

LESSON 2

BASIC CLASSIFICATION MANAGEMENT



Original Classification Authorities
OCAs

In Lesson 1, you learned that the Information Security Program provides uniform guidance for the management of classified information. In this lesson, we'll define the three levels of classification and identify the basis for them. We'll discuss original classification authority - where it comes from and how personnel in the Executive Branch become original classification authorities (OCAs). We'll cover OCA training and limitations on OCA authority. We'll look one by one at the determinations that an OCA must make before originally classifying information. We'll wind up by looking briefly at derivative classification and at the responsibilities of - and procedures for - those who implement the OCAs' decisions. At the end of this lesson, you will be able to do the following:

- Define the terms Top Secret, Secret, and Confidential as they apply to information.
- Describe original classification authority.
- Identify the steps in the original classification process.
- Distinguish between original and derivative classification actions.
- Identify the responsibilities of original classifiers and derivative classifiers.
- Explain tentative classification and how to challenge a classification.

Classification Designation



Rudy Tucker

"In our last session," Wally begins, "we defined classified information as *official government information that has been determined to require protection against unauthorized disclosure and that has been so designated*. We noted that the three designations for classified information are *Top Secret, Secret, and Confidential*. Can anyone tell me what determines whether information is designated Top Secret, Secret, or Confidential?"

"If unauthorized disclosure causes a lot of damage, the information is designated Top Secret. If only minor damage will occur, the information is classified Confidential. Secret falls somewhere in between," offers Rudy Tucker.

"Right, Rudy. The difference between the designations is the *extent of the damage that unauthorized disclosure would likely cause*.

Designation	Unauthorized disclosure of this information could reasonably be expected to cause
Top Secret	exceptionally grave damage to our national security that the Original Classification Authority is able to identify or describe.
Secret	serious damage to our national security that the Original Classification Authority is able to identify or describe.
Confidential	damage to our national security that the Original Classification Authority is able to identify or describe.

Be aware that *all* classified information can cause damage to the national security if disclosed without authorization. Don't fall into the trap of thinking of Confidential information as *only Confidential*. And if you hear of anyone doing so, you may want to take them aside and give them a bit of one-on-one security education. Remember, *all three types of classified information must be protected.*"

The Two Types of Classification

"We've defined classified information and discussed the levels of security classification. Now it's time we talked about how information becomes classified," Wally continues.

Information becomes classified by either...

◆ **Original classification**

or

◆ **Derivative classification**

Original Classification Authority



Original Classification Authority

"Let's look first at original classification. Original classification is an *initial determination that information needs to be protected*. This determination can be made only by a designated *Original Classification Authority* (OCA.) There are about 4,130 OCAs in the Executive Branch and about 1,200 in the DoD. What positions in the DoD carry original classification authority? Any ideas?"

"I'll bet the Secretary of Defense is an OCA," Alice responds.

"And how about the Secretaries of the Military Departments?" Peg suggests.

"This is too easy! Yes, the President has delegated original classification authority to the people in those positions. And since they are all very busy, they have delegated original classification authority to other officials who need it. For example, at DIVA we have one OCA - General Kent."

"What happens when he's away from DIVA and original classification decisions need to be made?" asks Rudy.

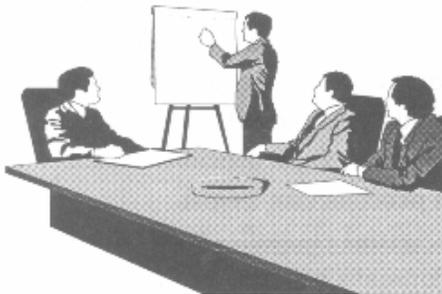
"Good question! People who hold positions move on to other positions and, as Rudy points out, they're sometimes away on business or vacation. That's why . . .



Within the DoD, original classification authority is delegated to the occupant of a position - not a person by name.

That way, whoever is occupying the position, has the authority that goes with it. For instance, in General Kent's absence, DIVA's Deputy Director, Captain Douglas, assumes the position of Director. Since it's the position that has the authority, while Captain Douglas serves as Acting Director, she can exercise original classification authority.

Note carefully that not all OCAs are delegated Top Secret original classification authority. Some OCAs are delegated Secret authority, while others are delegated Confidential authority. *The delegation of the authority will specify the highest level at which the OCA can classify a piece of information.* They can classify at that level and below. OCAs with Confidential original classification authority can't assign the designations Secret or Top Secret to information. And OCAs with Secret original classification authority can't assign the designation Top Secret."



OCAs in training

"It seems to me," Rudy says, "that being an OCA is a big responsibility. How do these folks learn what they're supposed to do?"

"All OCAs are required to go through training before they can make any original classification decisions. This training covers the fundamentals of security classification, limitations on an OCA's authority to classify information, and an OCA's responsibilities."

"Whose job is it to train the OCA?" Rudy asks.

"The security manager at the OCA's organization," Wally replies.

"But, Wally, those people at high level positions, such as General Kent, are really busy. How are you going to make sure they get the proper training?"



orientation package

"E.O. 12958, as amended, stresses that OCAs must be aware of their responsibilities. After all, they're accountable for their classification decisions! To ensure accountability, the E.O. makes the management of classified information a critical element of their performance evaluations. Our security manager tapped me to give the training to General Kent. I used the OCA orientation package developed by the Defense Security Service Academy.

The Original Classification Process



Now let's look at how an OCA classifies information. Before an OCA can make a classification determination, each item that may require protection needs to be identified. This is called *identification of specific information*. Then the original classification process can begin. Although the process of original classification can be complex and difficult, it consists basically of the following steps.

Original Classification Process

- 1. Determine current classification status**
- 2. Determine if official government information**
- 3. Determine if in an authorized category**
- 4. Determine if prohibited intent or type**
- 5. Determine likelihood of damage to national security and be able to identify or describe the damage**
- 6. Weigh advantages and disadvantages**
- 7. Assign a level of classification**
- 8. Make a decision about the duration of classification**
- 9. Communicate the decision**

Step 1. Determine Current Classification Status

In this step, the OCA must answer the question, 'Is the piece of information *already classified?*' If the answer is yes, the OCA stops. There's no need to classify the information a second time! If the answer is no, the OCA proceeds to the next step.

Step 2. Determine If Official Government Information



Next, to be eligible for classification, information must be *official government information*. Last time we said that official government information is owned by, produced by, or for, or under the control of the U.S. Government. Now that you know the long version, we can simply say that the U.S. *Government must own, have a proprietary interest in, or control the information.*

Step 3. Determine If In An Authorized Category

Authorized Classification Categories, Section 1.4 of E. O. 12958, as amended:

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

Step 4. Determine If Prohibited Intent or Type

The OCA must rule out that classification is being considered for some reason other than to protect the national security. In other words, classification must never be used as a smoke screen to cover up or promote wrongdoing.

Prohibitions, E.O. 12958, as amended:

You cannot classify information 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.**

You cannot classify . . .

- **Basic scientific research information unless it clearly relates to national security.**

Step 5. Determine Likelihood Of Damage

This step and the next one are particularly difficult. The OCA's good judgment is essential.

The OCA must now determine that *the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security*. And this determination can't be just a vague notion or a hunch. E.O. 12958, as amended, requires that the damage *can be identified or described*."

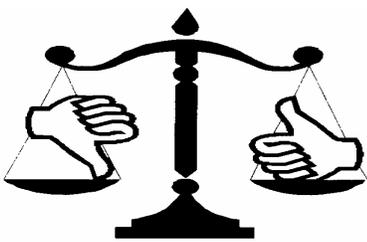


"Does the OCA have to give a written description of the damage each time a decision is made to classify information?" Josh asks.

"No, it's not necessary for the OCA to produce a written description of the damage at the time of classification. But the OCA must be prepared to do so if the information becomes the subject of a *classification challenge* - a request for mandatory review for declassification, or a request for release under the Freedom of Information Act (FOIA), or a damage assessment."

"As you can see, there are no easy answers, pat solutions, or handy formulas for the OCA's decisions."

Step 6. Weigh Advantages and Disadvantages



Josh says, "It must cost a lot of money to keep information protected - buying the safes to store it and clearing the people to have access to it."

"You bet it does! In fact, the next step is to determine the *advantages and disadvantages of classification*. Here is where the OCA, who is used to making management decisions on a daily basis, must consider the benefits and drawbacks of the classification. If the OCA has a significant doubt about classification during this step, the information should not be classified.

Step 7. Assign the Level Of Classification



"Once the determination to classify is made," Wally continues, "the OCA must assign a level of classification. Remember, the levels of classification are based upon the *degree of damage unauthorized disclosure would likely cause*. Unfortunately, there are no handy formulas to determine degrees of damage. Here again it's a judgment call. If there's a significant doubt about the appropriate level of classification, the information must be classified *at the lower level*."

Step 8. Set the Duration

"At the same time an OCA decides that information should be classified, he or she must make a decision about *how long the classification should last*," Wally

says. "The OCA has several options available. We'll look at them in a future session.

Step 9. Communicate the Decision

"Finally, the OCA must *communicate the decision*. An OCA can communicate a classification decision in two main ways.

Two ways to communicate an original classification decision are...

- **Issuing classification guidance.**
- **Ensuring that the information is properly marked in a document.**



General Kent

Let's say you're working on a new project. The project involves the creation of a new military aircraft - the TK47 Bomber. Since it's a new project and a new aircraft, the related information is also new. First, General Kent will identify any information that may require protection. He then determines which of that information needs to be classified and assigns a level of classification to each element of information. Perhaps he decides that certain information related to the design of the aircraft will be classified Secret. Other information related to the aircraft's capabilities will be classified Confidential.



a new project

"How does General Kent communicate his classification decisions concerning the TK471 Bomber project to the rest of us? He issues *classification guidance*. Classification guidance can take many forms - security classification guides, project directives, memoranda, and plans. In this case, General Kent will issue a Security Classification Guide for the TK47 Bomber. The Executive Order requires each OCA to issue a security classification guide for each classified system, program, plan, and project. These guides contain

instructions on the classification of project information, including the level of classification. We now cross the border from original classification to ...

Derivative Classification



derivative classification

"As a member of the project team, you are responsible for applying General Kent's classification decisions to project information. Suppose you're developing a report about the project. The first sentence you write is about the aircraft's design. You need to find out if the information is classified, and, if so, at what level. You look in the TK47 Bomber Security Classification Guide. The guide indicates that the aircraft design is classified Secret. Since you include information in your sentence about the design of the TK47 Bomber, you classify your sentence Secret. Then you continue developing the rest of your report in a similar manner. What you're doing is called *derivative classification*."

"So you're saying that only OCAs can perform original classification, but people like us can perform *derivative classification*," Josh says."

"And in the DoD we refer to derivative classification *responsibility*, not derivative classification authority. The authority is assumed."

Derivative classification is the responsibility of...

- **All who apply markings in accordance with classification guidance**
- and
- **All who incorporate, paraphrase, restate, or generate in new form, information that is already classified.**



"Wally, you gave an example of someone applying markings in accordance with classification guidance from an OCA. Could you give an example of the other way to perform derivative classification?" Peg asks.

"Sure, Peg. Let's say you're tasked with writing an information paper about the Russian military. You discover that there is no Security Classification Guide available on the subject. However, you use several classified documents to develop your report. You have to classify your document in accordance with instructions provided by those documents. In this case, *the documents' markings are your instructions.*



derivative classification

"Let me give you a simple situation. Suppose document 1 contains a one sentence paragraph that says 'Russian soldiers receive 80 hours of language training every year.' The paragraph is marked (S), which indicates Secret. In your report you write 'Russian soldiers are provided 80 hours of language training annually.' The words are a bit different, but the information in your sentence is the same as the information in the sentence from document 1. Since the document 1 sentence is marked (S), you should *carry forward the classification* and mark your sentence (S).

"This is a simple example. Believe me, derivative classification is *not* usually an easy process. It takes time and effort and a lot of thought. We're not going to go very deep into derivative classification now. I'm saving that."

Requesting an Original Classification Decision-----

Peg says what if I come up with information I think should be protected. It's never been classified, but I don't have the original classification authority to classify it. What do I do?"

"Good question, Peg! Let's say you think the information should be classified Secret because you think it would cause serious damage to national security if unauthorized disclosure should occur. All you do is mark the information 'TENTATIVE SECRET' and *send it to an OCA with jurisdiction over the information for a classification determination*. The OCA will make a decision and notify you. You mark your document accordingly.

Derivative Classifier's Responsibility-----



"When OCAs classify information, they are responsible for the classifications they assign. Now, if you develop a derivative document and classify it, who do you suppose is responsible for the assigned classifications?"

"My boss?" Rudy says with an innocent look.

"That's partially true, Rudy. If your boss reviews the document and signs off on it, he or she becomes *jointly responsible* for the assigned classifications. *But you are also responsible for the classification decisions. You are the accountable classifier.*

Approver's Responsibility-----



"All right, we've established that if your boss reviews your derivatively classified document and signs off on it, he or she becomes jointly responsible for the assigned classifications. Suppose your boss reviews the document you derivatively classified and doesn't agree with some of the markings you've assigned. Your boss feels that the classification guidance doesn't support the markings you've assigned. What do you suppose happens?"

"I suppose my boss would tell me what markings she disagrees with and why," Josh says. "She'd have me review the guidance and re-evaluate my

decision. I'd change or remove markings to reflect the actual classification level of the information following the classification guidance for that information."

Challenges to Classification-----

"Right! Here's another situation. Suppose you're reading a document that someone else has classified, and you find yourself disagreeing with some of the classification markings assigned to the information. Is there anything you can do?"

"Yes, I read that E.O. 12958, as amended, encourages challenges. I could get in touch with the person who classified the document and challenge the classification," Alice says.

"Right, Alice. You could contact the classifier and give the reasons why you think that the classification should be different. Or you could talk to your security manager about it. Most of the time the situation can be handled informally. But if there's a real disagreement, every DoD Component has procedures set up for you to challenge a classification you believe to be improper. If you run into a situation of this sort, come see us in the Security Office. We'll be glad to give you a hand.

Summary

"In this session you learned that classified information is designated by the extent of the damage to national security that unauthorized disclosure would likely cause and that the Original Classification Authority (OCA) is able to identify or describe: Top Secret - exceptionally grave damage, Secret - serious damage, and Confidential - damage.

"Information becomes classified by either original or derivative classification. Within the DoD original classification authority is delegated to the occupant of a position, not to a person by name. The President delegates this authority to key positions. Whoever occupies those positions may delegate authority for original classification to subordinates requiring it, and so on.



Derivative classifiers
applying markings

"OCAs are delegated authority at the highest level they may assign: Top Secret, Secret, or Confidential. OCAs must receive training before exercising their classification authority. Having identified specific kinds of information that may require protection, if the OCA 1) determines that certain information is not already classified and 2) is official government information that 3) falls within a category authorized by E.O. 12958, as amended, but that 4) is not prohibited for classification under E.O. 12958, as amended, the OCA then 5) determines the likelihood of damage to national security that can be identified or described and 6) weighs the advantages and disadvantages of classification. The OCA then 7) assigns the level of classification, 8) determines the duration of classification, and 9) communicates the decision to others by issuing classification guidance or by ensuring that information is properly marked in a document.

"Derivative classifiers apply markings following the guidance or carry forward document markings. They may challenge existing classification decisions, and if they originate information that warrants classification, they may request that an OCA review the information and make a decision regarding classification. They are responsible for the classifications they assign, and their supervisors are jointly responsible for the classifications they approve.

REVIEW EXERCISES

1. The level of classification is based on the amount of:
 - a. money that would need to be expended to mitigate the damage caused by an unauthorized disclosure.
 - b. damage that an unauthorized disclosure would cause.
 - c. foreign resources expended to compromise the information.
 - d. security resources expended to protect the information.

2. Top Secret information is information the unauthorized disclosure of which could reasonably be expected to cause _____
_____ to our national security which an OCA is able to identify or describe.

3. Within the DoD original classification is:
 - a. delegated to a position, not an individual by name.
 - b. applied every time a classified document is written.
 - c. determining whether information has already been classified, at what level, and for how long
 - d. delegated to an individual by name

4. Anyone who occupies a position with original classification authority can classify information at all three levels.

True. False.

5. The first step in the original classification process is to determine the current classification status of the information.

True. False.

6. The fifth step in the original classification process is to:
- determine if the information is official government information.
 - determine if the information is in an authorized category.
 - determine if the information has a prohibited intent.
 - determine the likelihood of damage to the national security and be able to identify or describe the damage.
7. In order to be eligible for classification, the information must fall within one of the eight categories listed in E. O. 12958, as amended.

True. False.

8. You are the Project Manager for the TX-22 aircraft and have been delegated original classification authority. You decide to classify the TX-22's maximum speed at the Secret level. What is the next step in your classification decision process?

- determine the amount of damage that would be caused by an unauthorized disclosure.
 - determine how long the classification should be applied.
 - determine how to communicate your decision.
 - weigh the advantages and disadvantages of classifying the information.
9. Derivative classification is:
- delegated to a position, not an individual by name.
 - applied every time a classified document is written
 - determining whether information has already been classified and at what level and for how long.
 - delegated to an individual by name.

10. Tentative classification is:

- a. classifying information that reveals an intelligence source.
- b. classifying two items because they are sensitive when related.
- c. classifying two or more pieces of information because when combined they reveal a more sensitive level of information.
- d. classifying information temporarily without having original classification authority.

11. The author of a derivatively classified document is not responsible for the classifications assigned in it if his/her supervisor signs it.

True. False.

12. If you disagree with the classification of an item, your options include:

- a. contacting the classifier and giving the reasons why you think the classification should be different.
- b. contacting your security manager about it.
- c. following the procedures that your Component has set up.
- d. all of the above.
- e. a and b only.

SOLUTIONS AND REFERENCES

1. b. (p. 2-2)
2. exceptionally grave damage (p. 2-2)
3. a. (p. 2-4)
4. False. (pp. 2-4-5)
5. True. (p. 2-6)
6. d. (p. 2-6)
7. True. (p. 2-7)
8. b. (pp. 2-9-10)
9. c. (pp. 2-11-12)
10. d. (pp. 2-12-13)
11. False. (p. 2-13)
12. d. (p. 2-14)