112113 Webinar

Original Classification Considerations

Good morning and thank you for standing by. As a reminder all lines will be in a listen only throughout the entire call today and today's call is being recorded. If you have any objections you may disconnect at this time. Mr. Ringrose you may now begin.

Mr. Ringrose: Thank you. Before we get started please be aware that the video portion of this webinar is being recorded. Once the red light comes on we will begin. Greetings everyone, my name is Roy Ringrose and I will be your host for the next 30 minutes. I appreciate you taking time out of your schedules to receive this information. I am an instructor here at CDSE, I am the course manager for the Security Awareness for Educators course but as of yesterday we are pulling that course down to be re-vamped, so look for it in the future. I am also an instructor in the Information Security Management. My producer today is Rachel Mongeau and before we get started Rachel will provide you with the ground rules for today's webinar and some instructions on how to use the tools you will need to participate.

Rachel: Okay, thank you Roy. You can see at the bottom left hand corner of your screen there is a notes box, and it has the call-in number and any other announcements. This will remain on screen throughout the presentation, you can always reference it. If you'd like to get a larger view of the screen, you can select the full-screen button up in the top banner of your screen. Remember though if you want to respond to a poll question you need to be out of full-screen mode, so just select the button again to get out of that mode. These poll questions, this is an example of what one looks like, and we'll pop up a few throughout the webinar, just select your answer and we'll provide some feedback. On the right there is a Q&A box if you have any questions please enter them in the box because your phone is muted and it's your only way to communicate with us. We can get to your questions at the end of the presentation; we'll also have a Q&A posted online after the webinar. You'll also find a file share box at the bottom of your screen, there are two files there, one is the webinar slides for today's presentation, and the other is an excerpt from the DoD manual, feel free to download those and print them out. I think I'm going to send this back to you Roy!

Roy: Thanks Rachel. So as she mentioned we have poll questions so let's begin with one. They are merely a knowledge check here. What's the definition of Original Classification? Looks like everybody is doing pretty good there. Let's continue on. The answer actually is C: The initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the National Security if subject to unauthorized disclosure and requires protection in the interest of National Security. I can also see why a lot of you chose B. Thank you for your response, we will continue on. Over the next thirty minutes we'll discuss the basics of Original Classification, Original Classification Authority, where does it come from, Original Classification Training, this is the training an OCA needs for Original Classification Authority, the Scope of their Authority and can that individual Assign or delegate their position to a subordinate. So let's start with our first topic. Let's begin with explaining why information is classified. We've included an excerpt from DoD Manual 5200.01, Volume 1, Enclosure 4, Paragraph 4 in the file share box that you see on your screen. This excerpt is from the manual that defines Original classification. The manual states that information must be classified only to protect National Security. Original classification is the first step in providing protection to information; all other classification decisions and safeguarding requirements are based on the original classification decision. The manual further states that if there is significant doubt about the need to classify information then the information should not be classified likewise unless they are higher than necessary classifications also prohibited. While the DoD manual describes why information will be classified, Executive Order 13526 establishes the legal authority for certain officials within the Executive Branch of the Federal Government to designate classified National Security information. The individuals who perform classification are referred to as classifiers. Additionally Executive Order 13526 mandates that "no information can remain classified indefinitely". So information must be de- classified as soon as it is no longer qualifies for classification. There are certain conditions under which information can be classified. Classifying may be appropriate only to information that is owned by, produced by or for, or is under the control of the U.S. government. Section 1.4 of the Executive Order 13526 further defines categories of information that may be classified. There's a summary of these categories on our screen.

Classifying information occurs costs, things like security clearances, physical security measures, countermeasures, therefore original classifiers must be careful, consistent in their decision making in order to minimize the cost impact, while ensure the proper level of classification. If there is significant doubt about the need to classify then the original classification authority should not classify that information. In fact, only a limited number of people are authorized to perform original classification. These individuals must follow a specific process when doing so to ensure the classification is appropriate and reasonable. An individual who is authorized to perform original classification duties is referred to an Original Classification Authority or an OCA.

Derivative Classifications is quite different it is the process of using existing classified information to create new material and marking that new developed material consistent with classification markings that apply to the source information. Individuals who perform derivative classifications are known as derivative classifiers, in contrast to original classifiers. There are a great many individuals who do do derivative classification. Original classification authorities have an important responsibility to ensure they make effective classified decisions. They must follow a specific six step process which takes different elements into account at different stages of the process. Before considering and original classification an OCA must determine whether decisions have already been made about classification of the information. If another OCA already has an original classification determination then the information cannot be originally classified again. However, if the information has not been classified, OCAs can proceed with the decision making process. The process OCAs follow when determining whether to classify information are showing on our slide. At each step if the information does not meet the criteria to become classified, the process terminates and the OCA will not classify the information. So before we move on to our next topic, let's look at another poll question.

Poll Question: What policies establish the legal authority for certain officials to designate classified National Security information? Our answer here is B, it is Executive Order 13526. Looks like most everybody has answered that question correctly. Thank you for your quick response.

We'll now discuss Original Classification Authority. Who has authority to make original classification decisions? Original classification authority is not granted to a particular individual in the government but rather to specific positions. The positions that have original classification authority include: the President of the United States, the Vice President, the performance of the Executive duties, Secretary of Defense, the Secretaries of the Military Departments. Original classifications are also granted to certain officials within the Office of the Secretary of Defense or otherwise known as OSD. The government will grant requests for original classification authority under a specific set of circumstances. A request for original classification authority will be granted when there is a demonstrable and continuing need to exercise OCA during the normal course of operations. The candidate has adequate information and experience available to make classified decisions. Requests will be granted only when existing Security Classification Guides are insufficient in addressing the information in question, and when it is impractical to refer the decisions to another OCA. In order for an individual to exercise original classification authority, he or she must have appropriate level of security clearance, must have received training in the fundamentals of proper security classification to include the avoidance of over-classification. Individual also must also have significant experience and information available to permit effective decision classification making.

We'll now switch gears and discuss original classification training. What training is required to be an original classification authority? OCAs must be trained extensively before they can start executing their authority to originally classified information. And they must receive refresher training once a year after the initial training. The training shall address OCA responsibilities and classification principles, proper safeguarding of classified information, and the criminal, civil, and administrative sanctions that may be brought against an individual. As part of their training, OCAs must know the answers to these questions related to classifying information:

- What is the difference between original and derivative classification?
- What are the prohibitions and limitations on classifying information?

OCAs must also know the following related to duration and declassification:

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

OCAs must also know the basic portion, banner, and classification authority box markings for those that must appear on classified information. Regarding communicating classification decisions, OCAs must know the requirements and standards for creating, maintaining and publishing Security Classification Guides. And finally, OCAs must be aware of procedures and sanctions related to safeguarding classified information.

Next, we'll discuss the scope of the authority possessed by an original classification authority. Once appointed, OCAs are granted classification authority at a specific level of classification. This authority can extend to lower classification levels. For example, an OCA that has Top Secret classification authority may classify information at the Top Secret, Secret, and Confidential levels. However, an OCA that has been granted Secret classification authority may only classify information at the Secret and Confidential levels. When OCAs are appointed, they are given a specific area of jurisdiction. That is, they are assigned a specific realm in which they are qualified to make original classification decisions. This jurisdictional limit on authority helps ensure that OCAs are working in their realm of expertise and experience. For example, an air wing commander would not be granted original classification jurisdiction for an undersea warfare program. It's been a while since we've had a poll question so let's take another one. In this question, think back to the OCA basics we discussed earlier in the presentation.

Poll Question #3: How are classification decisions made? Looks like everybody has the correct answer. The correct answer is D, both a and c, originally and derivatively. Thank you for responding. We will continue.

Our last topic is assigning or delegating OCA to a subordinate. Let's see if it is possible to delegate OCA authority to a subordinate. An OCA may not delegate or assign his or her authority to someone else. If a person in a position with original classification authority will be unable to perform his or her duties for an extended period, the authority to perform original classification may be assumed by another individual. For example, that person's deputy, vice commanders, chiefs of staff, and similar immediate subordinates of the OCA are empowered to exercise authority when they officially assume the OCA position in an "acting" capacity. This is the same as being the acting commander, they assume that responsibility when the other is not there.

Before a subordinate acting in the capacity of an OCA can perform original classification, he or she must certify in writing that they have been trained as an OCA. Those records of delegation or training must be maintained by your activity security manager. Let's do another poll question.

Poll Question 4: Can an OCA assign their authority to someone else? Looks like the majority of our folks have answered the correct question which is B. They can't assign their authority to someone else, but when someone is taking their place that authority can be passed to that individual. It's kind of tricky sometimes.

The National Security of the United States depends on the protection of sensitive information. The initial determination that information needs to be protected as classified is known as original classification. Only certain individuals known as original classification authorities have the authority to make these decisions. In this webinar you learned about their role and responsibilities, the requirements they must meet, as well as the processes they follow in making these important determinations. Remember this was just the basics that we're covering today.

CDSE produces and provides a wide range of security education, training, and awareness products to support the Security Manager's mission. This includes instructor-led training, eLearning courses, and training products across the entire range of responsibilities assigned to an activity security manager. On the CDSE website you can find additional information about CDSE products, access eLearning courses, register for instructor-led courses, download job aids and security awareness materials. For further information about original classification, you can take our online Original Classification training course. Information security-related eLearning is accessed on CDSE's learning management system called STEPP. The STEPP system not only provides multimedia-rich courseware but also retains and maintains learner records and transcripts. STEPP is available for use by DoD and other US Government personnel and contractors within the National Industrial Security Program. CDSE also offers two extensive instructor-led courses for personnel engaged in DoD information security responsibilities. The DoD Security Specialist course provides an overview of a broad range of security-related topics and is targeted to those personnel with little or no security-related experience.

The Information Security Management course is a mid-level course that is intended for those personnel who have functional working knowledge of the DoD Information Security Program. In addition to instructor-led and eLearning courses, CDSE also offers a wide variety of instructional media in support of the DoD Information Security Program. This includes Security Shorts, which are targeted eLearning courses designed to be completed in less than 15 minutes, and short training videos on various security procedures and practices. CDSE also produces various job aids to assist security professionals. You'll find an Original Classification Authority Desktop Reference included in the list of job aids, and this guide outlines steps in the original classification process. Finally, CDSE also produces a variety of products aimed at assisting security managers in their security awareness efforts such as freely distributable awareness posters. Let's take a moment to address some of the questions we have received.

First Question: "Can an individual appointed as an OCA continue to make original classification decisions after leaving their OCA position or post"?

Answer: No, original classification authority is designated by virtue of position. Although we do mention individuals. The DoD Manual 5200.01, Volume 1, Enclosure 4 (which is in our File Share box) cites this requirement.

We received an additional question about a scenario in which an OCA has received classified information and determined that the information does not require protection, but release should be delayed in the interest of National Security. What determination should that OCA make? The answer is that the OCA may not classify the information. Although this information fits or may fit into one of the eligible categories of information, classifying information does not, if it does not require protection, you cannot classify it in an order to delay it. This is actually prohibited under Executive Order 13526.

Before we conclude today's presentation, we hope you'll take a moment to participate in our survey. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for further webinar topics, you're able to share those in the survey. Frequently asked questions for this webinar will be posted on the CDSE webinar website. You may also email Information Security related questions to us at InformationSecurity.Training@dss.mil.

Thank you for attending our webinar today. Have a good day!