Secret. LT Lukowicz is not an authorized source; however, you should research his disclosure through appropriate channels.

3. **Activity 3**

When there is a conflict between authorized sources, the **SCG** takes precedence over a properly marked existing document. You should ask for further guidance, however, to call attention to the inconsistency between the authorized sources of guidance.

Scenario 2

1. **Activity 1**

Based on the SCG, **compilation** is required to determine the classification. When combined or associated, these elements of information warrant classification.

2. **Activity 2**

Based on the SCG, compilation of departure and arrival Air Force Bases is **Confidential**.

3. Activity 3

Based on the properly marked source document, the in-theater arrival date can be determined without further interpretation or analysis; it is **contained in** the document.

4. Activity 4

Based on the properly marked source document, the in-theater arrival date is **Secret**.

5. Activity 5

Based on the SCG, **compilation** is required to determine the classification. When combined or associated, these elements of information warrant a higher classification.

6. Activity 6

Based on the SCG, compilation of exercise attendees and flight number is **Secret**.

7. Activity 7

Based on the properly marked source document, the information is not clearly stated, but can be determined by calculating the start date and number of days. This information is deduced or **revealed by** analysis of the information presented.

8. Activity 8

The SCG indicates that the exercise dates are **Secret**.

9. Activity 9

When a properly marked existing source document is unclear or conflicts with an SCG, use the classification indicated in the **Security Classification Guide**. Next, you would ask your Security Manager, OCA, FSO, or GCA for guidance. LT Lukowicz is not an authorized source and the existing document does not contain sufficient marking. Derivative classifiers are not authorized to make original classification decisions.

10. Activity 10

Use the properly marked source document. Next, you would ask your Security Manager, OCA, FSO, or GCA for guidance. LT Lukowicz is not an authorized source, and the existing document does not contain sufficient marking. Derivative classifiers are not authorized to make original classification decisions.

Student Guide

Course: Derivative Classification

Lesson: Course Conclusion

Course Summary

Protecting classified information from disclosure is a critical responsibility of the individuals who work with it. Whenever new classified documents or materials are derived from an authorized source of classification guidance, derivative classifiers are responsible for ensuring the information is accurately identified. This course taught you about the resources you must use and the processes you must follow to properly perform derivative classification.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Derivative Classification Basics
- Classification Concepts
- Limitations, Prohibitions and Challenges
- Practical Exercise
- Course Conclusion

Course Objectives

You should now be able to:

√ Identify the responsibilities associated with derivatively classifying information

√ Identify the processes and methods for derivatively classifying information

√ Identify authorized sources to use when derivatively classifying information

√ Applying authorized sources, derivatively classify information based on the concepts of “contained in,” “revealed by,” and "compilation"

√ Explain the limitations and prohibitions of classifying information and ways to promote information sharing through classification

√ Identify the process for managing classification challenges, security incidents, and sanctions

Conclusion

Congratulations. You have completed the Derivative Classification Course. To receive credit for this course, you *must* take the Derivative Classification Examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam. For more information and additional guidance on how to mark classified information, use STEPP to register for the "Marking Classified Information" eLearning course (IF105.16).