Introduction to Information Security

Student Guide

Center for Development of Security Excellence (CDSE)
March 2024

Introduction to Information Security Student Guide

Contents

Overview

You've probably heard of classified information. Maybe in the news, in a spy movie, or in your job. But do you understand what types of information are classified and why information is classified at different levels? Do you know who makes those classification decisions or how the Department of Defense, or DOD, classifies information? Do you know the requirements for protecting classified information?

Course Objectives

During this course you will learn about the DOD Information Security Program. This course will provide a basic understanding of the program, the legal and regulatory basis for the program, and how the program is implemented throughout the DOD. It covers the Information Security Program lifecycle which includes who, what, how, when, and why information is classified, protected, shared, downgraded, declassified, and destroyed to protect national security.

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

Lesson Objectives, you will be able to:

- Define the purpose and phases of the DOD Information Security Program.
- Describe the classification process.
- Describe safeguarding and secure dissemination of classified information.
- Describe the declassification processes and destruction methods for classified information.

Lesson: Overview of the Information Security Program

Lesson Objectives

Welcome to the Overview of the Information Security Program! In this lesson we will briefly describe information security, why we need it, and how it is implemented in the DOD. Take a moment to review the lesson objectives.

Lesson Objectives:

- Describe the DOD Information Security Program Lifecycle.
- Locate policies relevant to the DOD Information Security Program.

Purpose of the DOD Information Security Program

The purpose of the DOD Information Security Program is to promote the proper and effective way to classify, protect, share, apply applicable downgrading and appropriate declassification

instructions, and use authorized destruction methods for official information which requires protection in the interest of national security.

Classification is the act or process by which information is determined to require protection against unauthorized disclosure and is marked to indicate its classified status.

Safeguarding refers to using prescribed measures and controls to protect classified information.

Dissemination refers to the sharing or transmitting of classified information to others who have authorized access to that information.

Declassification is the authorized change in status of information from classified to unclassified.

Destruction refers to destroying classified information so that it can't be recognized or reconstructed.

Classified information does not only come in the form of paper documents; it comes in electronic and verbal forms too, and regardless of what form it is in, it must be appropriately protected.

Effective execution of a robust information security program gives equal priority to protecting information in the interest of national security and demonstrating a commitment to transparency in Government.

An effective information security program requires an accurate and accountable application of classification standards; and routine, secure downgrading and declassification of information no longer requiring the same level of protection.

No matter your individual role within the DOD workforce, we all play a vital part in ensuring the effectiveness of the DOD Information Security Program.

History of the Information Security Program

The United States has had a need to protect sensitive information since George Washington and the Constitutional Convention. However, a formal classification system was not established until President Roosevelt issued the first Information Security Executive Order, or E.O., 8381 in 1938, which formalized and provided a basis for existing classification systems being used by both the Army and Navy.

During World War II, it was evident that there were many problems and dangers that resulted from the lack of a standard information security system within the Government.

In 1951 President Truman issued E.O. 10290, which established the first umbrella program to protect classified information for all departments and agencies of the Executive Branch. Prior standardization was only implemented for the military departments. Since then, the modern-day Information Security Program, or ISP, has evolved through a series of E.O.s and presidential policy directives affected by factors facing national security and the political climate.

For example, E.O. 12958, as amended, issued by President George W. Bush, was directly affected by the events of 9/11. Following those attacks, provisions were added for the classification of information pertaining to weapons of mass destruction and terrorism.

In 2009, President Obama implemented our current guidance, E.O. 13526, which addressed

overclassification, declassification, increased accountability, considerations for the electronic environment, and greater openness and transparency of government to the American people. This E.O. also strengthened training requirements for those who classify information.

DOD Policy Guidance

E.O. 13526 assigns responsibility to the Director of the Information Security Oversight Office, or ISOO, for the overall policy direction for the Information Security Program. The ISOO issued the Classified National Security Directive 32 CFR, Parts 2001 and 2003, Final Rule, which implements E.O. 13526 and further defines what the Executive Branch agencies must do to comply with E.O. requirements.

The Undersecretary of Defense for Intelligence, or USD(I), provides implementation guidance for the Information Security Program within the DOD. The USD(I) issued DOD Instruction, or DODI, 5200.01, DOD Information Security Program and Protection of Sensitive Compartmented Information, or SCI, which establishes policy and assigns responsibilities for collateral, special access program, SCI, and controlled unclassified information within an overarching DOD Information Security Program.

The USD(I) also issued DOD Manual 5200.01, Volumes 1, 2, and 3 to implement policy, assign responsibilities, and provide uniform procedures on classification management, marking, protection, and handling requirements for classified information. It is important to remember that the heads of DOD Components and Defense Agencies may add additional component-specific requirements to the DOD standards. This ensures effective security measures for unique missions and functions.

Review the DOD Policy Flowchart on the Course Resources.

Note: that Controlled Unclassified Information, or CUI, will be discussed in a separate product due to CUI reform outlined in E.O. 13556 and the implementing guidance in 32 CFR Part 2002. Currently, CUI awareness training is available on the CUI Toolkit on the Center for Development of Security Excellence, or CDSE, website.

Knowledge Check Activity

In the next two questions, let's see what you recall about the Information Security Program Lifecycle.

Knowledge Check 1

What are the steps of the information security program lifecycle?

- Classification, dissemination, downgrading, declassification, and destruction
- Classification, safeguarding, dissemination, declassification, and destruction

- Classification, marking, dissemination, downgrading, and destruction

Answer: Classification, safeguarding, dissemination, declassification, and destruction

Knowledge Check 2

Which volumes of DoDM 5200.01 provide guidance and direction on classification management, marking, protection, and handling requirements for classified information? Select all that apply.

- □ Volume 1
- □ Volume 2
- □ Volume 3
- □ Volume 4
- □ All of the above

Answer: Volume 1, Volume 2, Volume 3

Lesson Summary

This lesson provided an overview of the purpose and history of the Information Security Program, the ISP lifecycle and information security policy. At this point, you should have an understanding of how the Information Security Program has evolved and why it is so important. At any time, you may access the Student Guide on the Course Resources.

Lesson Objectives:

- Describe the DOD Information Security Program Lifecycle.
- Locate policies relevant to the DOD Information Security Program.

Lesson: Classification

Lesson Objectives

As a security professional, one of your vital duties is to protect our country's classified information! In order to protect this information, you will need to identify it as sensitive, appropriately mark it as such, and ensure that only authorized personnel with a need-to-know gain access to it.

There are requirements for properly classifying, safeguarding, handling, transmitting, and destroying classified materials.

This lesson will look at the classification of information and provide you with an introduction to working with classified materials. Take a moment to review the lesson objectives.

Lesson Objectives:

- Correlate the levels of classification to their impact on national security.
- Compare and contrast original classification to derivative classification.
- Identify the sequence of marking classified information.
- Explain the components of the classification authority block.
- Describe the purpose and origin of the security classification guide (SCG) and how to access it for derivative classification.

Levels of Classification

Classified materials contain information that requires protection against unauthorized disclosure in order to protect our national security.

What is national security? National security concerns the national defense and foreign relations of the United States. Let's break this down further.

Unauthorized disclosure of classified information could inhibit our national defense or adversely affect our foreign relations. For information to be eligible for classification, it must be official government information that is owned by, produced by, produced for, or under strict control of the U.S. Government which means the U.S. Government has the authority to regulate access to the information.

So, if materials are controlled by the U.S. Government and disclosure of the information could cause damage to national security, it may be classified.

Once the determination is made that the information must be classified, the next step is to designate the level of classification. The three levels of classification for national security information are Top Secret, Secret and Confidential, which are delineated by E.O. 13526.

Top Secret is applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our national security.

Secret is applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to our national security.

Confidential is applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to our national security.

Always remember that ALL classified information can cause damage to national security if disclosed without proper authorization. The difference between the classification levels is the severity of the damage that can be caused.

Access to Classified Information

There is a formula for granting access to classified information. In order to have authorized access to classified information, an individual must have national security eligibility and a need-to-know

the information, and must have executed a Standard Form 312, also known as SF-312, Classified Information Nondisclosure Agreement.

Eligibility for access to classified information or performance of national security duties is a determination made on the merits of an individual's case and involve examining a sufficient period of an individual's life and background. Eligibility determinations are made by adjudication authorities. For more information about national security eligibility, reference the DODM 5200.02, DOD Personnel Security Program, on the Course Resources.

Need-to-know is the determination made by an authorized holder of classified information, or custodian, that specific classified information be accessed by an individual in order to perform or assist in a lawful and authorized governmental function.

The SF-312 is a contractual agreement between the U.S. Government and a cleared employee that must be executed as a condition of access to classified information. The SF-312 advises cleared employees of their responsibility to protect information from unauthorized disclosure, and the possible consequences if they fail to honor that responsibility. By signing the SF-312, the cleared employee agrees to never disclose classified information to an unauthorized person.

If an individual is missing any of these parts to the formula, they may not access classified information.

Now that you know what classified information is and what levels are assigned to it, let's look at who classifies information.

Knowledge Check Activity

Knowledge Check 3

Select the correct classification (Top Secret, Secret, Confidential) to complete each sentence.

Unauthorized disclosure of _____ information could reasonably be expected to cause serious damage to our national security.

Unauthorized disclosure of _____ information could reasonably be expected to cause exceptionally grave damage to our national security.

Unauthorized disclosure of _____ information could reasonably be expected to cause damage to our national security.

Answer: Unauthorized disclosure of **Secret** information could reasonably be expected to cause serious damage to our national security.

Unauthorized disclosure of **Top Secret** information could reasonably be expected to cause exceptionally grave damage to our national security.

Unauthorized disclosure of **Confidential** information could reasonably be expected to cause damage to our national security.

Knowledge Check 4

What is the basic formula for granting access to classified information for individuals? Select all that apply.

- □ Verify the individual's eligibility determination
- □ Determine the individual's need-to-know
- □ Acknowledge that the SF-312 has been executed
- □ None of the above

Answer: Verify the individual's eligibility determination, Determine the individual's need-to-know, Acknowledge that the SF-312 has been executed

Original Classification

The process of making an initial classification decision on Government information is called

Original Classification.

DODM 5200.01, Volume 1, Enclosure 4 describes original classification as "the initial decision that information could reasonably be expected to cause identifiable damage to national security if subjected to unauthorized disclosure." This determination can only be made by a designated Original Classification Authority, or OCA. The OCA is an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information.

Within the DOD, Original Classification Authority is delegated to a position, not to an individual person, which means that if someone moves to another position, or is on leave, the person occupying the position that was granted OCA holds the authority. Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to perform original classification. They may do this when they have been officially designated to assume the duty position of the OCA in an acting capacity during the OCA's absence and have certified in writing that they have received required OCA training.

Positions within the DOD that are designated as OCAs are those carrying out a unique mission with responsibility in one of the subject areas which are the authorized categories from which information may be classified as outlined in E.O. 13526.

The delegation of authority will specify the highest level the OCA can classify a piece of information. This means, if the OCA is authorized to classify information at the Secret level, then they can also classify information at the Confidential level.
Because of the importance of their responsibilities, OCAs must complete training prior to exercising their authority and then annually thereafter. Select OCA Annual Training to see the annual training requirements for OCAs.

OCA Annual Training

OCA annual training covers topics such as:

- The difference between original and derivative classification
- Who can be an OCA
- The requirement to certify, in writing, before initially exercising OCA authority, and annually thereafter, that training has been received
- The prohibitions and limitations on classifying information
- The responsibility and discretion in classifying information
- Classification principles, the classification process, and the need to avoid over classification
- Safeguarding classified information from unauthorized disclosure
- Criminal, civil, and administrative sanctions that may be imposed due to unauthorized disclosure

Original Classification Process

OCAs follow a standard process to make classification determinations. CDSE packages the standard process into 6 digestible steps.

In Step 1, the OCA must ensure that the information is official government information. Remember, for information to be classified, the U.S. Government must own, have proprietary interest in, or control the information. During this step, the OCA must ensure that the information was not already classified by another OCA. If the information was already classified, then the original classification process ends.

In Step 2, the OCA will determine whether the information is eligible for classification by first examining the categories of information E.O. 13526 authorizes. The second part of determining eligibility is to ensure that the information is not specifically prohibited, or limited, from being classified as outlined in E.O. 13526.

In Step 3, the OCA must determine if unauthorized disclosure of the information could cause damage to national security, which includes defense against transnational terrorism. E.O. 13526 requires that the damage can be identified or described by the OCA.

In Step 4, the OCA assigns a level of classification to the information. Remember, the levels of classification are based upon the degree of damage the unauthorized disclosure of the information could cause to national security.

In Step 5, at the same time an OCA determines that information should be classified, they must also make the decision on how long the classification should last. Once again, E.O. 13526 provides guidance regarding the duration of classification.

The final step is where the OCA documents the level of classification and communicates the decision. There are two methods for communicating the decision: the security classification

guide, or SCG, and properly marked source documents. All DOD personnel must understand how this step applies to their daily work activities. We will discuss security classification guides in the next lesson.
Select each step to review.

Derivative Classification

Earlier you learned that only the OCA has the authority to declare original classification of information, but the rest of us can perform something called derivative classification, which makes us derivative classifiers. Derivative classifiers create new materials based on existing classification guidance. Derivative classification is not an authority, but an assumed responsibility of all cleared personnel within the DOD who generate or create material that is to be derivatively classified.

DOD Manual 5200.01, Volume 1, states that derivative classification is incorporating, paraphrasing, restating, or generating in new form any information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. The duplication or reproduction of existing classified information is not derivative classification.

As a derivative classifier, you must be aware of your responsibilities, and just as OCAs must go through training prior to exercising their authority and annually thereafter, so do derivative classifiers.

Visit Derivative Classifier Responsibilities and Derivative Classifier Annual Training to learn more.

Derivative Classifier Responsibilities

Derivative Classifier responsibilities:

- Observe and respect the OCA's initial classification decision
- If you believe information has been improperly classified, refer to DODM 5200.01, Volume 1, Enclosure 4: Challenges to Classification
- Apply required markings
- Use only authorized sources of classification guidance
- Security Classification Guide (SCG)
- Properly marked source document
- Use caution when paraphrasing or restating classified information extracted from a source document as these can change the classification
- Take appropriate and reasonable steps to resolve doubts or apparent conflicts about the classification, level and duration

Derivative Classifier Annual Training

Derivative classifiers must be trained annually on the following topics:

- Principles of derivative classification
- Classification levels
- Duration of classification
- Identification and markings
- Avoidance of over classification
- Prohibitions and limitations of classification
- Sanctions
- Classification challenges
- Classification guides
- Information sharing

Classification Concepts

Some important factors affecting classification are the concepts of contained in, compilation, and revealed by.

Contained in applies when derivative classifiers incorporate classified information, word for word, from an authorized source into a new document, and no additional interpretation or analysis is needed to determine the classification of that information.

Compilation occurs in some circumstances when information that is individually unclassified, or classified at a lower level, may be classified, or classified at a higher level, only if the compiled information reveals an additional association or relationship. Types of information that are commonly classified through compilation are budgets and tables of distribution, staffing and equipment allowances, and mission and geographic location.

The OCA will include a clear explanation of the basis for classification by compilation within the SCG for the system, plan, program, project, or mission.

Revealed by applies when classified information has been paraphrased or restated and not taken word for word from an authorized source document, but the classification is deduced from interpretation or analysis.

Knowledge Check Activity

In the next two questions, can you identify the different ways that classified information is created?

Knowledge Check 5

Select the correct term (Original Classification, Derivative Classification) to complete each

sentence.

_____ is defined as the incorporating, paraphrasing, restating, or generating in new form any information that is already classified.
_____ is defined as an INITIAL determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Answer: Derivative Classification is defined as the incorporating, paraphrasing, restating, or generating in new form any information that is already classified.

Original Classification is defined as an INITIAL determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Knowledge Check 6

Question 2 of 2
True or False: A derivative classifier may overrule an original classification determination if it is in the interest of national security.

- True
- False

Answer: False

Markings Overview

Marking classified information is the specific responsibility of original and derivative classifiers.

Markings serve to alert holders to the presence of classified information and technical information with restriction on its dissemination; identify, as specifically as possible, the exact information that needs protection; indicate the level of classification assigned to the information; provide guidance on downgrading and declassification; give information on the source(s) and reason(s) for classification or other restrictions; and warn holders of special access, control, or safeguarding requirements.

Types of Markings

All documents containing classified information must be marked using a sequential process where portion markings must be done before banner markings to mitigate confusion, marking errors and potential unauthorized disclosure.

Portion markings indicate the highest level of classification in every portion of the document and must be placed at the beginning of the respective portion. Portion markings utilize authorized abbreviations to indicate the classification level:

- TS stands for Top Secret
- S stands for Secret

- C stands for Confidential
- U stands for Unclassified

Banner markings indicate the highest level of classification of the overall document, as determined by the highest level of any one portion within the document. They are placed on the top and bottom of every page of the document. In banner markings, the classification level, TOP SECRET, SECRET, or CONFIDENTIAL, must be completely spelled out and in all capital letters.

The classification authority block, or CAB, identifies the authority and the duration of classification determination. The CAB is placed on the face of each classified document near the bottom.

For more information regarding marking principles, refer to the CDSE website.

Security Classification Guides

As referenced earlier, a security classification guide, or SCG, is a document issued by an OCA that provides derivative classification instructions. SCGs are issued for any system, plan, program, project, or mission to facilitate proper and uniform derivative classification of information.

Derivative classifiers use the information from an SCG to identify specific items or elements of information to be protected; the specific classification assigned to each item or element of information; concise reason for classifying each item, element, or category of information outlined in E.O. 13526; any applicable instructions for downgrading the level of classification and the declassification instructions for each item or element of classified information; special control notices; or other information pertinent to the proper classification and dissemination of the information in question.

Finally, SCGs provide contact information for the OCA so that anyone using classified information regarding the system, plan, program, project, or mission can contact them for clarification or review if necessary. The OCA contact information can be found on the front cover of the SCG**.**

Knowledge Check Activity

In the next three questions, let's see what you recall about the proper marking of classified documents.

Knowledge Check 7

When marking a classified document, the classifier must always start with which section?

- The banner
- The portions/paragraphs within the document
- The classification authority block

Answer: The portions/paragraphs within the document

Knowledge Check 8

True or False? If the banner marking is TOP SECRET, it is possible that some portion markings in that document can be U for Unclassified.

- True
- False

Answer: True

Knowledge Check 9

What information will you find in the classification authority block in the front page of any classified document?

- Classified By
- Post At
- Derived From
- Downgrade To
- Declassify On
- All of the above

Answer: The classification authority block contains who classified the document, where the classification of the document was derived from (for a derivative document), what level the document should be downgraded to and when (if applicable), and when the document must be declassified (excluding DOE information).

Knowledge Check Activity

In the next two questions, let's see what you recall about security classification guides.

Knowledge Check 10

Who issues security classification guides?

- Derivative classifiers
- Original classification authorities
- Security managers

Answer: Original classification authorities issue security classification guides.

Knowledge Check 11

What information does a security classification guide provide a derivative classifier? Select all that apply.

- □ Classification level for each element of information to be protected
- □ Reason for classification
- □ Duration of classification and any applicable downgrading instructions
- □ Special control notices
- □ OCA contact information

Answer: Classification level for each element of information to be protected, Reason for classification, Duration of classification and any applicable downgrading instructions, Special control notices, OCA contact information.

Lesson Summary

This lesson provided an overview of the classification process.

At this point, you should understand why information is classified, who classifies information and how they do it, as well as who may have access to classified information.

At any time, you may access the Student Guide from the Course Resources.

Lesson Objectives:

- Correlate the levels of classification to their impact on national security.
- Compare and contrast original classification to derivative classification.
- Identify the sequence of marking classified information.
- Explain the components of the classification authority block.
- Describe the purpose and origin of the security classification guide (SCG) and how to access it for derivative classification.

Lesson: Safeguarding and Dissemination

Lesson Objectives

Let's explore learn how to protect information when you are handling it storing it or sharing it with others. We want to avoid security incidents!

This lesson will provide you an overview of how to safeguard and safely share classified information with authorized individuals. We will look at the security requirements related to storing and disseminating classified information and the different types of security incidents that occur when safeguarding and dissemination procedures are not followed.

Take a moment to review the lesson objectives.

Lesson Objectives:

- Describe the security requirements related to storing classified information.
- Describe the high-level security requirements related to disseminating classified information.
- Define security incidents and describe the different types.

Authorized Storage Methods

Do you know how many places are authorized for storage of classified information? Take a guess. If you guessed four places, you are correct! The four authorized places to store classified information are:

- in an authorized individual's head,
- in an authorized individual's hands,
- in a General Services Administration, or GSA, approved security container;
- in authorized information technology.

When the information is in an authorized individual's head or hands, it should stay there and only be shared with other authorized individuals that meet the criteria we discussed earlier.

When not directly in an authorized individual's possession, classified information must be put back into a GSA-approved security container, such as a 2- or 4-drawer cabinet, safe, or vault.

All locks for GSA-approved security containers must conform to Federal Specification FF-L-2740.

When using information technology to access classified information, you must follow cybersecurity policies related to accessing or sharing classified information on classified systems such as the Secure Internet Protocol Router Network, or SIPRNET.

Forms Used to Protect Classified Information Outside GSA-approved Containers

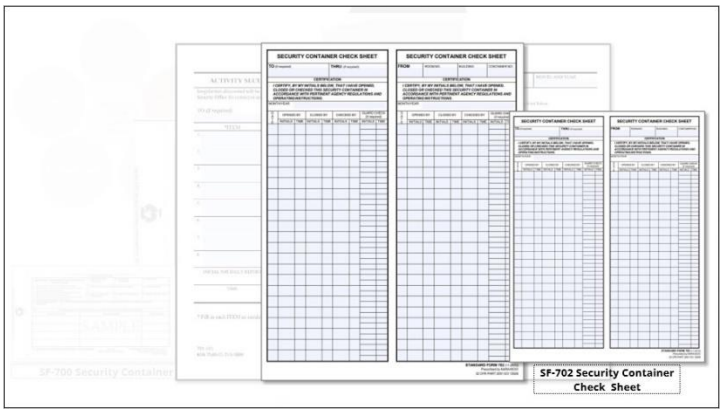
Specific forms and procedures are required when classified information is outside GSA-approved security containers as well as for those security containers themselves.

When classified information is in an authorized individual's hands, the individual should use a classified document cover sheet to alert holders to the presence of classified information and to prevent inadvertent view of classified information by unauthorized personnel.

- SF-703 is the cover sheet for Top Secret,
- SF-704 is the cover sheet for Secret, and
- SF-705 is the cover sheet for Confidential information.

Forms Used for GSA-Approved Security Containers

Here are some forms that you will use when working with GSA-approved security containers:



- The SF-700, Security Container Information, is used to maintain a record for each container and to record the combination.
- The SF-701, Activity Security Checklist, is used to record checks of work areas at the end of each working day.
- The SF-702, Security Container Check Sheet, is used to record the securing of vaults, rooms, and containers used for storing classified material.

Access Control

Our first responsibility is to ensure that only authorized personnel have access to classified information. Access means the ability and opportunity to obtain knowledge of classified information.

Earlier in this course, we discussed the formula for access to classified information. In addition to verifying individual access, we must also be concerned with access control measures which detect and deter deliberate attempts to gain unauthorized access.

To do this, we implement security countermeasures such as fences, badges, guards, security containers, locks, intrusion detection systems, and other countermeasures.

For more information on access control measures, refer to the course resources.

Waivers and Exceptions

Sometimes classified information cannot be safeguarded to the standards or requirements specified in DODM 5200.01, Volume 1, Enclosure 3. When this occurs, a request for a waiver or exception can be made. The template for requesting waivers and exceptions is called the DOD Component Request for Waiver or Exception and is located in the Appendix to Enclosure 3 of

DODM 5200.01, Volume 1.

Waivers and exceptions are approved exclusions or deviations from information security standards. The difference between the two is that waivers are temporary exclusions or deviations while exceptions are permanent exclusions or deviations.

Requests for waivers and exceptions must contain sufficient information to permit a complete and thorough analysis of the impact to national security.

Requests must identify the specific provision(s) of the DOD Information Security Manual for which the waiver or exception is sought.

Requests from DOD Components must provide rationale and justification, including negative impacts to cost, schedule, mission, or operations; a mission analysis summary to identify vulnerabilities and risk management considerations; a summary of proposed mitigation measures to reduce risk; and the necessary duration for any waivers.

Current waivers and exceptions will continue to be valid until they are due for renewal. Unless otherwise specified in DODM 5200.01, Volume 1, DOD Components must submit requests for information security waivers or exceptions to the standards and requirements through the chain of command to the USD(I).

For waivers involving marking of classified information or requests involving prescribing standard forms, refer to DODM 5200.01, Volume 2, Enclosure 2, and Enclosure 3.

Knowledge Check Activity

In the next two questions, let's see what you recall about the requirements for safeguarding classified information.

Knowledge Check 12

True or False? You may store classified information in your locked desk drawer while you go to lunch as long as you cover it with the appropriate classified cover sheet.

- True
- False

Answer: False

Knowledge Check 13

If your office is preparing to undergo renovations for the next few months and you will not be able to store classified information according to the requirements as specified in DoDM 5200.01, Volume 3, which of the following should you request?

- Waiver

- Exception
- Security Incident

Answer: Waiver

Transmission

You must continue to safeguard classified information when you disseminate it to other authorized individuals via phone, information systems, and fax.

When using a phone to share classified information with other authorized individuals, you must only use phones with approved secure communication circuits.

Know how to use your secure communication device. And remember, just because you are on a Secure Terminal Equipment, or STE, does not mean that someone can't hear your end of the conversation. So, always be vigilant of your surroundings and know who is nearby when using this phone.

Cybersecurity refers to the measures that protect and defend information and information systems. Processing classified information on an information system presents unique and challenging security issues. When processing classified information on an information system, only use an information system that has been specifically authorized to process classified information and only email classified information over a classified network.

When using a fax machine to transmit classified information, the fax machine must be connected through appropriate secure communication equipment over secure communication circuits approved for transmission of information at the specific level of classification.

Transportation

Transmission and Transportation Method	Top Secret	Secret	Confidential
Direct contact between appropriately cleared personnel	X	X	X
Approved secure communications systems (i.e., an authorized cryptographic system or protected distribution system)	X	X	X
Defense Courier Service (DCS)	X	X	X
Authorized U.S. Government agency courier services (i.e., Dept. of State Diplomatic Courier Service, authorized DOD component courier service)	X	X	X
Cleared U.S. military and Government personnel and DOD contractor employees specifically designated to carry the information and traveling by surface transportation or on a scheduled commercial passenger	X	X	X

Go to Course Resources to download or print this chart.

There are different requirements for transporting Confidential, Secret, and Top Secret information.

As simple as it might be to just pop classified documents into a post office box, or hand them

over to the mail carrier, it can't be done that way. Precautions must always be taken to secure classified information. Classified information can be transported via hand carrying or an escort, courier, or mail.

This chart is broken down by levels of classification with helpful information to transmit or transport classified information. Note that certain methods of transportation can be used for all three levels of classified information. Some can only be used for Secret and Confidential. Others can only be used for Confidential. Take a moment to review the chart.

Refer to the Course Resources to download or print this chart.

Packaging Requirements

Whenever classified information is removed from an authorized area, the risk of loss or compromise increases. To minimize this risk, we need to follow special rules for packaging the material. Preparing classified information for transportation is an important aspect of trying to prevent unauthorized access to it while it is in transit.

DODM 5200.01, Volume 3 outlines baseline policies and procedures that must be followed to assist in safeguarding the information while it is being transported.

Additionally, heads of the DOD components are responsible for establishing procedures for transmission and transportation of classified information and information-bearing material that minimizes risk of compromise while permitting use of the most cost-effective transmission or transportation means.

Classified material needs to be prepared for shipment, packaged, and sealed in ways that minimize risk of accidental exposure and facilitates detection of tampering. But before actually wrapping the material, verify that all markings on the document itself are correct. Once you have verified your markings are correct, it is time to look at packaging the material.

There are two layers to preparing packages containing classified information: the inner wrapping and the outer wrapping.

Inner Wrapping:

- Address the envelope to an official government activity or DOD contractor. If there is a specific person to receive the package, indicate their name.
- Put your office's complete return address on the envelope.
- Conspicuously mark the envelope with the highest level of classified information it contains.
- Include any applicable special marking, such as "Restricted Data," on the envelope.
- Place the material within the inner envelope and carefully seal the envelope to minimize the possibility of access without leaving evidence of tampering.

Outer Wrapping:

- Insert the inner envelope within the outer envelope and seal the outer envelope to minimize the possibility of access without leaving evidence of tampering.

- Address the envelope to an official government activity or DOD contractor. Do NOT address it to an individual's name on the outer envelope.
- Put your office's full return address on the envelope.
- Do NOT put any markings or notations on the outer envelope that indicate its contents are classified.

For more information on transmission and transportation of classified information, refer to the CDSE website.

Classified Meetings and Conferences

When a DOD activity sponsors a classified meeting or conference, the activity will assign an official to serve as the security manager for the meeting. The security manager will be responsible for ensuring that, at a minimum, the following security provisions are met:

- Brief attendees on safeguarding procedures.
- Control the entrance so that only authorized personnel gain entry to the area.
- Control the perimeter to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would result in the compromise of classified information.
- Provide escorts for uncleared personnel who are providing services to the meeting or conference (such as food setup or cleaning) when classified presentations and/or discussions are not in session.
- Prohibit use of cell phones, personal electronic devices, or PEDs, 2-way pagers, and other electronic devices that transmit.
- Only permit note taking during classified sessions when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting. Ensure classified notes and handouts are properly safeguarded.
- Segregate classified sessions from unclassified sessions.
- Only disclose classified information to foreign nationals in coordination with your Foreign Disclosure Officer, or FDO.
- Conduct an inspection of the room(s) at the conclusion of the meeting or conference (or at the end of each day of a multi-day event) to ensure all classified materials are properly stored.

Prepublication Review

The Defense Office of Prepublication and Security Review, or DOPSR, is responsible for managing the DOD security review program, and reviewing written materials for public and controlled release. This includes government and industry work products, as well as materials submitted by current and former DOD civilians, contractors, and military members pursuant to their non-disclosure agreement obligations.

The security review protects classified information, controlled unclassified information, and unclassified information that may individually or in aggregate lead to the compromise of classified information or disclosure of operations security.

Some examples of materials DOPSR reviews include manuscripts, articles, theses, conference papers, briefings, brochures, reports to Congress, and books.

DOPSR derives its authority from DODI 5230.09, Clearance of DOD Information for Public Release, and DODI 5230.29, Security and Policy Review of DOD Information for Public Release.

Heads of DOD Components must ensure that component specific documents, including official correspondence, are reviewed internally and that information is reviewed for operations security before public release. The review must also address technology transfer and public releasability of technical data.

For more information on disseminating classified information, refer to the CDSE website.

Knowledge Check Activity

In the next two questions, let's see what you recall about disseminating classified information.

Knowledge Check 14

When can Top Secret information be sent via the United States Postal Service (USPS)?

- When Defense Courier Operations (DCO) is not available
- When the information needs to be signed for
- Never

Answer: Never

Knowledge Check 15

True or False. While manuscripts, articles, theses, conference papers, briefings, brochures, and books must be sent to the Defense Office of Prepublication and Security Review (DOPSR) for review and approval before publishing, reports to Congress do not require prepublication review.

- True
- False

Answer: False

Types of Security Incidents

When someone fails to use proper security requirements for protecting classified information, we have a security incident that must be handled. Before we learn how to react to a security incident,

we need to understand the types of incidents that could occur. These types of security incidents are a security violation, security infraction, spillage, and unauthorized disclosure.

For more information on security incidents, refer to the CDSE website.

Security Violation

What specifically is a security violation? A security violation occurs when there is a knowing, willful, or negligent action that could reasonably be expected to result in the loss, suspected compromise, or compromise of classified information.

For example, an individual fails to secure the SCIF at the end of the day and subsequently, unescorted cleaning personnel access the SCIF and see classified information.

A security violation occurs when an inquiry reveals there has been a compromise of classified information. Depending on the type of information which has been compromised, an investigation may also be required.

Security Infraction

A security infraction is a failure to comply with security requirements which cannot reasonably be expected to, and does not result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent.

For example, an individual neglects to complete the SF-702 after securing the container.

A security infraction requires an inquiry and confirms that the security incident did not result in a compromise of classified information.

Spillage

Spillage occurs when classified data is introduced on an information system not approved for that level of information.

For example, an individual inserts a thumb drive containing classified information on a computer in the office that is not part of the classified information system.

Per DOD regulation, a spillage requires an investigation to determine the extent of the compromise of classified information.

Unauthorized Disclosure

Unauthorized Disclosure is the communication or physical transfer of classified information to an unauthorized recipient.

Knowledge Check Activity

In the next two questions, let's see what you recall about security incidents.

Knowledge Check 16

Your manager hands you a Top Secret document but you are only eligible for Secret access. If you think this is a security incident, what type of security incident do you think it is?

- Infraction
- Violation
- Spillage
- This is not a security incident because it was handed to you by your manager.

Answer: Violation

Knowledge Check 17

Your co-worker, Bob, did not place an SF-704, Secret classified document cover sheet, on a classified document while it was out of the security container. However, Bob did maintain positive control of the document until he returned to the security container. If you think this was a security incident, what type of security incident do you think it was?

- Infraction
- Violation
- Spillage
- This is not a security incident because Bob maintained positive control of the document.

Answer: Infraction

Lesson Summary

This lesson provided an overview of the security requirements for safeguarding and disseminating classified information.

At this point, you should understand the authorized places for storing classified information and how to protect that information when it is not being stored. You should also know the requirements for securely sharing classified information with others. And finally, you should understand the different types of security incidents and what must happen when a security incident occurs.

At any time, you may access the Student Guide from the Course Resources.

Lesson Objectives:

- Describe the security requirements related to storing classified information.
- Describe the high-level security requirements related to disseminating classified information.

- Define security incidents and describe the different types.

Lesson: Declassification and Destruction

Lesson Objectives

Everyone who works in a classified environment is responsible for making sure classified information is always handled correctly, from the time it is originated to the time it is destroyed.

In this lesson we will look at declassification and destruction of classified information. We will discuss declassification and how it works. We will then review authorized methods for destroying classified information.

Take a moment to review the lesson objectives.

Lesson Objectives:

- Define four processes for declassifying classified information.
- Define authorized methods for destroying declassified information.

Declassification Processes

Declassification is the authorized change in the status of information from classified to unclassified. As you will remember, when an OCA determines the level of classification for information, they must also determine when the information can be declassified.

Declassifying information means that the information no longer requires protection in the interest of national security at any level.

There are four types of declassification processes: scheduled declassification, automatic declassification, mandatory declassification review, and systematic declassification.

- Scheduled Declassification is the set date or event, determined by the OCA, which will occur within 25 years from the date of original classification.
- Automatic Declassification is the declassification of information that (1) is more than 25 years old and (2) is not otherwise prevented from being declassified by an approved exemption. Such information shall be declassified on the 31st of December, 25 years from the date of original classification.
- Mandatory Declassification Review is a way for members of the public to request the review of specific classified information. The requestor must describe the information in sufficient detail to allow the agency to locate it.
- Systematic Declassification is the review of classified information that has been exempted from automatic declassification.

Authorized Methods of Destruction

Destruction refers to destroying classified information so that it can't be recognized or reconstructed.

Authorized methods for destroying classified information include burning, shredding, pulverizing, disintegrating, wet pulping, melting, chemical decomposition, and mutilation. Regardless of what method is used, the destruction should preclude recognition of the classified information.

Just as there are approved methods of destroying classified documents and materials, actual destruction must take place on approved equipment. The National Security Agency, or NSA, maintains listings of evaluated destruction products that have been tested and meet performance requirements. These products are on the evaluated products list, or EPL. For more information on the approved destruction methods by classification level, review DODM 5200.01, Volume 3, Enclosure 3. Additionally, the web link to the NSA EPL is available on the Course Resource page.

Each activity with classified holdings shall establish at least one day each year when specific attention and effort is focused on disposing of unneeded classified materials, also known as "clean out day".

For destruction procedures for paper-based products and non-paper-based products, select the appropriate button.

Destruction Procedures for Paper-based Products

Destroying classified paper-based material is the most common type of classified destruction within the DOD. Shredders are the preferred destruction equipment. They are relatively inexpensive compared to an incinerator, and they are convenient.

DOD follows standards set by NSA. Current specification requires shredders to have crosscut capability to cut the material into confetti-like bits, not just into long strips, as well as the capability to cut the material into 1mm by 5mm pieces.
Check inside the shredder after using it. Larger pieces may get stuck on the sides or may slip through.

Destruction Operations for Non-Paper based Products

Classified information resides on a variety of material other than paper. Just like paper-based classified material, these non-paper-based items must be properly destroyed when they are no longer required. Certain materials can present problems in the destruction process because of their composition.

Compact and digital video discs are considered optical media devices. The NSA has a list of established destruction methods for these devices.

Destruction of any other storage media to include thumb drives or zip disks should be coordinated with your local information systems personnel and must conform to the applicable

DOD and Component guidance.

Refer to the NSA website for additional information on IS storage devices. Be safe and security conscious at the same time.

Knowledge Check Activity

What do you recall about declassification and destruction?

Knowledge Check 18

Select the appropriate term for each definition.

_____ The declassification system where the public can ask for classified information to be reviewed for declassification and public release
_____ The declassification system where information exempted from automatic declassification is reviewed
_____ The declassification system where an OCA sets a date or event for declassification
_____ The declassification system where information is declassified when it is 25 years old

Scheduled Declassification
Automatic Declassification
Mandatory Declassification Review
Systematic Declassification

Answer:

- Mandatory Declassification Review is the declassification system where the public can ask for classified information to be reviewed for declassification and public release.
- Systematic Declassification is the review of classified information that has been exempted from automatic declassification.
- Scheduled Declassification is when an OCA, at the time is originally classified, sets a date or time for declassification.
- Automatic Declassification is when system information is declassified when it is 25 years old.

Knowledge Check 19

In the next two questions, let's see what you recall about destruction requirements for classified information.

Question 1 of 2
Where would you find approved destruction equipment?
Best Buy
GSA Catalog
NSA EPL

Amazon

Answer: NSA Evaluated Products Listing (EPL) contains listings of evaluate destruction products that have been tested and meet performance requirements.

Knowledge Check 20

True or False: The only type of acceptable document shredding is with a crosscut shredder.
True
False

Answer: True

Lesson Summary

This lesson provided an overview of the declassification and destruction processes.
At this point, you should understand how, when, and why information is declassified. You should also know the proper methods for destroying classified information and where to find the authorized equipment for destruction.

At any time, you may access the Student Guide from the Course Resources.

Lesson Objectives:

- Define four processes for declassifying classified information.
- Define authorized methods for destroying declassified information.

Lesson: Conclusion

Course Conclusion

This course introduced you to the DOD Information Security Program and the lifecycle of classified information. It also introduced you to the federal and DOD policies relevant to the DOD Information Security Program.

You can now use what you learned to do your part to protect our national security.