Safeguarding Classified Information in the NISP

Student Guide

August 2016

Center for Development of Security Excellence

Lesson 1: Course Introduction

Course Introduction

Course Information

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

Item	Explanation
Purpose	Provide a thorough understanding of the requirements for safeguarding classified material in the NISP as delineated in the National Industrial Security Program Operating Manual (NISPOM).
Audience	• Contractor Facility Security Officers • Security staff of cleared DoD contractors participating in the NISP • DSS Industrial Security Representatives • DoD Industrial Security Specialists
Pass %/Fail	75% on final examination
Estimated completion time	150 minutes

Course Overview

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 DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM). (See NISPOM Chapter 5 Safeguarding Classified Information.)

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:

- 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
- Using Classified Information
- Reproducing Classified Information
- Disposition of Classified Information
- Practical Exercise
- Course Conclusion

Lesson 2: Basic Concepts

Lesson Introduction

Objectives

Before you learn about the various measures for safeguarding classified information, there are some concepts related to safeguarding that you should know. This lesson will familiarize you with these concepts.

Here are the lesson objectives:

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

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Confidential	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
Secret	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Term	Definition/Explanation
Top Secret	The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe

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 waste, and classification-pending material.

Classified working papers are documents that are generated in the preparation of a finished document. Classified waste is classified information that is no longer needed and is pending destruction. Classification-pending documents are documents that require a classification determination from the Government Contracting Activity (GCA). These documents must be safeguarded in accordance with the proposed highest classification level until guidance is received from the GCA.

Throughout this course you will learn the safeguarding requirements for each of these types of classified information.

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 need-to-know for classified information in the performance of official duties and who has been granted a personnel security clearance at the required level.

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 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Authorized persons	A person who has a need-to-know for classified information in the performance of official duties and who has been granted a PCL at the required level.
Personnel security clearance	A personnel security clearance (PCL) is an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted. Note: Eligibility plus access are considered to be equivalent to a personnel security clearance.
Cleared contractors	To become a cleared contractor, a company must obtain a Facility Clearance which is an administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).
Multiple facility organization	A multiple facility organization (MFO) is a legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more contractor facilities.
Classified contract	Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. A contract may be a classified contract even though the contract document is not classified. The requirements prescribed for a "classified contract" also are applicable to all phases of the pre-contract activity.
Prime contract	A contract let by a Government Contracting Agency (GCA) to a contractor for a legitimate government purpose.
Subcontract	Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. For purposes of this manual (the NISPOM), a subcontract is any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

When Authorization is Required

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 NISPOM 5-511 Disclosure to the Public.

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 System

Contractors are required to establish an information management system to protect and control the classified information in their possession. The purpose of this requirement is to ensure that you have the capability to retrieve classified information when it is necessary and to ensure the appropriate disposition of classified information in a reasonable period of time.

There is no required format for such an information management system. The information management system may be in the form of an electronic database or as simple as a spreadsheet or log. You merely have to demonstrate capability for timely retrieval of classified information within the company and the capability to dispose of any and all classified information in the facility's possession when required to do so.

Top Secret Accountability

Access and accountability records must be kept at various points in the Top Secret information lifecycle. When Top Secret information is produced by a contractor, a record must be kept indicating when the finished document was completed, when the information is retained for more than 180 days regardless of its stage of development, or 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 (TTFI IS107.16) offered by the Center for Development of Security Excellence (CDSE).

Each TOP SECRET item must be numbered in a series and the copy number must be placed on TOP SECRET documents and all associated transaction documents. 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.

Review Activity

Review Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: All classified information should be afforded the same level of protection regardless of the classification level of the information.

- ○ True
- ○ False

2 of 4: Classified waste must be safeguarded until it is destroyed.

- ○ True
- ○ False

3 of 4: Contractors are required to establish an information management system to protect and control classified information in their possession.

- ○ True
- ○ False

4 of 4: All classified information must be numbered in a series.

- ○ True
- ○ False

Review Activity 2

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

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

- ☐ Classification jurisdiction
- ☐ Need-to-know
- ☐ Personnel security clearance (PCL)
- ☐ Original classification authority

Lesson 3: Obtaining Classified Information

Lesson Introduction

Objectives

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 in obtaining classified information.

Here are the lesson objectives:

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

Receiving Classified Information

Clearance of Receiving Individual

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. 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 companies 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 transporting and transmitting classified information, refer to the Transmission and Transportation for Industry e-Learning course (TTFI IS107.16) offered by the Center for Development of Security Excellence (CDSE).

Handling Upon Receipt

Once a Registered or Certified classified package has been received by an authorized person, he or she should examine the outer package for evidence of tampering. If the receiver suspects tampering, the Facility Security Officer (FSO) should be immediately notified. The FSO or another cleared employee that the FSO has delegated the responsibility to perform these duties 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 had occurred. If a loss, compromise or suspected compromise has occurred, the FSO must notify both the sender and their Cognizant Security Office (CSO).

If the receiver does not suspect any tampering on 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 had occurred. If a loss, compromise or suspected compromise has occurred, the FSO must notify both the sender and their CSO.

Next the designated custodian incorporates the material into the facility's information management system (IMS) and checks the contents of the package against the receipt. If there is a discrepancy, or if there is no receipt in a TOP SECRET or SECRET package, the sender must be contacted immediately. Receipts are not required for CONFIDENTIAL packages, but may be included at the sender's discretion. If the package contents match the receipt, the designated custodian signs and returns it to the sender.

Next, the designated custodian verifies through the current DoD system of record or the facility's records that the intended recipient has the appropriate clearance level (JPAS/DISS), 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, he or she should

contact the cleared project manager for that contract to determine who should receive the classified material.

See the Flow Chart for this process at the end of this Student Guide.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Tampering	Tampering is a deliberate attempt to gain illegal or unauthorized access to the contents of a shipment.
JPAS	Joint Personnel Adjudication System
DISS	Defense Information System for Security (successor to Joint Personnel Adjudication System or JPAS)

From Commercial Carriers

When a shipment is received via a cleared commercial carrier, usually a trucking firm, the sender notifies the recipient in advance as to when the shipment is to be expected. If the shipment is not received within 48 hours after the expected time of arrival, the recipient must contact the sender immediately.

For more detailed information, refer to the Transmission and Transportation for Industry e-Learning course (TTFI IS107.16) 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 (IF103.16) offered by CDSE.

Contractors are required to properly safeguard any classified materials they generate, or derivatively classify, and implement an IMS which is capable of facilitating the retrieval and disposition of their classified holdings in a timely manner.

Depending on the type of information, additional requirements may apply. The NISPOM requires contractors to keep a formal record of any Top Secret material they receive or generate at their company. Contractors must follow guidance from the Central Office of Record for entering any COMSEC material they generate into the accountability system. The NISPOM also contains guidance about generating and marking 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 Classified Information e-Learning course (IF105.16) and the Marking in the Electronic Environment Short offered by CDSE.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
COMSEC	Communications Security
JPAS	Central Office of Record
Derivative Classification	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.
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
IMS	Information Management System

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

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 the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

Working Papers

The NISPOM also contains requirements that apply when a contractor creates classified working papers in preparation of a finished document. The working papers must be dated when created, marked with their 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 at the same classification level when it is transmitted outside the facility, filed permanently, emailed within or released

outside the originating activity, or retained for more than 180 days from the date of creation. (See NISPOM 5-203b Generation of Classified Material)

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Working Papers	Working papers can be rough drafts, notes, or anything that is not a finished document.
Document	A recorded information, regardless of the nature of the medium or the method or circumstance of recording

Review Activity

Review Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: A person may be authorized to receive and sign for classified information if they are cleared to the level of the classified information they are receiving.

- ○ True
- ○ False

2 of 4: Only an authorized person may receive and sign for packages that may contain classified information.

- ○ True
- ○ False

3 of 4: 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.

- ○ True
- ○ False

4 of 4: The designated document custodian must contact the sender immediately if there is no receipt in a CONFIDENTIAL package.

- ○ True
- ○ False

Review Activity 2

Formal accountability records of material generated within a facility are required for which classification level?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ TOP SECRET
- ○ SECRET
- ○ CONFIDENTIAL

Lesson 4: Storing Classified Information

Lesson Introduction

Objectives

In order to safely store classified information, there are various requirements that must be met, such as use of proper equipment and closed areas, locks, supplemental protection, and safeguarding procedures. In this lesson, you will learn about the various requirements for the physical protection of classified material.

Here are the lesson objectives:

- Identify types of and requirements for using storage equipment and closed 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

Storage Options

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 storage containers or in 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.

Storage Containers

A 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. You can search for the container you need on the GSA Qualified Products List

(QPL). 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 waste pending destruction, there are various types and sizes of GSA-approved storage containers.

For more information on procuring GSA-approved storage containers, refer to the Procuring GSA Security Container Short offered by the Center for Development of Security Excellence (CDSE).

Whether new or used, 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. For used models, 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
GSA	General Services Administration
Types and sizes	Types/sizes of GSA-approved security containers: o 2–drawer, 4-drawer, 5-drawer o Legal size and letter size o Single, dual, or multi-lock o Map and plan containers
GSA test certification label	GSA test certification label: o Indicates class of security container o Class relates to delay afforded against forced, covert, or surreptitious entry o Only Class 5 and 6 containers are available new
GSA-approved security container label	GSA-approved security container label: o Verifies that container is GSA-approved o 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, Neutralization and Repair of GSA Approved Containers and Vault Doors.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Approved methods	Repair procedures may be obtained from the Cognizant Security Agency (CSA). A container that has been repaired using methods other than approved methods may no longer be used for storage of Secret information even with supplemental controls as of October 1, 2012.
FED-STD-809	Neutralization and Repair of GSA Approved Containers and Vault Doors

Storage Areas

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 (NISPOM 5-802). 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 a closed 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 a closed area. Closed areas are much less expensive to build than vaults and are more commonly used. The Cognizant Security Agency (CSA) and the contractor must agree on the need to establish a closed area and its extent, based on the safeguarding requirements of a classified contract, either before or during the life of the contract. The CSA may grant self-approval authority to qualified Facility Security Officers (FSOs) for closed area approvals.

Storage requirements inside closed areas depend on classification level. Open-shelf or bin storage may be used for Secret and Confidential information only if approved by the CSA.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

The CSA may approve open shelf or bin storage of classified documents if there is an operational necessity. The contractor request for open storage must provide justification that the use of GSA-approved security containers will have an adverse impact on contract cost and performance, and describe the security features and practices that will ensure that the documents are properly safeguarded. DSS (CSA) may also require endorsement of the request by the government contracting activity.

ISL 06-02, Paragraph 16 (Closed Areas and Open Storage)

Top Secret information, however, must always be stored in a security container, even in a closed area. Access to closed areas must be protected either through use of a guard, an authorized person, or an access control system. 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 closed areas.

For more information on access control systems, refer to the Physical Security Measures eLearning course (PY103.16) offered by CDSE. The NISPOM contains specific construction requirements for both vaults and closed areas. (See Chapter 5 Safeguarding Classified Information and Chapter 6 Construction Requirements)

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
CSA	Cognizant Security Agencies (CSAs) are agencies of the Executive Branch that have been authorized to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are the Department of Defense, DOE, CIA, DNI, and NRC and DHS.
FSO	Facility Security Officer
GSA	General Services Administration
NISPOM	National Industrial Security Program Operating Manual

Locking Devices

Overview

Security containers, closed 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. Built-in combination locks must meet Federal Specification FF-L-2740B, and padlocks must meet Federal Specification FF-P-110.

The Department of Defense Lock Program has a website with useful information, and a hotline number (805-982-1212) 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 (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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

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 a multiple facility organization, to the home office, and to establish procedures for CSA notification upon the death or incapacitation of that person.

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.

Changing Combinations

Combinations must be changed by an authorized person, or by the Facility Security Officer (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 has his or her 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 the CSA.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Authorized person	A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel security clearance (PCL) at the required level.

Padlocks and Keys

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). These systems must meet specific standards (UL 2050 standards). For more information about intrusion detection systems and their requirements, refer to the NISPOM (Chapter 5 Safeguarding Classified Information and Section 9 Intrusion Detection System), and to the Physical Security Measures eLearning course (PY103.16) 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
UL 2050 standards	These standards are established by the Underwriters Laboratory, Inc. (UL) in cooperation with the US Government. UL is an independent, not-for-profit product safety certification organization. An alarm service company listed by UL must install and service the alarm.
NISPOM	National Industrial Security Program Operating Manual

Storage Procedures

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 closed area must be.

TOP SECRET Storage

Top Secret information must be stored in a GSA-approved security container, vault, or closed 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 a closed 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

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, or 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 Cognizant Security Agency (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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Working hours	Working hours is that time during which the work force in the closed area is working on a regularly scheduled shift.
Non-working hours	Non-working hours includes any time of day when cleared employees are not in the work area.

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

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Non-working hours	Non-working hours includes any time of day when cleared employees are not in the work area.

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 three reports related to storage be sent to the CSA. For DoD, these reports are sent to Defense Security Service (DSS) 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. (See NISPOM 1-0302h)

The next report, Inability to Safeguard Classified Material, is required to be submitted after an emergency that makes a facility incapable of safeguarding classified material. 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. (See NISPOM 1-302i)

The last report, Security Equipment Vulnerability, is required when significant vulnerabilities are identified in security equipment used to protect classified information -- for example, if the locking

mechanism on a security container fails. Any time there is an inability to safeguard classified information or a vulnerability occurs, steps must be taken to ensure that the material is protected at all times until the situation is corrected. This may require an authorized person to stay with the material until it is properly secured. (See NISPOM 1-302j)

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 (NISPOM Para. 5-102 End of Day Security Checks). 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.

An example of a security container record is one that has columns to record the date and time a security container was opened, closed, and checked.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
NISPOM	National Industrial Security Program Operating Manual

Review Activity

Review Activity 1

Which of the following are approved for storing Top Secret information (with supplemental controls)?

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

- ☐ Six-sided steel cabinet
- ☐ GSA-approved container
- ☐ Steel cabinet
- ☐ Closed area
- ☐ Vault

Review Activity 2

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: You should keep a written record of the combination to the lock of any container in which classified information is stored.

- ○ True
- ○ False

2 of 4: 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.

- ○ True
- ○ False

3 of 4: When supplemental protection is required, each facility must decide whether to use an intrusion detection system or security guards.

- ○ True
- ○ False

4 of 4: 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.

- ○ True
- ○ False

Review Activity 3

Which of the following are reasons for changing the combination to the lock for a container used to store classified information?

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

- ☐ Before the initial classified use of the container
- ☐ After the termination of employment or the withdrawal, suspension, or revocation of clearance of a person knowing the combination
- ☐ After the compromise or suspected compromise of the container or the combination
- ☐ After the container has been left unlocked and unattended
- ☐ When the FSO or CSA decide that the combination needs to be changed
- ☐ At least once per year

Review Activity 4

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

Select all that apply. Check your answers in 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 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

Objectives

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.

Here are the lesson objectives:

- Identify requirements for handling classified information
- Identify best practices for oral discussions regarding classified information

Handling Classified Information

Physical Handing

Contractors are responsible for safeguarding classified information in their custody or under their control to reasonably foreclose the possibility of its 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 and the area becomes a regular work area once again.

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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Restricted areas	A restricted area is a controlled access area established to safeguard classified material, that because of its size or nature cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

It is recommended that an authorized person conduct the actual perimeter control inspections. Ensure this authorized person knows that they are looking for classified information and the proper safeguarding procedures to follow should classified information be found.

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 a good idea to consult with your company's safety officer.

Classified Visitors

When a classified visitor arrives at your facility, 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 classified visitor leaves, you must also ensure all classified information that they used during their visit has been returned.

For more information on classified visits, refer to the Visits and Meetings in the NISP e-Learning course (IS105.16) offered by the Center for Development of Security Excellence (CDSE).

Oral Discussions

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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
NISPOM	National Industrial Security Program Operating Manual

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. Depending on the device, appropriate security measures range from requiring them to be turned off to not allowing them in the area. (See ISL 2006-02.)

Review Activity

Review Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

An authorized person:

1 of 4: May lock classified information in his or her desk drawer while he or she goes down the hall to get a cup of coffee

- ○ True
- ○ False

2 of 4: May turn classified information over on his or her desk when an unauthorized person is present

- ○ True
- ○ False

3 of 4: Is responsible for safeguarding classified information in a restricted area

- ○ True
- ○ False

4 of 4: Must escort or control the activities of their classified visitor

- ○ True
- ○ False

Review Activity 2

Where may classified information be discussed between authorized persons?

Select all that apply. 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

Objectives

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.

Here are the lesson objectives:

- 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 guideless regarding when to obtain prior authorization from the contracting officer or some other government authority.

The NISPOM states that TOP SECRET information may be reproduced without GCA authorization when preparing a contract deliverable. GCA authorization would be required for the reproduction of TOP SECRET documents for any other reason.

The NISPOM also states that GCA authorization would not be required for the reproduction of SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract in the furtherance of a prime contract, in preparation of a solicited or unsolicited bid, quotation, or proposal to a Federal agency or prospective subcontractor, or in preparation of patent applications to be filed in the U.S. Patent Office. Reproductions of SECRET and CONFIDENTIAL information for any other purpose would require authorization from the GCA.

(See NISPOM Para 5-601 Limitations)

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
NISPOM	National Industrial Security Program Operating Manual
GCA	Government Contracting Activity

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.

(See NISPOM Para. 5-600 General and Section 6 Reproduction)

Reproduction Requests

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 Facility Security Officer (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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
NISPOM	National Industrial Security Program Operating Manual
SPP	Standard Practice Procedures

Procedures

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 accredited in accordance with NISPOM Chapter 8 before they are used for any classified work.

The facility should coordinate with their DSS 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 DSS Information Systems

Security Professional (ISSP) to determine what approvals or accreditations are needed for a particular piece of equipment and what procedures need to be followed.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
NISPOM	National Industrial Security Program Operating Manual
ISSP	Information Systems Security Professional

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 has 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 no 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 accredited as an information system. Since copiers that have memory or hard drives may have to be accredited 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Equipment vulnerabilities	o Paper jams may cause paper with images to be retained in the machine o Ink on rollers may retain images of classified information o Extra copies or partial copies may be retained in the machine or discarded via a special port

Review Activity

Review Activity 1

In which of these cases may classified information be reproduced without obtaining GCA authorization?

Select all that apply. 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 or unsolicited bid, quotation or proposal to a Federal agency or prospective subcontractor
- ☐ SECRET and CONFIDENTIAL documents in preparation of patent applications to be filed in the U.S. Patent Office
- ☐ TOP SECRET documents in preparation of a solicited or unsolicited bid, quotation or proposal to a Federal agency or prospective subcontractor
- ☐ SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract in furtherance of a prime contract

Review Activity 2

Select your response. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: 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?

- ○ Permissible
- ○ Problematic

2 of 4: 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.

- ○ Permissible
- ○ Problematic

3 of 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.

- ○ Permissible
- ○ Problematic

4 of 4: After making copies of classified information, Sarah made three blank copies on the copier.

- ○ Permissible
- ○ Problematic

Lesson 7: Disposition of Classified Information

Lesson Introduction

Objectives

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:

- Identify the requirements for retaining classified information
- Identify the requirements for returning classified information to the Government Contracting Activity (GCA)
- 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 classified information received or generated under a classified contract for two years after completion of the contract, provided the GCA does not instruct otherwise. 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 2 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.

MORE

Contractors must identify classified information for retention beyond 2 years as follows: TOP SECRET information must be identified in a list of specific documents unless the GCA authorizes identification by subject matter and the approximate number of documents; SECRET and CONFIDENTIAL information may be identified by general subject matter and the approximate number of documents.

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).

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.

(See NISPOM Section 7 Disposition and Retention)

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Declassify	Declassification is the determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.
GCA	Government Contracting Activity
NISPOM	National Industrial Security Program Operating Manual

Disposition Schedule

Requirements

Classified information must be returned or destroyed if the facility security 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 1 year after receiving it.

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

Destruction

Requirements

Types of classified information that contractors must destroy include multiple copies, obsolete material, and classified waste. 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 2 years. 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

TOP SECRET destruction records can be combined with other control records and must be retained for 2 years.

Methods

According to the NISPOM, the method of destruction must preclude recognition or reconstruction of the classified information. (See NISPOM Chapter 5 Safeguarding Classified Information and Section 7 Disposition and Retention)

Classified information may be destroyed by various methods such as burning, shredding, pulping, melting, mutilation, chemical decomposition, pulverizing, overwriting, degaussing, sanding or grinding. Paper products may be destroyed using incinerators, pulpers, pulverizers, or shredders. However, water repellant 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.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

MORE

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 ½ 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 NSA Evaluated Products List of High Security Crosscut Shredders. This list may be obtained from the CSA.

The current Department of Defense (DoD) specification for shred size is 1 mm X 5 mm or less.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Term	Definition/Explanation
Burning	Note that if you intend to use public destruction facilities, such as a public incinerator, you must obtain approval from your CSA, usually the DSS 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 repellant paper products	High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellant 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 CDs and DVDs.

Review Activity

Review Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

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 documents for the Army contract would be of great value in performing on the Navy contract, if WW is the successful bidder.

1 of 4: WW can request retention authority from the Navy.

- ○ True
- ○ False

2 of 4: If WW requests retention authority, they would need to do it within 180 days.

- ○ True
- ○ False

3 of 4: The Navy would need to issue a final DD Form 254 indicating the final retention period and final disposition instructions.

- ○ True
- ○ False

4 of 4: The Army would need to issue a final DD Form 254 or a letter indicating the final retention period and final disposition instructions.

- ○ True
- ○ False

Review Activity 2

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

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

- ☐ If the contractor's FCL is terminated
- ☐ If the information was part of an unsubmitted bid, proposal, or quote, and 180 days have passed since the opening date
- ☐ If the information was part of a withdrawn bid, proposal, or quote, and 180 days have passed since the date withdrawn

- ☐ If the information was part of a bid, proposal, or quote that was not accepted, and 180 days have passed since the notification of declination
- ☐ If the information was not obtained under a specific contract and 1 year has passed since receipt of that information

Review Activity 3

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

1 of 4: Classified information in the form of regular paper may be burned.

- ○ True
- ○ False

2 of 4: Destruction of classified information must ensure the information cannot be recognized or reconstructed.

- ○ True
- ○ False

3 of 4: When destroying classified information through a shredder, shred size is not important.

- ○ True
- ○ False

4 of 4: Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL information.

- ○ 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 This Area

Visitors 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.

Classified information must be:

- Received by an authorized person who:
  - Has a need-to-know
  - Is cleared to the level of the classified material
  - Can properly safeguard the package if necessary
- Refused if an authorized person is not available to receive the package

Package

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

When receiving classified information:

- Inspect the package for evidence of tampering
- Coordinate with the Facility Security Officer (FSO) to contact the sender immediately, if you suspect tampering

Visitor Log

Make sure you know the procedures for receiving classified visitors so they are easy to apply when visitors arrive. When classified visitors visit your facility, you must:

- Positively identify the visitor
- Verify visitor's:
  - Personnel clearance
  - Need-to-know
- Brief the visitor on security procedures relevant to this visit
- Prevent visitor from having unauthorized access to information outside the scope of the approved visit
- Recover all classified information used by the visitor
- Keep required records:
  - NATO visits (NISPOM 10-721)
  - Foreign visits (NISPOM 10-507)
  - Record of all visitors is NOT required by NISPOM, but is a good security practice

Drawer in unsecured filing cabinet

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

When receiving classified information:

- Store unopened package as if it contains classified information

Handling Classified Information

Look around this classified work area. What items can you find that have implications for safeguarding classified information?

Telephone

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.

Discuss classified information ONLY on approved secure telephones:

- Use Secure Telephone Equipment (STE) or other secure telephones, and
- Follow procedures approved by the CSA

- Be aware of any unauthorized individuals who might overhear the classified conversation

When making unsecured phone calls:

- Be aware that background discussions in the area of the phone may be overheard over the phone line
- Ensure no classified discussions are taking place around the phone

Wireless Device

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

Protect classified information from disclosure through the use of wireless devices. When working with classified information, do not carry:

- Cell phones
- Other mobile devices

Why? Cell phones and other wireless devices introduce an unacceptable vulnerability by which information may be compromised.

Open Safe Drawer

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

Locks on security container and vaults:

- Must be kept locked when not supervised by an authorized person
- Must be an approved type:
  - Combination locks
  - Padlocks with combinations
  - Padlocks with keys
- Must meet standards established by the CSA

Security Check Record

At the end of the day, you need to 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.

End of day security checks:

- Purpose:
  - To ensure classified information is properly stored
  - To ensure the security container or area is locked
- Required at end of last working shift
- Records not required but good security practice

Classified Information Inventory

You must have and use a system to manage classified information so that it can be retrieved and disposed of in a timely manner.

Information Management System (IMS):

- Protect and control classified information to ensure timely:
  - Information retrieval
  - Disposition
- No specific format required; possibilities include:
  - Electronic database
  - Spreadsheet
  - Log

See NISPOM Paragraph 5-200 (Control and Accountability, Policy)

SECRET Document

Make sure you protect classified information at all times!

When working with classified information:

- Limit access to your work area to prevent unauthorized people from gaining access to classified information
- Protect classified information when an unauthorized person is present:
  - Cover it

- Turn it face down
- Place it back in its storage container
- Turn off computer monitor

White Board

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

When working with classified information:

- Protect it from unauthorized disclosure by not posting it in an open area

Computer Monitor

When working with classified information, be sure to use only approved information systems, and remember to protect what appears on your monitor.

When working with classified information:

- Only information systems approved in accordance with NISPOM Chapter 8 may be used to process classified information
- When unauthorized persons are present, you must turn your computer monitor off if it is displaying classified information

Printer

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

Printing classified information:

- Immediately retrieve it from the printer as soon as you print it
- Report to FSO any classified information you find left on a printer

Copy Room

Copy Machine

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

When making copies of classified information:

- Use equipment specifically designated for reproduction of classified information

- Do not use equipment that retains an image or electronic record or memory of the item copied unless specifically approved by the CSA
    - This equipment may require special treatment

Equipment Use Rules

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

When making copies of classified information:

- Post rules for using designated equipment

Shredder

Be sure to destroy classified material appropriately!

Manner of destroying classified information:

- Must prevent recognition or reconstruction of information
- Residue must not contain any traces of classified information
- Must use methods approved by the CSA

A shredder may be used for destroying paper products and water-repellant paper products. Cross-cut shredders must satisfy NISPOM 5-705.

Classified Documents for Reproduction

Limit the number of copies you make. Make only as many as you need.

When making copies of classified information:

- First determine the purpose and seek approval if required
- Determine exact number of copies needed
- Consider how to minimize number of copies
- Review copies to ensure appropriate markings are visible
- Allow only authorized personnel to make copies
- Top Secret information is accounted for and entered into the information management system

Classified Papers for Destruction

Be sure you destroy extra copies, anything that is obsolete, and all classified waste. Remember, when destroying Top Secret information, two individuals must be present and destruction record retained for 2 years.

What to destroy:

- Multiple copies
- Obsolete material
- Classified waste

How to destroy:

- Top Secret information requires two individuals and destruction record retained for 2 years
- Secret/Confidential information requires one individual

Recycle Bin

Do not put classified waste in with the ordinary trash or recyclables. You must protect it as classified material until it is properly destroyed.

Manner of destroying classified information:

- Protect classified waste until it is properly destroyed
- It is a good security practice to segregate recycle and trash bins from classified destruction collection points

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 DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM). (See NISPOM Chapter 5 Safeguarding Classified Information.)

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
- Safeguarding Challenge
- Course Conclusion

Course Objectives

You should now be able to perform all of 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 credit for this course, you must take the Safeguarding Classified Information in the NISP examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Appendix A: Answer Key—Review Activities

Lesson 2 Review Activities (Answer Key)

Review Activity 1

1 of 4: All classified information should be afforded the same level of protection regardless of the classification level of the information.

- ○ True
- ⦿ False (correct response)

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

2 of 4: Classified waste must be safeguarded until it is destroyed.

- ⦿ True (correct response)
- ○ False

Feedback*: Classified waste must be safeguarded until it is properly destroyed.*

3 of 4: Contractors are required to establish an information management system to protect and control classified information in their possession.

- ⦿ True (correct response)
- ○ 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.*

4 of 4: All classified information must be numbered in a series.

- ○ True
- ⦿ False (correct response)

Feedback*: Only TOP SECRET information must be numbered in a series.*

Review Activity 2

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

- ☐ Classification jurisdiction
- ☑ Need-to-know (correct response)

- ☑ Personnel security clearance (PCL) (correct response)
- ☐ Original classification authority

***Feedback**: A person authorized to handle classified information must have a need-to-know for the classified information and a personnel security clearance.*

Lesson 3 Review Activities (Answer Key)

Review Activity 1

1 of 4: A person may be authorized to receive and sign for classified information if they are cleared to the level of the classified information they are receiving.

- ⦿ True (correct response)
- ○ 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.*

2 of 4: Only an authorized person may receive and sign for packages that may contain classified information.

- ⦿ True (correct response)
- ○ False

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

3 of 4: 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.

- ○ True
- ⦿ False (correct response)

***Feedback**: Only an authorized person may pick up and sign for packages from a P.O. box that may contain classified information.*

4 of 4: The designated document custodian must contact the sender immediately if there is no receipt in a CONFIDENTIAL package.

- ○ True
- ⦿ False (correct response)

***Feedback**: Receipts are not required for transmission of Confidential information.*

Review Activity 2

Formal accountability records of material generated within a facility are required for which classification level?

- ⦿ TOP SECRET (correct response)
- ○ SECRET

○ CONFIDENTIAL

***Feedback**: Records are required for TOP SECRET material generated by a contractor.*

Lesson 4 Review Activities (Answer Key)

Review Activity 1

Which of the following are approved for storing Top Secret information (with supplemental controls)?

- ☐ Six-sided steel cabinet
- ☑ GSA-approved container (correct response)
- ☐ Steel cabinet
- ☑ Closed area (correct response)
- ☑ Vault (correct response)

***Feedback**: These storage containers or areas are all approved for storing Top Secret information.*

Review Activity 2

1 of 4: You should keep a written record of the combination to the lock of any container in which classified information is stored.

- ○ True
- ⦿ False (correct response)

***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..*

2 of 4: 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.

- ⦿ True (correct response)
- ○ 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.*

3 of 4: When supplemental protection is required, each facility must decide whether to use an intrusion detection system or security guards.

- ○ True
- ⦿ False (correct response)

***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.*

4 of 4: 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.

- ⊙ True (correct response)
- ○ False

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

Review Activity 3

Which of the following are reasons for changing the combination to the lock for a container used to store classified information?

- ☑ Before the initial classified use of the container (correct response)
- ☑ After the termination of employment or the withdrawal, suspension, or revocation of clearance of a person knowing the combination (correct response)
- ☑ After the compromise or suspected compromise of the container or the combination (correct response)
- ☑ After the container has been left unlocked and unattended (correct response)
- ☑ When the FSO or CSA decide that the combination needs to be changed (correct response)
- ☐ At least once per year

***Feedback**: These are all reasons 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.*

Activity 4

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

- ☑ 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. (correct response)
- ☐ 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 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. (correct response)

***Feedback**: In the highlighted cases you would need to make a report to the DSS Field Office. 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 storing all of the material in a GSA-approved container or by having an appropriately cleared authorized person stay with the material until the situation is resolved.*

Lesson 5 Review Activities (Answer Key)

Review Activity 1

An authorized person:

1 of 4: May lock classified information in his or her desk drawer while he or she goes down the hall to get a cup of coffee

- ○ True
- ⦿ False (correct response)

***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.*

2 of 4: May turn classified information over on his or her desk when an unauthorized person is present

- ⦿ True (correct response)
- ○ False

***Feedback**: An authorized person may turn classified information over on his or her 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.*

3 of 4: Is responsible for safeguarding classified information in a restricted area

- ⦿ True (correct response)
- ○ False

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

4 of 4: Must escort or control the activities of their classified visitor

- ⦿ True (correct response)
- ○ False

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

Review Activity 2

Where may classified information be discussed between authorized persons?

- ☐ In elevators if only authorized persons are on the elevator

- ☑ In a restricted area (correct response)
- ☐ On cell phones in restricted areas
- ☑ On secure telephones (correct response)

***Feedback**: Classified information may be discussed between authorized persons in these manners. Even when in a restricted area a cleared employee must ensure that no unauthorized person can overhear the conversation.*

Lesson 6 Review Activities (Answer Key)

Review Activity 1

In which of these cases may classified information be reproduced without obtaining GCA authorization?

- ☑ TOP SECRET documents in preparation of a contract deliverable (correct response)
- ☑ SECRET and CONFIDENTIAL documents in preparation of a solicited or unsolicited bid, quotation or proposal to a Federal agency or prospective subcontractor (correct response)
- ☑ SECRET and CONFIDENTIAL documents in preparation of patent applications to be filed in the U.S. Patent Office (correct response)
- ☐ TOP SECRET documents in preparation of a solicited or unsolicited bid, quotation or proposal to a Federal agency or prospective subcontractor
- ☑ SECRET and CONFIDENTIAL documents in the performance of a prime contract or a subcontract in furtherance of a prime contract (correct response)

***Feedback**: Classified information may be reproduced without obtaining GCA authorization in these cases.*

Review Activity 2

1 of 4: 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?

- ○ Permissible
- ⊙ Problematic (correct response)

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

2 of 4: 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.

- ○ Permissible
- ⊙ Problematic (correct response)

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

3 of 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.

- ○ Permissible
- ⦿ Problematic (correct response)

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

4 of 4: After making copies of classified information, Sarah made three blank copies on the copier.

- ⦿ Permissible (correct response)
- ○ 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 (Answer Key)

Review Activity 1

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 documents for the Army contract would be of great value in performing on the Navy contract, if WW is the successful bidder.

1 of 4: WW can request retention authority from the Navy.

- ○ True
- ⦿ False (correct response)

***Feedback**: WW can request retention authority from the Army, not the Navy, by identifying the documents 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 documents.*

2 of 4: If WW requests retention authority, they would need to do it within 180 days.

- ○ True
- ⦿ False (correct response)

***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.*

3 of 4: The Navy would need to issue a final DD Form 254 indicating the final retention period and final disposition instructions.

- ○ True
- ⦿ False (correct response)

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

4 of 4: The Army would need to issue a final DD Form 254 or a letter indicating the final retention period and final disposition instructions.

- ⦿ True (correct response)
- ○ False

***Feedback**: The Army would need to issue a final DD Form 254 or a letter indicating the final retention period and final disposition instructions.*

Review Activity 2

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

- ☑ If the contractor's FCL is terminated (correct response)
- ☑ If the information was part of an unsubmitted bid, proposal, or quote, and 180 days have passed since the opening date (correct response)
- ☐ If the information was part of a withdrawn bid, proposal, or quote, and 180 days have passed since the date withdrawn
- ☑ If the information was part of a bid, proposal, or quote that was not accepted, and 180 days have passed since the notification of declination (correct response)
- ☑ If the information was not obtained under a specific contract and 1 year has passed since receipt of that information (correct response)

***Feedback**: These are the correct scenarios in which classified information must be returned to the GCA or destroyed.*

Review Activity 3

1 of 4: Classified information in the form of regular paper may be burned.

- ⦿ True (correct response)
- ○ False

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

2 of 4: Destruction of classified information must ensure the information cannot be recognized or reconstructed.

- ⦿ True (correct response)
- ○ False

***Feedback**: Destruction of classified information must preclude recognition or reconstruction of the information.*

3 of 4: When destroying classified information through a shredder, shred size is not important.

- ○ True
- ⦿ False (correct response)

***Feedback**: When destroying classified information through a shredder, shred size does matter. The NISPOM prescribes a maximum shred size of 1/32 inch by ½ inch and the DoD has a new specification of 1 mm by 5 mm or less.*

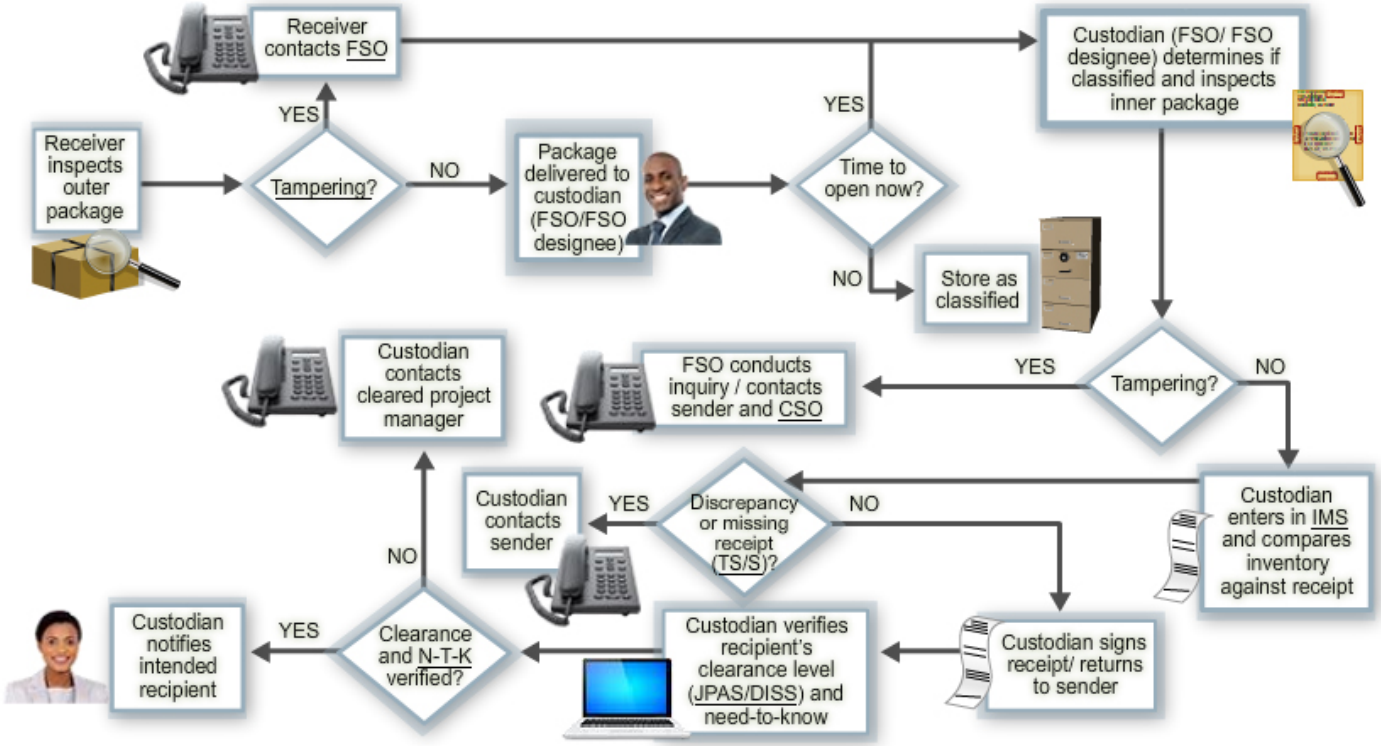
4 of 4: Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL information.

- ○ True
- ⦿ False (correct response)

***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.*

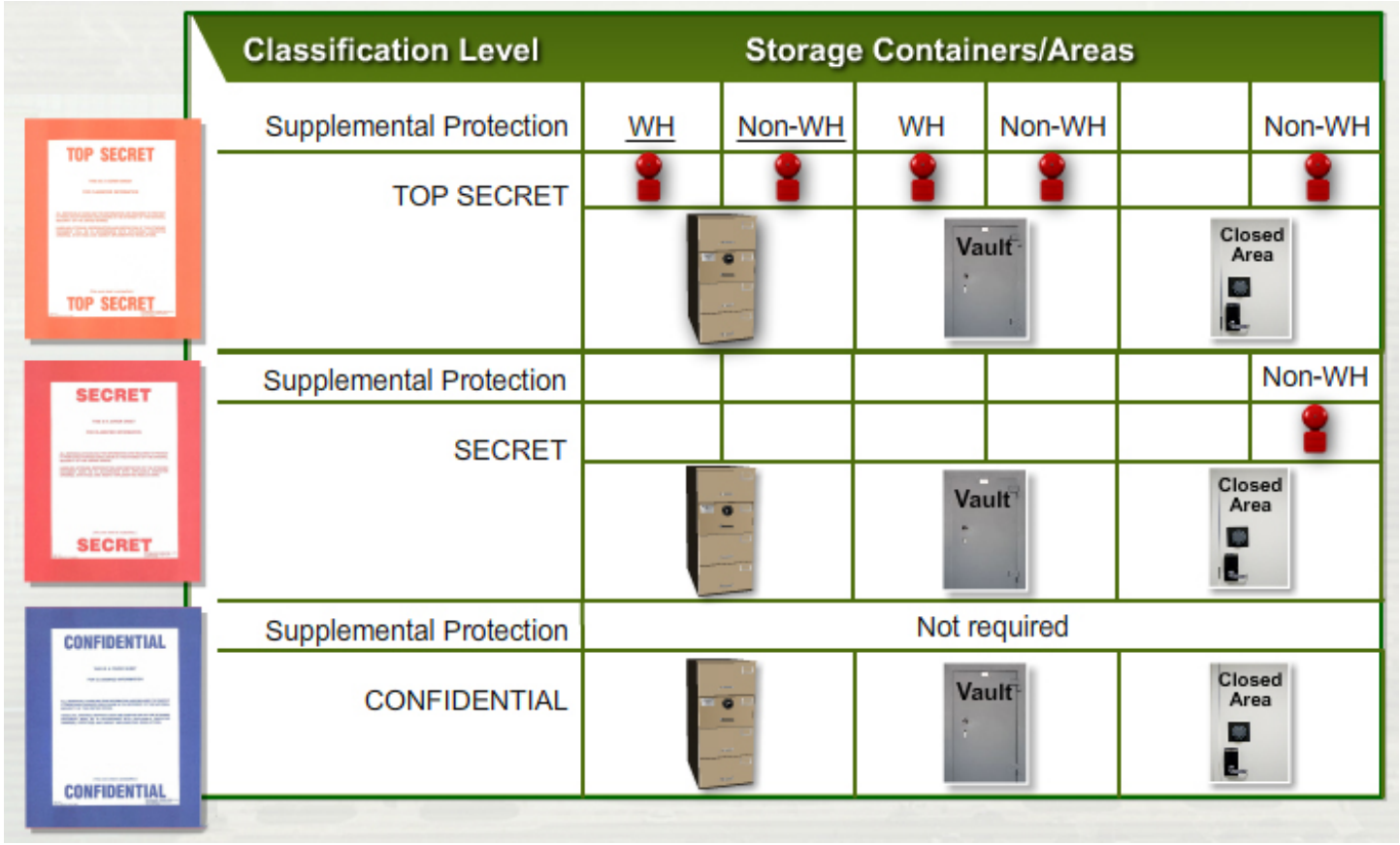
Appendix B: Job Aids

Handling Classified Information Flow Chart



KEY:			
CSO	Cognizant Security Office	JPAS	Joint Personnel Adjudication System
DISS	Defense Information System for Security	N-T-K	need-to-know
FSO	Facility Security Officer	TS/S	Top Secret/Secret
IMS	Information Management System	tampering	Tampering is a deliberate attempt to gain illegal or unauthorized access to the contents of a shipment.

Storage Requirements by Classification Level



WH = Working hours