

Safeguarding Classified Information in the NISP IS109v6

Student Guide

January 2023

Center for Development of Security Excellence

Table of Contents

Lesson 1: Course Introduction.....	1
Lesson Introduction.....	1
Course Objectives.....	1
Course Structure.....	1
Lesson 2: Basic Concepts.....	2
Lesson Introduction.....	2
Objectives.....	2
Types of Classified Information.....	2
Classification Levels.....	2
Forms of Classified Information.....	2
Disclosure of Classified Information.....	3
Disclosure to Authorized Persons.....	3
Disclosure to Authorized Persons.....	3
Information Management Requirements.....	3
Information Management Systems.....	3
TOP SECRET Accountability.....	4
Lesson 2: Review Activities.....	5
Review Activity 1.....	5
Review Activity 2.....	5
Review Activity 3.....	5
Review Activity 4.....	5
Review Activity 5.....	6
Lesson 3: Obtaining Classified Information.....	7
Lesson Introduction.....	7
Objectives.....	7
Receiving Classified Information.....	7
Clearance of Receiving Individual.....	7
Handling Upon Receipt.....	8
From Commercial Delivery Entities.....	10
Generating Classified Information.....	10
Derivatively Classified Material.....	10
Working Papers.....	11
Lesson 3: Review Activities.....	12
Review Activity 1.....	12

Review Activity 2	12
Review Activity 3	12
Review Activity 4	12
Review Activity 5	13
Lesson 4: Storing Classified Information	14
Lesson Introduction	14
Objectives	14
Overview	14
Storage Options	14
Storage Containers	14
Storage Containers	17
Locking Devices	17
Overview	17
Combination Locks	18
Keys and Padlocks	20
Supplemental Protection	20
Alarms and Guards	20
Storage Procedures	20
Storage by Classification Level	21
Storage by Classification Level	21
Reports	22
End of Day Security Checks	23
Lesson 4: Review Activities	24
Review Activity 1	24
Review Activity 2	24
Review Activity 3	24
Review Activity 4	24
Review Activity 5	25
Review Activity 6	25
Review Activity 7	25
Lesson 5: Using Classified Information	26
Lesson Introduction	26
Objectives	26
Handling Classified Information	26
Physical Handling	26
Restricted Areas	27

Perimeter Controls 27

Emergency Procedures 27

Classified Visits..... 28

Oral Discussions 28

Lesson 5: Review Activities 30

 Review Activity 1 30

 Review Activity 2 30

 Review Activity 3 30

 Review Activity 4 30

 Review Activity 5 31

Lesson 6: Reproducing Classified Information..... 32

 Lesson Introduction..... 32

 Objectives..... 32

 Authorizations 32

 GCA Authorizations..... 32

 Procedures..... 32

 Copy Requirements 32

 Equipment Requirements..... 33

 Best Practices..... 33

Lesson 6: Review Activities 35

 Review Activity 1 35

 Review Activity 2 35

 Review Activity 3 35

 Review Activity 4 36

 Review Activity 5 36

Lesson 7: Disposition of Classified Information 37

 Lesson Introduction..... 37

 Retention 37

 Requirements..... 37

 Disposition Schedule 38

 Requirements..... 38

 Destruction..... 39

 Requirements..... 39

 Methods..... 39

Lesson 7: Review Activities 42

 Review Activity 1..... 42

Review Activity 2.....	42
Review Activity 3.....	42
Review Activity 4.....	43
Review Activity 5.....	43
Review Activity 6.....	43
Review Activity 7.....	43
Review Activity 8.....	44
Lesson 8: Safeguarding Challenge	45
Introduction	45
Getting Started.....	45
Explore These Areas.....	45
Visitor’s Desk.....	45
Handling Classified Information.....	45
Copy Room.....	47
Lesson 9: Course Conclusion.....	48
Course Conclusion.....	48
Course Summary.....	48
Lesson Review.....	48
Course Objectives.....	48
Appendix A: Answer Key.....	50
Lesson 2 Review Activities.....	50
Review Activity 1.....	50
Review Activity 2.....	50
Review Activity 3.....	51
Review Activity 4.....	51
Review Activity 5.....	52
Lesson 3 Review Activities.....	53
Review Activity 1.....	53
Review Activity 2.....	53
Review Activity 3.....	54
Review Activity 4.....	54
Review Activity 5.....	55
Lesson 4: Review Activities.....	56
Review Activity 1.....	56
Review Activity 2.....	56
Review Activity 3.....	57

Review Activity 4..... 57

Review Activity 5..... 58

Review Activity 6..... 58

Review Activity 7..... 59

Lesson 5: Review Activities..... 60

 Review Activity 1..... 60

 Review Activity 2..... 60

 Review Activity 3..... 61

 Review Activity 4..... 61

Lesson 6: Review Activities..... 62

 Review Activity 1..... 62

 Review Activity 2..... 62

 Review Activity 3..... 63

 Review Activity 4..... 63

 Review Activity 5..... 64

Lesson 7: Review Activities..... 65

 Review Activity 1..... 65

 Review Activity 2..... 65

 Review Activity 3..... 66

 Review Activity 4..... 67

 Review Activity 5..... 67

 Review Activity 6..... 68

 Review Activity 7..... 68

 Review Activity 8..... 68

Lesson 1: Course Introduction

Lesson Introduction

Welcome to the Safeguarding Classified Information in the National Industrial Security Program (NISP), course.

Safeguarding classified information is imperative for our national security. Safeguarding classified information means being able to securely receive, use, store, transmit, reproduce and appropriately dispose of classified information either generated by or entrusted to your company.

Requirements for safeguarding classified information in the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM).

In this course, you will learn about the measures you and your company must take to ensure that classified information is protected from loss or compromise.

Course Objectives

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

- Identify the general requirements for safeguarding classified information
- Identify the requirements for control and accountability of classified information
- Identify options and requirements for storage of classified information
- Identify requirements for disclosure of classified information
- Identify requirements for reproduction of classified information
- Identify requirements for disposition of classified information

Course Structure

This course is organized into the lessons listed here.

- Course Introduction
- Basic Concepts
- Obtaining Classified Information
- Storing Classified Information
- Reproducing Classified Information
- Disposition of Classified Information
- Safeguarding Challenge
- Course Conclusion

Lesson 2: Basic Concepts

Lesson Introduction

Before you learn about the various measures for safeguarding classified information, there are some concepts related to safeguarding that you should know.

Objectives

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

- Distinguish between the different types of classified information
- Identify the disclosure requirements for classified information
- Identify the information management requirements for classified information

Types of Classified Information

Classification Levels

Classified information is categorized into three classification levels, CONFIDENTIAL, SECRET, and TOP SECRET.

Classification levels are applied to national security information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to national security.

Each classification level has its own set of requirements for safeguarding. The higher level of classification, the more protection the classified information requires to reasonably prevent the possibility of its loss or compromise.

Forms of Classified Information

All forms of classified information must be protected.

Forms of classified information include classified finished or final documents, both paper-based and electronic, classified working papers, classified information identified for destruction, and classification-pending material.

Classified working papers are documents that are generated to prepare a finished document.

Classified information identified for destruction is no longer needed and shall be destroyed using approved methods and equipment prescribed by the NISPOM or other government guidance provided.

Classification-pending material is material that requires a classification determination from the Government Contracting Activity (GCA).

This material must be safeguarded in accordance with the proposed highest classification level until guidance is received from the GCA.

Disclosure of Classified Information

Disclosure to Authorized Persons

You must ensure that classified information is disclosed only to authorized persons. An authorized person is someone who has a favorable determination of eligibility, also referred to as a personnel clearance (PCL), for access to classified information, has signed an approved nondisclosure agreement (NDA), and has a need-to-know (NTK) for the classified information in performance of official duties.

So you are only authorized to disclose classified information to your cleared employees, to another cleared contractor or sub-contractor, to a cleared parent company or subsidiary, within a multiple facility organization (MFO), to Department of Defense (DOD) activities, or to Federal agencies when their access is necessary for the performance of tasks or services essential to the fulfillment of a classified contract, prime contract, or subcontract.

Note that disclosure of classified information may be done in oral form.

This will be discussed later in the course.

Disclosure to Authorized Persons

Before disclosing classified information to another DOD activity, Federal agency, foreign person, attorney, or Federal or state courts, you must have authorization from the DOD activity or Federal agency that has classification jurisdiction over the information in question.

Finally, classified information must never be disclosed to the public, and unclassified information about classified contracts may only be released to the public in accordance with the NISPOM.

Although it is no longer classified, declassified information may not be disclosed to the public, unless approved in the same manner as classified information

Information Management Requirements

Information Management Systems

Contractors are required to establish an information management system (IMS) to protect and control all classified information in their possession, regardless of media, to include information processed on

authorized information systems.

The purpose of the IMS is to verify that classified information in the contractor's custody is used or retained for a lawful and authorized U.S. Government purpose only. There is not a required format for information management systems. An information management system can be in the form of an electronic database, or as simple as a spreadsheet or log. You must demonstrate how the IMS accounts for, protects, and justifies the retention of classified information at the facility.

TOP SECRET Accountability

Access and accountability records must be kept at various points in the TOP SECRET information lifecycle. Contractors are required to establish controls for TOP SECRET information and material to validate that procedures are in place to address accountability, need-to-know, and retention.

These controls are in addition to the IMS and must be applied to TOP SECRET information, regardless of the type of media. This includes TOP SECRET information processed and stored on authorized classified information systems.

When TOP SECRET information is produced by a contractor, a record must be kept of the following: when the finished document was completed, when the information is retained for more than 180 days regardless of its stage of development, and when it is transmitted inside or outside the facility.

For more information about transmitting outside the facility, refer to the Transmission and Transportation for Industry e-Learning course offered by the Center for Development of Security Excellence (CDSE).

If the TOP SECRET material is not stored in an electronic format on an authorized classified information system, each TOP SECRET item must be numbered in a series and the copy number must be placed on each TOP SECRET document and all associated transaction documents.

The Cognizant Security Agency (CSA), may make specific determinations regarding the contractor's procedures for TOP SECRET accountability.

TOP SECRET control officials must be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information.

An inventory must be conducted annually unless a written exception is obtained from the GCA.

Lesson 2: Review Activities

Review Activity 1

All classified information should be afforded the same level of protection regardless of the classification level of the information.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 2

Classified information identified for destruction must be safeguarded until it is destroyed.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 3

Contractors are required to establish an information management system to protect and control classified information in their possession.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 4

All classified information must be numbered in a series.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 5

Which of the following must a person have to be authorized to handle classified information?

Select all the correct answers. Then check the Answer Key at the end of this Student Guide.

- Classified jurisdiction
- Need-to-know for the classified information in performance of official duties
- Favorable determination of eligibility, or (PCL) for access to classified information
- A signed and approved nondisclosure agreement
- Original classification authority

Lesson 3: Obtaining Classified Information

Lesson Introduction

Contractors can obtain classified information either by receiving it from the government or another cleared contractor, or by generating it internally.

In this lesson you will learn about the guidelines contractors must follow when obtaining classified information.

Objectives

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

- Identify the contractor's responsibilities and procedures for receiving classified information
- Identify the contractor's responsibilities and procedures for generating classified or derivatively classifying information

Receiving Classified Information

Clearance of Receiving Individual

Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient.

Classified material coming into a facility must be received directly by authorized personnel, whether it's in the form of a package, envelope, fax, email, or phone call.

Persons transmitting the classified information are responsible for ensuring that the intended recipients are authorized persons with the capability to store classified information.

An authorized person means a cleared person who has been assigned this duty and, therefore, has a need-to-know. This means that the individual who picks up the mail or accepts deliveries from the U.S. Postal Service or commercial delivery entities approved for transmitting classified material must be cleared to the level of the classified material expected to be received by the contractor.

All employees who are authorized to receive or sign for U.S. Registered or U.S. Express mail must have SECRET clearances.

Likewise, employees who are authorized to receive or sign for U.S. Certified Mail must have CONFIDENTIAL clearances. If the person who normally accepts deliveries is not cleared, that

individual must call the Facility Security Officer (FSO) or other cleared person to sign for packages that require signatures.

If no cleared employee is available, the uncleared person must refuse the package. This is true even if the uncleared person does not have any intention of ever opening the package.

In the case of delivery to a P.O. Box, an authorized person must go to the post office, unlock the post office box, sign for its contents when a signature is required, and bring the classified information directly back to the facility.

For more information on authorized methods for transmitting and transporting classified information, refer to the Transmission and Transportation for Industry e-Learning course offered by CDSE.

Handling Upon Receipt

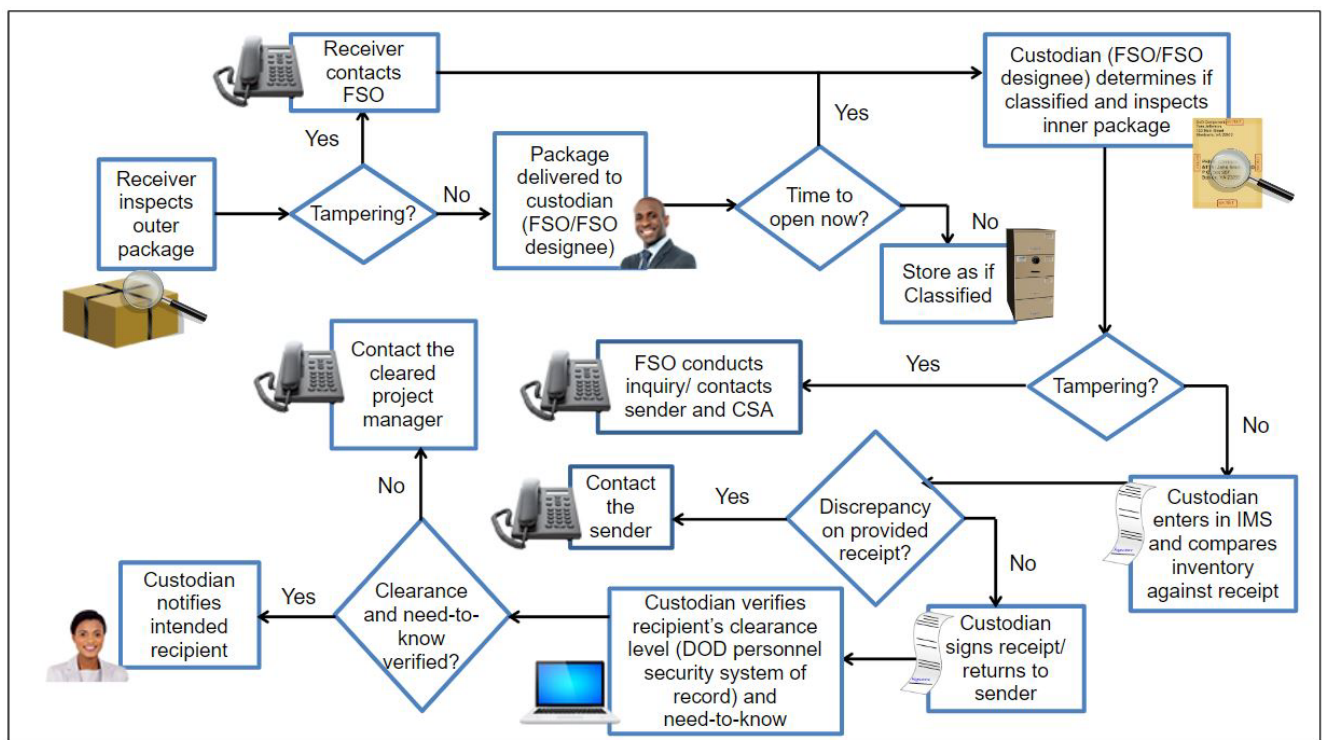


Figure 1: Receiving Flowchart

The company is responsible for establishing procedures for transmitting and receiving classified information. Once a Registered or Certified package has been received by an authorized person, the receiver should examine the outer package for evidence of tampering.

If the receiver suspects tampering, the Facility Security Officer, or FSO, should be immediately notified.

The FSO or FSO designee should first determine if the package contains classified information by inspecting the inner package. If it does contain classified information and the inner package has been tampered with, then the FSO or designee must conduct an inquiry and determine whether a loss, compromise or suspected compromise of classified information in accordance with the NISPOM has occurred. If a loss, compromise or suspected compromise has occurred, the FSO must notify both the sender and their CSA.

If the receiver does not suspect any tampering of the outer package, they must immediately turn the package over to the designated document custodian, who may be the FSO, or the FSO's designee for processing.

If the designated custodian is not able to open and process the package at that time, it must be protected as if it were classified until it is opened and a classification determination is made.

When the designated custodian opens and processes the package, the inner package should also be inspected for evidence of tampering.

If tampering is detected, the FSO or designee must conduct an inquiry and determine whether a loss, compromise or suspected compromise of classified information in accordance with the NISPOM has occurred.

If a loss, compromise or suspected compromise has occurred, the FSO must notify both the sender and their CSA.

Next, the designated custodian incorporates the material into the facility's IMS, and checks the contents of the package against the receipt, if a receipt is provided. If there is a discrepancy, the sender must be contacted immediately.

If the package contents match the provided receipt, the designated custodian should sign and return it to the sender.

Next, the designated custodian verifies through the current DOD personnel security system of record or the facility's records that the intended recipient has the appropriate clearance level, and verifies the intended recipient's need-to-know. This may be done by contacting the recipient's supervisor or project manager. In many cases this determination will be made by the FSO who is aware of what projects each cleared employee is working on.

After verification of these items, the designated custodian notifies the intended recipient that the

material has arrived and arranges for that person to access the information.

If the designated custodian cannot verify the intended recipient's clearance level or need-to-know, the designated custodian should contact the cleared project manager for that contract to determine who should receive the classified material.

A continuous receipt system is required for all TOP SECRET information within and outside the company's location.

The above chart is also available to you as a reference on the Course Resources page.

From Commercial Delivery Entities

Commercial delivery entities may transmit SECRET or CONFIDENTIAL information within the U. S. and its territorial areas if the entity is a current holder of the GSA contract for overnight delivery and provides nation-wide, overnight service with computer tracking and reporting features, and is approved by the CSA.

When a shipment is received via a commercial delivery entity, the company must have procedures in place to ensure that the incoming shipments are received by appropriately cleared personnel.

The list of approved commercial delivery entities may be found on our Course Resources page.

For more detailed information, refer to the Transmission and Transportation for Industry e-Learning course offered by CDSE.

Generating Classified Information

Derivatively Classified Material

In addition to receiving classified information from outside sources, contractors may produce classified information internally.

This process of generating new classified materials from already existing classified information is known as derivative classification.

For more information about the process, refer to the Derivative Classification e-Learning course offered by CDSE.

Contractors are required to properly safeguard any classified materials they generate, or derivatively classify. Depending on the type of information, additional requirements may apply.

Contractors must follow guidance from the Central Office of Record (COR) for entering any

Communications Security, or COMSEC material they generate into the accountability system.

The NISPOM also contains guidance about generating and marking North Atlantic Treaty Organization (NATO) materials.

Finally, contractors must properly mark all classified information they generate, or derivatively classify.

For more information about properly marking classified information, refer to the Marking Special Categories of Classified Information e-Learning course and the Marking in the Electronic Environment Short offered by CDSE.

Derivative Classification

Derivative Classification is the incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

Derivative classification includes classifying information based on classification guidance.

Duplicating or reproducing existing classified information is not derivative classification.

Working Papers

The NISPOM also contains requirements that apply when a contractor creates classified working papers to prepare a finished document.

Working papers must be dated when created.

Each page must be marked with the highest classification level and protected at that level, marked with the annotation "WORKING PAPERS," and destroyed when they are no longer needed.

Working papers must be marked in the same manner prescribed for a finished document and at the same classification level when transmitted outside the facility, or retained for more than 180 days from the date of creation.

Lesson 3: Review Activities

Review Activity 1

A person may be authorized to receive and sign for classified information if they are cleared to the level of classified information they are receiving.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 2

Only an authorized person may receive and sign for packages that may contain classified information.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 3

All employees may pick up classified packages at a P.O. Box as long as they sign a form stating they will not open the package.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 4

The intended recipient of classified information must assure the sender that they are an authorized person at a facility with classified storage capability.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 5

Working papers must be marked in the same manner prescribed for a finished document at the same classification level when it is transmitted outside the facility or retained for more than

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- 180 days from the date of creation
- 120 days from the date of completion
- 90 dates from the date of creation

Lesson 4: Storing Classified Information

Lesson Introduction

In order to safely store classified information, there are various requirements that must be met. These include proper use of equipment and open storage areas, locks, supplemental protection, and safeguarding procedures.

In this lesson, you will learn about the various requirements for physical protection of classified material.

Objectives

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

- Identify types of and requirements for using storage equipment and storage areas
- Identify types of and procedures for using locking devices
- Identify types of and guidelines for using supplemental protection
- Identify the requirements for all possessing facilities

Overview

Storage of classified information requires having a secure and approved container or area in which to put classified information when authorized persons are not using it.

The higher the classification level of the information, the more secure the storage place must be. Classified information must be stored in approved storage containers or in open storage areas. Storage containers or areas must be large enough to hold all of the classified information on hand. And there should be no external markings on storage containers indicating the level of classified information authorized for storage. Finally, once classified material is stored properly, it is critical to maintain the integrity of the storage container or area.

Now let's take a look at some different types of storage containers and areas.

Storage Options

Storage Containers

A General Services Administration (GSA) GSA-approved security container is the only type of container that may be used to safeguard classified information. A GSA-approved security container is a steel file container with a built-in combination lock constructed to withstand certain hazards, such as lock manipulation, for specified lengths of time.

The GSA establishes and publishes uniform standards, specifications, and supply schedules for its

approved containers. All GSA approved containers must be procured through the GSA Global Supply System. You can search for the container you need on the GSA website, which may be found on the course resources page.

Because the type and size of storage container you need depends on how much classified information and the types of classified information you need to store, including classified information identified for destruction, there are various types and sizes of GSA-approved storage containers.

For more information on GSA-approved storage containers, refer to the Storage Containers and Facilities course offered by CDSE.

All GSA-approved storage containers must have two labels affixed to them: a GSA test certification label on the side of the locking drawer and a GSA-approved security container label on the left-hand side of one of the upper drawers.

Always ensure these two labels are affixed. And, if the container has been repaired, you must also obtain the locksmith certification from the seller that the container's integrity has not been impaired.

In the event that any of these storage containers is not operating correctly, there are special requirements about repairing them.

Hazards

Look at these examples of integrity compromises and attacks on GSA security containers.



Figure 2: Compromises on GSA Security Containers

Security personnel should routinely inspect their security containers for hidden drilled holes and openings. A few places to check are behind label holders.

Containers

Types/sizes of GSA-approved security containers:

- 2-drawer; 4-drawer, 5-drawer
- Legal size and letter size
- Single, dual, or multi-lock
- Map and plan containers

GSA test certification label:

- Indicates class of security container
- Class relates to delay afforded against forced, covert, or surreptitious entry
- Only Class 5 and 6 containers are available new

GSA-approved security container label:

- Verifies that container is GSA-approved
- Color-coding:
 - Black: pre-1990
 - Red: post-1990 (container has a case-hardened locking drawer that requires a different method of neutralization and repair)”

Repairs

Repairs of storage containers must be completed by appropriately cleared or continuously escorted personnel who are specifically trained in approved methods of maintenance and repair of

these containers.

In order to continue to be used to protect classified information, an approved security container must be restored to its original state of security integrity and have a signed and dated certification stating the method of repair used.

All repairs must follow Fed Standard 809 (FED-STD-809), Neutralization and Repair of GSA Approved Containers and Vault Doors.

Storage Containers

There are two types of areas in which you may store classified information.

The first type is an approved vault. Vaults have very substantial construction requirements. Vaults are considered to be equivalent, from a security perspective, to a GSA-approved container.

The second type of area for storing classified information is an open storage area. Due to the size and nature of the classified material to be stored, or for operational necessity, GSA-approved containers may not be practical. In these cases, it may be necessary to construct an open storage area.

Open storage areas are much less expensive to build than vaults and are more commonly used. The Cognizant Security Agency, or CSA, and the contractor must agree on the need to establish an open storage area and its extent, based on the safeguarding requirements of a classified contract, either before or during the life of the contract. If qualifying criteria are met, the CSA may grant an interim approval for an open storage area. Access to open storage areas must be protected either through use of a guard, an authorized person, or an access control system.

For more information on access control systems, refer to the Physical Security Measures eLearning course offered by CDSE.

The NISPOM contains specific construction requirements for both vaults and open storage areas.

Guard

Only companies that used guards prior to 1995 have been grandfathered to still use guards. Any company cleared after 1995 is not authorized to use guards for open storage areas.

Locking Devices

Overview

Security containers, open storage areas, and vaults must be kept locked when not under direct supervision of an authorized person entrusted with the contents.

Depending on the type of storage container or area, the locks can be either built-in combination locks or padlocks. All locks on security containers and vaults must meet Federal specifications.

The Department of Defense Lock Program has a website with useful information, and a hotline number you can call with any questions related to locks for security containers and areas.

You can also call the hotline to obtain free magnetic Secured and Open signs to attach to the side of your security containers. These signs are a great way to indicate whether a security container has been locked or not.

Combination Locks

Built-in combination locks are the most widely used type of lock on security containers and vaults for protecting classified information.

Six locks have been approved under FF-L-2740B for the protection of classified material.

The X10 and the Sargent and Greenleaf, or S&G, 2740B are the two models currently in production. They have sophisticated anti-manipulation security features to resist certain types of attacks, such as an attack using an auto-dialer. Older locks on GSA-approved containers can continue to be used until they no longer work properly.

Combination padlocks may also be used to secure classified information. The current padlock model that meets Federal specifications is S&G 8077AD.

To ensure that classified information inside a security container or vault is fully protected, the combination must be protected. In addition, there are specific requirements and procedures for changing combinations.

Protecting Combinations

Here are some guidelines for protecting combinations to security containers and vaults.

Allow only a minimum number of authorized persons to have knowledge of combinations to authorized storage containers.

Maintain a record of all persons who have knowledge of the combination.

Protect the combination in accordance with the highest classification of information authorized for storage in the container.

If a record is made of a combination, mark the record with the highest classification of information

authorized for storage in the container. Then safeguard the record accordingly.

However, it is better to create a combination that is easy to remember, so that you don't have to write it down.

A good way to do this is to think of a six letter word that you would easily remember, but that others wouldn't easily guess, and then use the numbers on a telephone keypad that correspond to the letters in your word.

For example, if your word is Harley, then the corresponding combination numbers would be 42-75-39.

There are special requirements for facilities at which only one person is assigned to make sure the combination is preserved if that person is unavailable for some reason.

It is important that your cleared employees know what they can and cannot do when it comes to remembering combinations.

Good security education is the key to safeguarding combinations.

Special Requirements

One-person facilities have special requirements for protecting combinations which are to:

- Provide current combination to the CSA field office, or in the case of an MFO, to the home office
- Establish procedures for CSA notification upon the death or incapacitation of that person

Changing Combinations

Combinations must be changed by an authorized person, or by the FSO, or his or her designee.

Never allow a commercial locksmith to change your combination.

Change combinations at the initial use of an approved container or lock.

Change them when anyone who has knowledge of the combination is either terminated or their clearance withdrawn, suspended, or revoked.

Also change combinations when a container or its combination has been compromised or suspected of compromise, or when a container has been left unlocked and unattended.

Finally, combinations must be changed at other times when deemed necessary by the FSO or CSA.

Keys and Padlocks

Although not used as frequently as combination locks, high-security keyed padlocks are still used on some security containers for classified information.

One drawback of using padlocks, however, is that there is no authorized method of repair for some models.

Like combinations, keys and padlocks to security containers must also be safeguarded.

Follow these guidelines for protecting keys and padlocks for security containers:

- Appoint a key and lock custodian to ensure proper custody and handling of keys and locks used for the protection of classified information.
- Keep a key and lock control register to identify keys for each lock and their current location and custody.
- Audit keys and locks each month, and inventory keys with each change of custody.
- Provide protections for keys and spare locks equivalent to the level of classified information involved.
- Change or rotate locks at least once a year, and replace them if a key is compromised or lost.

Removing keys from the premises and making master keys are prohibited.

Supplemental Protection

Alarms and Guards

In certain cases, supplemental protection is required to protect classified information. This usually takes the form of an intrusion detection system (IDS).

For more information about intrusion detection systems and their requirements, refer to the NISPOM, and to the Physical Security Measures eLearning course offered by CDSE.

Under certain circumstances security guards may continue to serve as supplemental protection. Only those facilities who were authorized to use guards prior to January 1, 1995 may continue their use.

These guards must make rounds at least every 2 hours for TOP SECRET and 4 hours for SECRET information.

One of the reasons security guards have been eliminated as a supplemental security measure is because IDS is a more cost-effective security option.

Storage Procedures

Storage by Classification Level













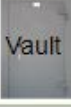
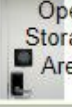




	Classification Level		Storage Containers/Areas				
	Supplemental Protection		WH	Non-WH	WH	Non-WH	Non-WH
	Supplemental Protection		WH	Non-WH	WH	Non-WH	Non-WH
	TOP SECRET						
							
	Supplemental Protection						Non-WH
	SECRET						
							
	Supplemental Protection		Not required				
	CONFIDENTIAL						

Figure 3: Storage Containers and Areas

Storage by Classification Level

Storage requirements are different for each level of classified information. The higher the classification level of the information, the more secure the storage container or open storage area must be.

TOP SECRET Storage

TOP SECRET information must be stored in a GSA-approved security container, vault, or open storage area.

Supplemental protection is required during working hours and non-working hours for TOP SECRET information that is stored in a GSA-approved container or vault.

Additionally, it is required during non-working hours for TOP SECRET information that is stored in an open storage area.

However, supplemental protection is not always required for storage of TOP SECRET information if it is located in an area of security-in-depth.

Supplemental protection may NOT be required for GSA-approved security containers and

approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740 (X-07, X-08, X-09, X-10 or S&G2740B) when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

Security-in-depth is a determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within a facility. Written authorization from the CSA is required before security-in-depth can take the place of supplemental controls such as IDS or guards.

SECRET Storage

SECRET information must be stored in any of the three areas approved for TOP SECRET information.

Supplemental protection is required during non-working hours only for SECRET information that is stored in an open storage area.

Supplemental protection is not required for storage of SECRET information if it is stored in a GSA-approved security container or vault.

CONFIDENTIAL Storage

CONFIDENTIAL information must be stored in any of the areas approved for SECRET information.

However, supplemental protection is never required for storage of CONFIDENTIAL information.

Reports

The NISPOM requires reports related to storage be sent to the CSA. For DOD, these reports are sent to the Defense Counterintelligence and Security Agency (DCSA), field office.

A report titled Change in Storage Capability must be submitted after the initial acquisition of an approved storage container that raises or lowers the level of classification that a contractor is able to safeguard – for example, when your facility acquires its first storage container for classified information.

The next report, Inability to Safeguard Classified Material, is required to be submitted after an emergency that renders the facility's location incapable of safeguarding classified material as soon as possible.

Imagine there is a sudden evacuation of your facility due to a fire alarm. There was no time for you to properly store your classified information and it was too voluminous for you to carry with you.

Any time there is an inability to safeguard classified information, steps must be taken to ensure that the material is protected at all times until the situation is corrected.

Depending on the circumstances, this may require an authorized person to stay with the material until it is properly secured.

End of Day Security Checks

The NISPOM requires end-of-day security checks to ensure that all classified information is protected and that the security container or area has been secured.

Security checks must be conducted at the end of the last working shift, unless operations are conducted 24 hours per day.

Although not required, records of security checks are a good security practice. Here is an example of a security container record that has columns to record the date and time a security container was opened, closed, and checked.

SECURITY CONTAINER CHECK SHEET

TO (if required) THRU (if required)

CERTIFICATION
 I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/DAY/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

SECURITY CONTAINER CHECK SHEET

FROM ROOM NUMBER BUILDING CONTAINER NUMBER

CERTIFICATION
 I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/DAY/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (REV. 1/2020)
 Prescribed by NARA/ISOG
 32 CFR PART 2001 EO 13526

Figure 4: Standard Form 702 Security Container Check Sheet

Lesson 4: Review Activities

Review Activity 1

Which of the following are approved for storing TOP SECRET information (with supplemental controls)?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- Six-sided steel cabinet
- GSA-approved container
- Steel cabinet
- Open storage area
- Vault

Review Activity 2

You must keep a written record of the combination lock of any container in which classified information is stored.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 3

Storage of TOP SECRET information always requires supplemental protection or security-in-depth during non-working hours regardless of the type of security container used.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 4

When supplemental protection is required, the facility must only use security guards.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 5

Security checks are required at the end of the last working shift of each day to ensure classified information is properly stored and security containers are locked.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 6

When must a combination be changed to the lock for a security container used to store classified information?

Select all that apply. Then check the Answer Key at the end of this Student Guide.

- At the initial use of an approved container or lock
- When anyone who has knowledge of the combination is either terminated or has his or her clearance withdrawn, suspended, or revoked
- When a container or its combination has been compromised or suspected of compromise
- When a container has been left unlocked and unattended
- Other times when deemed necessary by the FSO or CSA
- At least once per year

Review Activity 7

In which of these cases would you need to make a report to your DCSA Field Office?

Select all that apply. Then check the Answer Key at the end of this Student Guide.

- You need to store several cubic feet of CONFIDENTIAL documents and have decided to convert a room in the basement of your facility for this purpose.
- You currently store SECRET and CONFIDENTIAL documents in a two-drawer GSA-approved container. You need more storage space, so you have decided to replace the two-drawer model with a four-drawer model.
- You add another cleared employee to your list of persons who have knowledge of the combination to your storage container.
- An afternoon thunderstorm has knocked out the electrical power in your area. As a result, the alarm system that provides supplemental protection for your TOP SECRET storage during nonworking hours is not operating. You are told by the power company that service may not be restored until morning and you have no other way to adequately protect your classified material.

Lesson 5: Using Classified Information

Lesson Introduction

In addition to requirements for safeguarding classified information when it is stored, there are also requirements for safeguarding classified information when it is being used and when it is being discussed. In this lesson, you will learn about the requirements and best practices for properly handling classified material in your day-to-day work.

Objectives

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

- Identify requirements for handling classified information in the day-to-day work environment
- Identify best practices for oral discussions regarding classified information

Handling Classified Information

Physical Handling

Contractors are responsible for safeguarding classified information in their custody or under their control to reasonably protect it from loss or compromise.

When classified information is out of its security container, it must be kept under constant surveillance of an authorized person who can exercise direct security controls over the information.

This means that if the authorized person has to leave their work area, even momentarily, he or she must carry the classified information with them, have another authorized person watch it, or return it to its storage container.

When unauthorized persons are present, classified information must be covered, turned face down, placed back in its storage container or otherwise protected.

This includes taking appropriate steps to prevent an unauthorized person from seeing classified information on a computer screen in accordance with the Information System's System Security Plan (SSP).

Though not required, it is a good best practice to make room or area checks during working hours to ensure that employees are keeping classified information under constant surveillance or storing it properly.

Such checks foster good security habits. Once classified work is finished, classified material must be returned to the storage container for protection.

Restricted Areas

When it is necessary to control access to classified information in an open area during working hours, a restricted area may be established.

A restricted area will normally become necessary when it is impractical or impossible to protect classified information by simply covering it or turning it over because of its size, quantity, or other unusual characteristic.

Although physical barriers are not required by the NISPOM, the restricted area must have clearly defined perimeters.

Examples might be roped off areas, a specially designated cubicle, or an office with a closed door.

Authorized persons in the restricted area are responsible for protecting the classified information from unauthorized access.

Once classified work is finished, classified material must be returned to the storage container for protection and the area becomes a regular work area once again.

Perimeter Controls

Perimeter controls are entry and exit inspections that deter and detect the introduction or removal of classified information from a facility without proper authority.

Contractors who are authorized to store classified information are required to establish and maintain such perimeter controls.

Signs must be posted conspicuously informing everyone that they are subject to inspection upon entry and exit. The extent, frequency, and location of inspections must be accomplished in a manner consistent with contractual obligations and operational efficiency, and they must be applied consistently.

For example, inspections should occur in a set manner such as on every person, every other person, and so on.

Contractors are encouraged to seek legal advice when formulating their inspection policies.

These procedures are limited to buildings or areas where classified work is being performed.

Emergency Procedures

Contractors must develop procedures for safeguarding classified information in emergency situations.

The procedures should be as simple and practical as possible, and should be adaptable to any type of emergency that may arise. They should also take into consideration employee safety.

When formulating your emergency procedures, it is best practice to consult with your company's safety officer.

Classified Visits

When a visitor arrives at your facility for a classified visit, you must positively identify the visitor and verify clearance and need-to-know prior to disclosing any classified information.

You must brief the visitor on the security procedures at your facility and then escort the visitor or otherwise control their activities in your facility so that they only have access to the classified information consistent with the authorized purpose of their visit.

Before the visitor leaves, you must also ensure all classified information that they handled during their visit has been returned.

For more information on classified visits, refer to the Visits and Meetings in the NISP e-Learning course offered by CDSE.

Oral Discussions

The NISPOM requires contractors to ensure all cleared personnel know the rules about discussing classified information.

Authorized persons may discuss classified information only over secure telephone lines, or in areas where the discussion cannot be overheard by an unauthorized person.

Classified information may not be discussed over unsecure telephones or wireless devices, or in public conveyances or places that might permit unauthorized interception, such as in cubicles or in rooms where you can hear through the walls.

A best practice to prevent discussion of classified information in inappropriate locations is to post signs reminding employees that classified discussions are not authorized.

Good security education and awareness training is a key for ensuring that your employees know where classified discussions are allowed.

It is particularly important to provide guidance to employees working in a non-possessing facility where there is no capability to store any classified material, such as notes from a classified discussion.

No matter where the discussion takes place, employees must ensure that classified information is

disclosed only to authorized persons in a manner that prevents interception by unauthorized persons.

Select [Wireless Devices](#) for more information on the challenges they present.

Wireless Devices

One of the biggest challenges you will face is protecting classified information from disclosure through the use of wireless devices.

Many of these devices, such as cell phones, including those with remote activation capability, camera phones, mobile devices, such as smartphones, e-readers, tablets and so on, can be used to record and transmit classified information either orally or photographically.

Their use is strictly prohibited.

Different devices require different security measures, based on their capabilities.

Lesson 5: Review Activities

Review Activity 1

An authorized person may lock classified information in a desk drawer while going down the hall to get a cup of coffee.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 2

An authorized person may turn classified information over on their desk when an unauthorized person is present.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 3

An authorized person is responsible for safeguarding classified information in a restricted area.

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 4

An authorized person must escort or control the activities of their classified visitor.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 5

Where may classified information be discussed between authorized persons?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- In elevators if only authorized persons are on the elevator
- In a restricted area
- On cell phones in restricted areas
- On secure telephones

Lesson 6: Reproducing Classified Information

Lesson Introduction

When reproducing classified information, it is important to safeguard that information. In this lesson, you will learn about the NISPOM requirements and some best practices for reproducing classified information.

Objectives

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

- Identify when classified information may be reproduced without obtaining authorization
- Identify the security procedures for reproducing classified information

Authorizations

GCA Authorizations

Before reproducing classified information, you must follow these guidelines regarding when to obtain prior authorization from the contracting officer or some other government authority.

The NISPOM states that unless restricted by the GCA, classified information may be reproduced to the extent required by operational needs, or to facilitate review for declassification.

Some examples of this include, reproducing TOP SECRET documents in preparation and delivery of a contract deliverable, or reproducing SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract, in preparation of a solicited or unsolicited bid, quotation, or proposal or in preparation of patent applications to be filed in the U.S. Patent Office.

Reproductions of classified information for any other purpose would require authorization from the GCA.

Procedures

Copy Requirements

The NISPOM requires that reproduction of classified information be limited to the minimum consistent with contractual and operational requirements.

You will need to determine for each situation exactly how many copies you will need.

You should also consider if it is possible to reduce the number of copies.

The NISPOM also requires that the only individuals who can reproduce classified information be

authorized personnel knowledgeable of the procedures for classified reproduction.

The NISPOM does not require that these individuals submit reproduction requests, but it is a security best practice to do so.

Reproduction Request

The NISPOM imposes requirements on the reproduction of classified documents, including parts of documents.

To ensure that these requirements are met at a facility, the FSO, should consider requiring that authorized personnel submit a request form prior to reproducing classified information.

Although not a NISPOM requirement, a formal procedure for requesting permission to reproduce materials will ensure that all proposed reproduction is routed through the FSO. This process will help to avoid any unnecessary or improper reproduction of classified materials. If your facility decides to use these requests, include it in your Standard Practice Procedures (SPP), if you have one.

Equipment Requirements

Most modern copy machines, printers, and other multifunction devices have memory or hard drives where information is stored digitally. These machines are actually information systems. As such, they need to be authorized in accordance with the NISPOM before they are used for any classified work.

The facility should coordinate with their DCSA Industrial Security Representative (IS Rep) prior to purchasing or using any such equipment if it is to be used with classified information. The IS Rep may work with the DCSA Information Systems Security Professional (ISSP) also known as a Security Control Assessor (SCA), to determine what authorizations are needed for a particular piece of equipment and what procedures need to be followed.

Best Practices

Although not required by the NISPOM, it is a best practice to reproduce classified information on equipment specifically designated for this purpose as use of some equipment may not be cost-effective.

Using only designated equipment gives the FSO another level of control, and some reproduction equipment have features such as memory that are not appropriate for use with classified information.

The location of the equipment is also important. Use only equipment that is located within a

controlled area.

It is also a best practice to post the rules for using the designated equipment on or near the equipment so users know exactly what procedures to follow.

You should always ensure that only the planned number of copies are made.

If the copier malfunctions, do not leave it, but request help, if needed.

Fix the problem and verify that no classified pages remain inside the copier.

You should always ensure that the security markings on the original appear on all of the copies and have not been cut off.

You should account for all originals and copies before leaving the copier.

In order to ensure that no image remains on any image bearing part of the machine, make three blank copies and handle them as classified waste.

Do not leave waste at the copier.

Take all classified waste with you to be disposed of properly.

Note that some copiers are designed to store images of what they reproduce. If this is the case with your copier, you must erase all stored images of classified information according to the manufacturer's instructions.

This type of equipment may have to be authorized as an information system. Since copiers that have memory or hard drives may have to be authorized as an information system, always contact your IS Rep prior to using any of these types of equipment for reproduction of classified information.

Finally, always keep in mind the vulnerabilities of the reproduction equipment you are using.

Best Practices

Equipment vulnerabilities

- Paper jams may cause paper with images to be retained in the machine
- Ink on rollers may retain images of classified information
- Extra copies or partial copies may be retained in the machine or discarded via a special port

Lesson 6: Review Activities

Review Activity 1

Which of these cases represent good examples to reproduce classified information for operational needs?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- TOP SECRET documents in preparation of a contract deliverable
- SECRET and CONFIDENTIAL documents in preparation of a solicited bid, quotation or proposal
- SECRET and CONFIDENTIAL documents in preparation of patent applications to be filed in the U.S. Patent Office
- SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract

Review Activity 2

You are alone making classified copies and the machine jams. You go down the hall to ask for help. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- Permissible
- Problematic

Review Activity 3

John, an authorized person, has a very busy schedule today and, therefore, has requested that his administrative assistant, who is not an authorized person, make copies of classified information on his behalf for his 2 p.m. meeting. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- Permissible
- Problematic

Review Activity 4

You made copies of some classified information for your meeting in 10 minutes and noticed when you got to your meeting that some of the classification markings were cut off on the copies. You decided to distribute the copies to the meeting participants since they were just copies and not originals. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

Permissible

Problematic

Review Activity 5

After making copies of classified information, Sarah made three blank copies on the copier. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

Permissible

Problematic

Lesson 7: Disposition of Classified Information

Lesson Introduction

Classified information that is no longer needed must be processed for appropriate disposition.

Disposition is relevant during all stages of a contract.

While contractors should dispose of material they no longer need throughout the contract period, special emphasis is placed on disposing of classified information at the contract's conclusion.

The three modes of disposition are: retaining, returning, and destroying classified information.

In this lesson, you will learn about the requirements for making proper disposition of classified information.

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

- Identify the requirements for retaining classified information
- Identify the requirements for returning classified information to the Government Contracting Activity
- Identify the requirements for destroying classified information

Retention

Requirements

Contractors must establish procedures for reviewing their classified holdings on a regular basis to reduce their classified inventories to the minimum necessary for effective and efficient operations.

The NISPOM states that contractors are authorized to retain copies of U.S. government classified information received or generated under a classified contract for two years after completion of the contract, provided the GCA does not instruct otherwise.

All original documents and deliverables must be provided back to the GCA at contract conclusion.

By the end of the retention period, classified information must be destroyed, declassified if appropriate, or returned to the GCA.

However, if retention is required beyond the standard two year period, additional retention authorization must be requested from the GCA in a certain format, depending on the level of classified material involved, and must always include a statement of justification.

If the request for retention authority is approved, the GCA may issue a final DD Form 254, Department

of Defense Contract Security Classification Specification, for the classified contract and will enter the authorized retention period and final disposition instructions on the form.

In some cases the GCA provides a letter authorizing retention beyond the two-year period.

Classified Information

Contractors must identify classified information for retention beyond two years as follows

- TOP SECRET information must be identified in a list of specific documents unless the GCA authorized identification by subject matter and the approximate number of documents
- SECRET and CONFIDENTIAL information may be identified by general subject matter and the appropriate number of documents

Classified Information

Contractors must include a statement of justification for retention based on the following:

- The material is necessary for the maintenance of the contractor's essential records
- The material is patentable or proprietary data to which the contractor has title
- The material will assist the contractor in independent research and development efforts
- The material will benefit the U.S. Government in the performance of other prospective or existing agency contracts
- The material will benefit the U.S. Government in the performance of another active contract and will be transferred to that contract (specify contract)

Disposition Schedule

Requirements

Classified information must be returned or destroyed if the facility clearance (FCL) of your company is terminated.

Classified information obtained for the preparation of a bid, proposal, or quote must be returned or destroyed within 180 days after the opening date of the bid, proposal, or quote, if the bid, proposal, or quote was not submitted or if it was withdrawn.

If the bid, proposal, or quote was submitted but not accepted, then the classified information must be returned within 180 days after notification that it had not been accepted.

If classified information was not obtained under a specific contract, such as information obtained at classified meetings or from a secondary distribution center, it must be returned or destroyed within one year after receiving it.

The GCA will advise when classified information should be destroyed rather than returning it to the GCA.

Destruction

Requirements

Types of classified information that contractors must destroy include: multiple copies, obsolete material, and classified information identified for destruction.

Contractors must also destroy classified information in their possession as soon as possible after it has served the purpose for which it was released by the government, was developed or prepared by the contractor, or was retained after completion or termination of the contract.

Classified information that is taken from a cleared facility for destruction must be destroyed on the same day it is removed and must be performed using methods approved by the CSA.

Classified information may only be destroyed by authorized personnel who have a full understanding of their responsibilities.

For destruction of TOP SECRET information, two authorized persons are required, one to destroy the material and one to act as a witness.

The individual acting as the witness may be a subcontractor.

For destruction of SECRET and CONFIDENTIAL information, only one authorized person is required.

Destruction records are required for TOP SECRET information only and shall be maintained for two years after date of destruction.

The records must indicate the date of destruction, and the material being destroyed, and must be signed by the individuals who witnessed and carried out the destruction.

Although it is not required, it is a good security practice to maintain records for SECRET and CONFIDENTIAL destruction.

Methods

According to the NISPOM, the method of destruction must preclude recognition or reconstruction of the classified information.

Classified information may be destroyed by various methods such as: burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition, pulverizing, overwriting, degaussing,

sanding or grinding.

Paper products may be destroyed using: incinerators, pulpers, pulverizers, or shredders.

However, water repellent paper products cannot be sufficiently destroyed by pulping, so other methods such as: disintegration, shredding, or burning must be used.

Classified information in microform may be destroyed by: burning, or chemical decomposition.

Residue must be inspected after each destruction to ensure that the classified information cannot be reconstructed.

Electronic media can be destroyed in various ways.

Overwriting destroys data by entering new data in its place on solid state storage devices, such as smart cards and flash drives.

This method does not declassify electronic media.

Therefore the electronic media may only be reused within the same environment.

Degaussing erases data completely from magnetic media such as magnetic tapes, hard drives, and floppy drives.

Sanding and grinding are used to destroy optical media such as CDs and DVDs.

Physical destruction or mutilation is also used for electronic media by: shredding, crushing, disintegrating, pulverizing, and incinerating.

For more information on the disposal of classified information, refer to CDSE's Disposal and Destruction of Classified Information Short.

Recognition or Reconstruction

The NISPOM requires that crosscut shredders currently in use be capable of maintaining a shred size not exceeding 1/32 inch in width (with a 1/64 inch tolerance by 1/2 inch in length). However, it is recommended that any crosscut shredders requiring replacement of the unit and/or rebuilding of the shredder blades assembly be replaced by a crosscut shredder on the latest National Security Agency / Central Security Service (NSA/CSS) Evaluated Products List for Paper Shredders. This list may be obtained from the Course Resources page.

The current DOD specification for shred size is 1 mm X 5 mm or less.

Methods of Destruction

Burning – Note that if you intend to use public destruction facilities, such as public incinerator, you must obtain approval from your CSA, usually the DCSA field office. Also note that due to environmental concerns, most governmental jurisdictions and many companies discourage or prohibit the burning of refuse, classified or not.

Pulverizing – Examples of pulverizing include hammer mills, choppers and hybridized disintegration equipment.

Microform – Examples of microform material include microfilm, microfiche, and similar high data density material.

Water repellent paper products – High wet strength paper, paper Mylar, durable-medium paper substitute, or similar water repellent papers.

Solid State Storage Devices – Examples include smart cards and flash drives.

Magnetic Media – Examples include magnetic tapes, hard drives, and floppy drives.

Optical Media – Examples include Compact Disks (CDs) and Digital Video Disks (DVDs).

Lesson 7: Review Activities

Review Activity 1

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

WW can request retention authority from the Navy.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 2

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

If WW requests retention authority, they would need to do it within 180 days.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 3

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

The Navy would need to issue a final DD Form 24 indicating the final retention period and final disposition instructions.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 4

In which of the following cases must classified information be returned or destroyed?

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- When a contractor's FCL is terminated
- Within 180 days after the opening date of the bid, proposal, or quote if it was not submitted or if it was withdrawn
- Within two years after receipt of the classified information if it was not obtained under a specific contract
- Within 180 after notification that the submitted bid, proposal, or quote had not been accepted
- Within one year after receipt of the classified information if it was not obtained under a specific contract

Review Activity 5

Classified information in the form of regular paper may be burned.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 6

Destruction of classified information must ensure the information cannot be recognized or reconstructed.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 7

When destroying classified information with a shredder, shred size is not important.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Review Activity 8

Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL documents.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Lesson 8: Safeguarding Challenge

Introduction

Getting Started

Welcome to the Safeguarding Challenge.

This challenge will give you a chance to practice identifying the kinds of things that have implications for safeguarding classified information.

Here's how it works.

You'll go to several different areas in your cleared facility.

In each one, select the items that might have consequences for how you handle classified information.

When you select each one, you'll see some useful information about that item.

Explore These Areas

Visitor's Desk

Explore this visitor's desk area and see what you can learn about the items that relate to safeguarding classified information.

Clipboard

Make sure packages that may contain classified information are accepted only by cleared and authorized personnel.

Package

Anytime an authorized person receives a classified package, it is important to immediately examine the outer package for evidence of tampering.

Visitor Log

Make sure you know the procedures for classified visits so they are easy to apply when visitors arrive.

Drawer in storage container

When you accept delivery of an unopened package, you must store it as if it contains classified information until it can be opened.

Handling Classified Information

Look around this classified work area.

What items can you find that have implications for safeguarding classified information?

Telephone (landline)

Classified information must not be discussed over the telephone unless specifically approved secure telephone equipment and procedures are used.

Be aware also of who might overhear your classified call.

[Man]: Hello, this is an un-secure line

Wireless device

When working in areas where classified discussions take place, make sure you are not using cell phones, or anything that transmits information or could be used as a recording device.

Open security container Drawer

Make sure security containers and vaults are kept locked except when under the direct control of an authorized person.

Security Check Record

At the end of the day, conduct a security check to make sure classified information is properly secured.

It is a best practice to keep a record of these checks to help in the event an investigation becomes necessary.

Information Management System

You must have and use a system to protect and control classified information.

SECRET document

Make sure you protect classified information at all times!

Whiteboard

Be careful about putting classified notes up on a white board, where unauthorized individuals might view it.

Computer monitor

When working with classified information be sure to use only approved information systems, and

remember to protect what appears on your monitor.

Printer

As soon as you print classified documents, immediately retrieve them from the printer.

Copy Room

Now, look around this copy room.

What elements have implications for safeguarding classified information?

Copy machine

As a best practice, you should copy classified information on a designated copier.

Equipment use rules

As a best practice, post the rules for copying classified information on or near the copier.

Shredder

Be sure to destroy classified material appropriately!

Classified document for reproduction

Limit the number of copies you make.

Make only as many as you need.

Be mindful about additional controls that apply to TOP SECRET information.

Classified papers for destruction

Be sure you destroy extra copies, anything that is obsolete, and all classified information identified for destruction.

Remember, when destroying TOP SECRET information, two individuals must be present and destruction record retained for two years

Recycle bin

Do not put classified identified for destruction in with the ordinary trash or recyclables.

You must protect it as classified material until it is properly destroyed.

Lesson 9: Course Conclusion

Course Conclusion

Course Summary

Safeguarding classified information is imperative for our national security.

Safeguarding classified information means being able to securely receive, use, store, transmit, reproduce, and appropriately dispose of classified information either generated by or entrusted to your company.

Requirements for safeguarding classified information in the NISP are stated in the National Industrial Security Program Operating Manual, or NISPOM.

In this course, you learned about the measures you and your company must take to ensure that classified information is protected from loss or compromise.

Lesson Review

Here is a list of the lessons in the course.

- Course Introduction
- Basic Concepts
- Obtaining Classified Information
- Storing Classified Information
- Using Classified Information
- Reproducing Classified Information
- Disposition of Classified Information
- Practical Exercise
- Course Conclusion

Course Objectives

You should now be able to perform all the listed activities.

- Identify the general requirements for safeguarding classified information
- Identify the requirements for control and accountability of classified information
- Identify options and requirements for storage of classified information
- Identify requirements for disclosure of classified information
- Identify requirements for reproduction of classified information
- Identify requirements for disposition of classified information

Congratulations. You have completed the Safeguarding Classified Information in the NISP course.

To receive course credit, you MUST take the Safeguarding Classified Information in the NISP examination.

If you are taking this course from STEPP, return to the course page; then, select Launch Exam to begin the online exam.

If you are taking this course from the CDSE Security Awareness Hub, select the Take Exam button to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

All classified information should be afforded the same level of protection regardless of the classification level of the information.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Feedback:

The higher level of classification, the more protection the classified information requires to reasonably prevent the possibility of its loss or compromise.

Review Activity 2

Classified information identified for destruction must be safeguarded until it is destroyed.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Feedback:

Classified information identified for destruction must be safeguarded until it is properly destroyed.

Review Activity 3

Contractors are required to establish an information management system to protect and control classified information in their possession.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Although there is no required format, contractors are required to establish an information management system so that they are able to retrieve classified information or report on its disposition in a reasonable period of time.

Review Activity 4

All classified information must be numbered in a series.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Only TOP SECRET information not stored in an electronic format on an authorized classified information system must be numbered in a series.

Review Activity 5

Which of the following must a person have to be authorized to handle classified information?

Select all the correct answers. Then check the Answer Key at the end of this Student Guide.

- Classified jurisdiction
- Need-to-know for the classified information in performance of official duties
- Favorable determination of eligibility, or (PCL) for access to classified information
- A signed and approved nondisclosure agreement
- Original classification authority

Feedback:

A person authorized to handle classified information must have a favorable determination of eligibility, also referred to as a personnel clearance, or PCL for access to classified information, has signed an approved nondisclosure agreement, or NDA and has a need-to-know, or NTK for the classified information in performance of official duties.

Lesson 3 Review Activities

Review Activity 1

A person may be authorized to receive and sign for classified information if they are cleared to the level of classified information they are receiving.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

If receiving classified packages is an assigned duty of the cleared employee that establishes need-to-know to the extent necessary to receive the packages.

Review Activity 2

Only an authorized person may receive and sign for packages that may contain classified information.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Only an authorized person may receive and sign for packages that may contain classified information.

Review Activity 3

All employees may pick up classified packages at a P.O. Box as long as they sign a form stating they will not open the package.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Only an authorized person may receive and sign for packages that may contain classified information.

Review Activity 4

The intended recipient of classified information must assure the sender that they are an authorized person at a facility with classified storage capability.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information.

Review Activity 5

Working papers must be marked in the same manner prescribed for a finished document at the same classification level when it is transmitted outside the facility or retained for more than

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- 180 days from the date of creation
- 120 days from the date of completion
- 90 dates from the date of creation

Feedback:

Working papers must be marked in the same manner prescribed for a finished document at the same classification level when it is transmitted outside the facility or retained for more than 180 days from the date of creation.

Lesson 4: Review Activities

Review Activity 1

Which of the following are approved for storing TOP SECRET information (with supplemental controls)?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- Six-sided steel cabinet
- GSA-approved container
- Steel cabinet
- Open storage area
- Vault

Feedback:

Storage containers or areas are all approved for storing TOP SECRET information include a GSA-approved container, open storage area or vault.

Review Activity 2

You must keep a written record of the combination lock of any container in which classified information is stored.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

- True
- False

Feedback:

A written record of the combination is not required. If you keep a written record you must handle and store it at the same classification level as the information it is protecting

Review Activity 3

Storage of TOP SECRET information always requires supplemental protection or security-in-depth during non-working hours regardless of the type of security container used.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

TOP SECRET information always requires supplemental protection (alarms or guards) or security-in-depth (SID) during non-working hours regardless of the type of security container used.

Review Activity 4

When supplemental protection is required, the facility must only use security guards.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

An intrusion detection system is the form of supplemental protection required by the NISPOM, except where security guards were approved prior to January 1, 1995.

Review Activity 5

Security checks are required at the end of the last working shift of each day to ensure classified information is properly stored and security containers are locked.

Select the correct answer. Then check the Answer Key at the end of this Student Guide.

True

False

Feedback:

Security checks are required at the end of the last working shift each day.

Review Activity 6

When must a combination be changed to the lock for a security container used to store classified information?

Select all that apply. Then check the Answer Key at the end of this Student Guide.

At the initial use of an approved container or lock

When anyone who has knowledge of the combination is either terminated or has his or her clearance withdrawn, suspended, or revoked

When a container or its combination has been compromised or suspected of compromise

When a container has been left unlocked and unattended

Other times when deemed necessary by the FSO or CSA

At least once per year

Feedback:

These are all requirements for changing the combination to the lock for a container used to store classified information. The NISPOM does not require combinations to be changed annually, but an FSO may choose to change them annually in addition to the other items listed.

Review Activity 7

In which of these cases would you need to make a report to your DCSA Field Office?

Select all that apply. Then check the Answer Key at the end of this Student Guide.

- You need to store several cubic feet of CONFIDENTIAL documents and have decided to convert a room in the basement of your facility for this purpose.
- You currently store SECRET and CONFIDENTIAL documents in a two-drawer GSA-approved container. You need more storage space, so you have decided to replace the two-drawer model with a four-drawer model.
- You add another cleared employee to your list of persons who have knowledge of the combination to your storage container.
- An afternoon thunderstorm has knocked out the electrical power in your area. As a result, the alarm system that provides supplemental protection for your TOP SECRET storage during nonworking hours is not operating. You are told by the power company that service may not be restored until morning and you have no other way to adequately protect your classified material.

Feedback:

A Change in Storage Capability report must be submitted after the initial acquisition of an approved storage container that raises or lowers the level of classification that a contractor is able to safeguard, in this case because you have converted a room of your facility for the purpose of storing CONFIDENTIAL information. In the case of the power outage, the classified information must be protected continuously until the alarm system is restored and functioning properly. This may be accomplished by having an appropriately cleared authorized person stay with the material until the situation is resolved.

Lesson 5: Review Activities

Review Activity 1

An authorized person may lock classified information in a desk drawer while going down the hall to get a cup of coffee.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

True

False

Feedback:

An authorized person may not lock classified information in their desk drawer when they are not present. Classified information must be under the constant surveillance of an authorized person or returned to its security container.

Review Activity 2

An authorized person may turn classified information over on their desk when an unauthorized person is present.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

True

False

Feedback:

An authorized person may turn classified information over on their desk when an unauthorized person is present. An authorized person may also choose to cover the classified information with something or return the classified information to its security container when an unauthorized person is present.

Review Activity 3

An authorized person is responsible for safeguarding classified information in a restricted area.

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

True

False

Feedback:

An authorized person is responsible for not allowing anyone to have unauthorized access to classified information in the restricted area.

Review Activity 4

An authorized person must escort or control the activities of their classified visitor.

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

True

False

Feedback:

An authorized person must escort or control the movements of their classified visitor.

Lesson 6: Review Activities

Review Activity 1

Which of these cases represent good examples to reproduce classified information for operational needs?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- TOP SECRET documents in preparation of a contract deliverable
- SECRET and CONFIDENTIAL documents in preparation of a solicited bid, quotation or proposal
- SECRET and CONFIDENTIAL documents in preparation of patent applications to be filed in the U.S. Patent Office
- SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract

Feedback:

All of these are good examples of classified information that may be reproduced for a company's operational needs.

Review Activity 2

You are alone making classified copies and the machine jams. You go down the hall to ask for help. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- Permissible
- Problematic

Feedback:

When copying classified information, you should stay with the copier if it malfunctions and send for help, if necessary.

Review Activity 3

John, an authorized person, has a very busy schedule today and, therefore, has requested that his administrative assistant, who is not an authorized person, make copies of classified information on his behalf for his 2 p.m. meeting. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- Permissible
 Problematic

Feedback:

An authorized person may only designate someone who is also an authorized person to make copies of classified information on their behalf.

Review Activity 4

You made copies of some classified information for your meeting in 10 minutes and noticed when you got to your meeting that some of the classification markings were cut off on the copies. You decided to distribute the copies to the meeting participants since they were just copies and not originals. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

- Permissible
 Problematic

Feedback:

All security markings on the originals should also appear on the copies of classified information.

Review Activity 5

After making copies of classified information, Sarah made three blank copies on the copier. Is this action permissible or problematic?

Select the correct answer. Then check your answers in the Answer Key at the end of this Student Guide.

Permissible

Problematic

Feedback:

To ensure that no image of classified information remains on any image bearing part or surface of a copier, you should make three blank copies after you have finished copying classified information.

Lesson 7: Review Activities

Review Activity 1

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

WW can request retention authority from the Navy.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

WW can request retention authority from the Army, not the Navy, by identifying the classified information and justifying the retention on the basis that continued retention will benefit the U.S. Government in the performance of the prospective contract with the Navy. The request should indicate how much longer the company will need to retain the information.

Review Activity 2

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

If WW requests retention authority, they would need to do it within 180 days.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

WW would need to request retention authority within one month, not 180 days, since the standard two-year retention period will expire in one month

Review Activity 3

Scenario: Twenty three months ago Western Widgets (WW) made final delivery of goods and services under a classified contract with the Army. The company has just received a classified invitation for Bids from the Navy. WW's management thinks that the classified information generated for the Army contract would be valuable in performing on the Navy contract, if WW is the successful bidder.

The Navy would need to issue a final DD Form 24 indicating the final retention period and final disposition instructions.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

The Army, not the Navy, would need to issue a final DD Form 254 indicating the final retention period and final disposition instructions

Review Activity 4

In which of the following cases must classified information be returned or destroyed?

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- When a contractor's FCL is terminated
- Within 180 days after the opening date of the bid, proposal, or quote if it was not submitted or if it was withdrawn
- Within two years after receipt of the classified information if it was not obtained under a specific contract
- Within 180 after notification that the submitted bid, proposal, or quote had not been accepted
- Within one year after receipt of the classified information if it was not obtained under a specific contract

Feedback:

Scenarios in which classified information must be returned to the GCA or destroyed, include: when a contractor's FCL is terminated; within 180 days after the opening date of the bid, proposal, or quote if it was not submitted or if it was withdrawn; within 180 days after notification that the submitted bid, proposal, or quote had not been accepted; and within one year after receipt of the classified information if it was not obtained under a specific contract.

Review Activity 5

Classified information in the form of regular paper may be burned.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- True
- False

Feedback:

Classified information in the form of paper may be burned, shredded, pulped, or pulverized.

Review Activity 6

Destruction of classified information must ensure the information cannot be recognized or reconstructed.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

Destruction of classified information must preclude recognition or reconstruction of the information.

Review Activity 7

When destroying classified information with a shredder, shred size is not important.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

When destroying classified information through a shredder, shred size does matter. The NISPOM prescribes a maximum shred size of 1/32 inch by 1/2 inch and the DOD has a new specification of 1 mm by 5 mm or less.

Review Activity 8

Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL documents.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

True

False

Feedback:

Two authorized personnel are required to be present for the destruction of TOP SECRET information but only one authorized person is required to be present for the destruction of SECRET and CONFIDENTIAL information.