Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Course Introduction

Course Information

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
POC	DSS.Academy@dss.mil
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 destroy 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). 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

- 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

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: 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 destroy 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). 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:

- Basic Concepts
- Obtaining Classified Information
- Storing Classified Information
- Using Classified Information
- Reproducing Classified Information
- Disposition of Classified Information
- Safeguarding Challenge

Course Objectives

You should now be able to:

- √ 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

Conclusion

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 DSS Academy's ENROL system to register for the on-line exam.

Course Structure

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

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Basic Concepts

Lesson Introduction

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

The lesson objectives are:

- 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

1. Classification Levels

Classified information is categorized into three classification levels: Confidential, Secret, and Top Secret. Classification levels are applied to information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to national security.

Classification Level	Degree of Harm to National Security from Unauthorized Disclosure
Confidential	Damage
Secret	Serious damage
Top Secret	Exceptionally grave damage

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.

2. Forms of Classified Information

All forms of classified information must be protected. Forms of classified information include classified finished or final documents, 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 material is material that contains information that seems to require safeguarding but has not yet been marked classified. Throughout this course you will learn the safeguarding requirements for each of these types of classified information.

Disclosure of Classified Information

1. 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, or 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.

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

Information Management Requirements

1. 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 can 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.

2. 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 or received by a

contractor, a record must be kept indicating when the finished document was completed, when the information is retained for more than 30 days regardless of its stage of development, or when it is transmitted inside or outside the facility.

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

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Select True or False for each statement.

	True	False
All classified information should be afforded the same level of protection regardless of the classification level of the information.	○	○
Classified waste must be safeguarded until it is destroyed.	○	○
Contractors are required to establish an information management system to protect and control classified information in their possession.	○	○
All classified information must be numbered in a series.	○	○

Question 2

Which of the following must a person have to be authorized to handle classified information? Select all that apply.

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

Lesson Conclusion

In this lesson, you learned about key concepts related to safeguarding classified information, such as the types of classified information, authorized disclosure of that information, and the information management requirements for classified information.

Answer Key

Question 1

	True	False
All classified information should be afforded the same level of protection regardless of the classification level of the information.	○	●
Classified waste must be safeguarded until it is destroyed.	●	○
Contractors are required to establish an information management system to protect and control classified information in their possession.	●	○
All classified information must be numbered in a series.	○	●

Question 2

A person must have both a **need-to-know** and a **personnel security clearance (PCL)** to be authorized to handle classified information.

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Obtaining Classified Information

Lesson Introduction

Contractors can obtain classified information either by receiving it from the government or another contractor, or by generating it internally. In this lesson you will learn about the guidelines contractors must follow in obtaining classified information.

The lesson objectives are:

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

Receiving Classified Information

1. Clearance of Receiving Individual

Classified material coming into a facility must be received directly by authorized personnel, regardless of the delivery method. 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, or 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 web-based training course offered by the DSS Academy.

2. Handling Upon Receipt

Once a classified package has been received by an authorized person, he or she should examine the outer package for evidence of tampering. If the recipient suspects tampering, he or she coordinates with the Facility Security Officer, or FSO, to contact the sender immediately. The FSO must evaluate the situation and when appropriate report loss, compromise or suspected compromise of classified information in accordance with the NISPOM.

After inspection, the recipient must turn the package over to the designated document custodian for processing. This processing includes incorporating the material into the facility's information management system, or IMS. The document custodian may actually be the FSO or it could be an appropriately cleared person that the FSO has designated to perform these duties. If the custodian is not able to open and process the package at that time, it must be stored as if it were classified until it is opened and the determination is made as to whether the contents are classified or not.

When the designated custodian can open and process the package, he or she inspects the *inner* package for evidence of tampering. If the custodian detects tampering, he or she coordinates with the FSO to contact the sender immediately. The FSO must evaluate the situation and when appropriate report loss, compromise or suspected compromise of classified information in accordance with the NISPOM.

Next the custodian 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 custodian or FSO must contact the sender 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 FSO or designated custodian signs and returns it to the sender.

Next, the custodian verifies through the Joint Personnel Adjudication System (JPAS) or the facility’s records that the intended recipient has the appropriate clearance level, and verifies the intended recipient’s need-to-know. This may be done by contacting the recipient’s supervisor or project manager. In many cases this determination will be made by the FSO who is aware of what projects each cleared employee is working on.

After verification of these items, the custodian notifies the recipient that the material has arrived and arranges for that person to access the information. If the custodian cannot verify the intended recipient’s clearance level or need-to-know, the FSO should contact the sender or cleared project managers within the facility to determine who should receive the classified material.

3. From Cleared 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 web-based training course offered by the DSS Academy.

Generating Classified Information

1. 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 web-based training course offered by the DSS Academy.

Contractors are required to properly safeguard any classified materials they generate. Each time a contractor generates classified material, it needs to enter it into the facility's information management system (IMS). The IMS should include provisions for any classified material that the contractor will generate. Depending on the type of information, additional requirements may apply. The NISPOM requires contractors to keep a record of any Top Secret material they generate. Contractors must follow guidance from the Central Office of Record (COR) for entering any Communications Security (COMSEC) material they generate into the accountability system.

The NISPOM also contains guidance about generating and marking North Atlantic Treaty Organization (NATO) materials. Finally, contractors must properly mark all classified information they generate. For more information about properly marking classified information, refer to the Marking Classified Information web-based training course offered by the DSS Academy.

2. 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 overall classification and 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 or retained for more than 30 days from the date of creation for TOP SECRET material or 180 days from the date of creation for SECRET and CONFIDENTIAL material.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Select True or False for each statement.

	True	False
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.	○	○
Only an authorized person may receive and sign for packages that may contain classified information.	○	○
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.	○	○
The designated document custodian must contact the sender immediately if there is no receipt in a CONFIDENTIAL package.	○	○

Question 2

Formal accountability records of material generated within a facility are required for which classification level? Select the best response.

- ○ TOP SECRET
- ○ SECRET
- ○ CONFIDENTIAL

Lesson Conclusion

In this lesson you learned about the contractor's responsibilities related to obtaining classified information whether by receiving classified information or by generating classified information.

Answer Key

Question 1

	True	False
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.	●	○
Only an authorized person may receive and sign for packages that may contain classified information.	●	○
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.	○	●
The designated document custodian must contact the sender immediately if there is no receipt in a CONFIDENTIAL package.	○	●

The document custodian should contact the FSO. The facility that receives the information needs to contact the sender. Normally the FSO is the facility's POC for security related matters.

Question 2

Formal accountability records of material generated within a facility are required for **Top Secret** material received or generated by a contractor.

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Storing Classified Information

Lesson Introduction

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.

The lesson objectives are:

- 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

1. 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 storage areas. The storage container or area 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.

2. Storage Containers

There are two categories of storage containers that you can use to safeguard classified information. The preferred type is a GSA-approved security container. 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. Other types of storage containers are referred to as substandard containers, and may include safes, steel file cabinets or safe-type steel file containers with automatic unit locking mechanisms, and 6-sided steel file cabinets secured by a rigid metal lock bar and an approved key operated or combination padlock. These substandard containers may be used to protect classified information until October 1, 2012. In the event that any of these storage containers is not operating correctly, there are special requirements about repairing them.

a. GSA-approved Security Containers

The GSA establishes and publishes uniform standards, specifications, and supply schedules for its approved containers. You can obtain copies of specifications and schedules from any GSA regional office. Because the type and size of storage container you need depends on how much classified information you need to store, including classified waste pending destruction, there are various types and sizes of GSA-approved storage containers.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

Types/sizes of GSA-approved security containers:

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

There are currently only two suppliers of GSA-approved storage containers: Hamilton Products and Diebold. However, when purchasing *used* GSA-approved containers, you may see other manufacturers such as Mosler. 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.

GSA test certification label:

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

GSA-approved security container label:

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

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.

b. 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.

3. 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. 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.

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
- Describe the security features and practices that will ensure that the documents are properly safeguarded

DSS 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. For more information on access

control systems, refer to the Physical Security Measures web-based training course offered by the DSS Academy. The NISPOM contains specific construction requirements for both vaults and closed areas.

Locking Devices

1. 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. The Department of Defense Lock Program has a website with useful information, and a hotline number you can call with any questions related to locks for security containers and areas. You can also call the hotline to obtain free magnetic Closed 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.

2. Combination Locks

Built-in combination locks are the most widely used type of lock on security containers and vaults for protecting classified information. The most common models of combination locks used on security containers are the X07, X08, and X09 locks because they are the only locks that meet the current Federal Specification. The X09 is the model that is currently in production. They have sophisticated anti-manipulation security features to resist certain types of attacks, such as an attack using an auto-dialer. The locks also have audit features such as the ability to track the number of times the lock has been correctly opened.

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 Sargent and Greenleaf (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.

a. 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.

It is better to create a combination that is easy to remember, so that you don't have to write it down. A good way to do this is to think of a six letter word that you would easily remember, but that others wouldn't easily guess, and then use the numbers on a telephone keypad that correspond to the letters in your word. For example, if your word is Harley, then the corresponding combination numbers would be 42-75-39.

There are special requirements for facilities at which only one person is assigned to make sure the combination is preserved if that person is unavailable for some reason. It is important that your cleared employees know what they can and cannot do when it comes to remembering combinations. Good security education is the key to safeguarding combinations.

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
- Establish procedures for CSA notification upon the death or incapacitation of that person

b. 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 Cognizant Security Agency (CSA).

3. 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

1. 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. For more information about intrusion detection systems and their requirements, refer to the NISPOM, and to the Physical Security Measures web-based training course offered by the DSS Academy.

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 because IDS is a more cost-effective security option.

Storage Procedures

1. 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.

a. 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.

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) 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.

b. Secret Storage

Secret information must be stored in any of the three areas approved for Top Secret information, or in a safe, a steel file cabinet, or a safe-type, steel file container that has an automatic unit locking mechanism, or any 6-sided steel file cabinet welded, riveted, or bolted and secured by a rigid metal lock bar and an approved key operated or combination padlock. Supplemental protection is required during non-working hours only for Secret information that is stored in a closed area, a safe, a steel file cabinet, or a safe-type steel file container with automatic unit locking mechanism, or a 6-sided steel file cabinet with a rigid metal lock bar or an approved key operated or combination padlock. Supplemental protection is not required for storage of Secret information if it is stored in a GSA-approved security container.

c. Confidential Storage

Confidential information must be stored in any of the areas approved for Secret information. However, **s**upplemental protection is never required for storage of Confidential information.

2. 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. Change in Storage Capability

A report must be submitted after the initial acquisition of an approved storage container that raises or lowers the level of classification that a contractor is able to safeguard -- for example, when your facility acquires its first storage container for classified information. The report should be sent in the form of a letter to DSS.

b. Inability to Safeguard Classified Material

The next required report is 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. Upon your return, you would need to send an Inability to Safeguard Classified Material report to DSS via the fastest means possible, such as an email or a fax, with a follow-up letter, explaining what occurred.

c. Security Equipment Vulnerability

The last required report is when significant vulnerabilities are identified in security equipment used to protect classified information -- for example, if the locking mechanism on a security container fails. This report should also be sent to DSS via the fastest means possible with a follow-up letter.

Any time there is an inability to safeguard classified information or a vulnerability, 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.

3. End of Day Security Checks

The NISPOM requires end-of-day security checks to ensure that all classified information is protected and that the security container or area has been secured. Security checks must be conducted at the end of the last working shift, unless operations are conducted 24 hours per day. Although not required, records of security checks are a good security practice. Here is an example of a security container record that has columns to record the date and time a security container was opened, closed, and checked.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Which of the following are approved for storing Top Secret information (with supplemental controls)? Select all that apply.

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

Question 2

Select True or False for each statement.

	True	False
You should keep a written record of the combination to the lock of any container in which classified information is stored.	○	○
Storage of TOP SECRET information always requires supplemental protection or SID during non-working hours regardless of the type of security container used.	○	○
When supplemental protection is required, each facility must decide whether to use an intrusion detection system or security guards.	○	○
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.	○	○

Question 3

Which of the following are reasons for changing the combinations to the lock for a container used to store classified information? Select all that apply.

- ☐ 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

Question 4

In which of these cases would you need to make a report to the DSS Field Office? Select all that apply.

- ☐ 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 Conclusion

In this lesson, you learned about the requirements to safely store classified information, such as use of proper equipment and closed areas, locks, supplemental protection, and storage procedures.

Answer Key

Question 1

The marked items are approved for storing Top Secret information (with supplemental controls).

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

Question 2

	True	False
You should keep a written record of the combination to the lock of any container in which classified information is stored.	○	●
Storage of TOP SECRET information always requires supplemental protection or SID during non-working hours regardless of the type of security container used.	●	○
When supplemental protection is required, each facility must decide whether to use an intrusion detection system or security guards.	○	●
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.	●	○

Question 3

These are reasons for changing the combinations to the lock for a container used to store classified information.

- ☒ 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

Question 4

The marked items are the cases in which you would need to make a report to the 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.
- ☐ 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.

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Using Classified Information

Lesson Introduction

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

The lesson objectives are:

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

Handling Classified Information

1. Physical Handling

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, or 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.

2. Restricted Areas

When it is necessary to control access to classified information in an open area during working hours, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect classified information by simply covering it or turning it over because of its size, quantity, or other unusual characteristic. Although physical barriers are not required by the NISPOM, the restricted area must have clearly defined perimeters. Examples might be roped off areas, a

specially designated cubicle, or an office with a closed door. Authorized persons in the restricted area are responsible for protecting the classified information from unauthorized access. Once classified work is finished, classified material must be returned to the storage container for protection and the area becomes a regular work area once again.

3. Perimeter Controls

Entry and exit inspections are perimeter controls that deter and detect the introduction or removal of classified information from a facility without proper authority. Contractors who are authorized to store classified information are required to establish and maintain such perimeter controls. Signs must be posted conspicuously informing everyone that they are subject to inspection upon entry and exit. The extent, frequency, and location of inspections must be accomplished in a manner consistent with contractual obligations and operational efficiency, and they must be applied consistently. For example, inspections should occur in a set manner such as on every person, every other person, and so on. Contractors are encouraged to seek legal advice when formulating their inspection policies. These procedures are limited to buildings or areas where classified work is being performed.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

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.

4. 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.

5. 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 web-based training course offered by the DSS Academy.

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 can not 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.

1. 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, personal digital assistants, such as Blackberries, 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.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Select True or False for each statement.

An authorized person:	**True**	**False**
May lock classified information in his or her desk drawer while he or she goes down the hall to get a cup of coffee	○	○
May turn classified information over on his or her desk when an unauthorized person is present	○	○
Is responsible for safeguarding classified information in a restricted area	○	○
Must escort or control the activities of their classified visitor	○	○

Question 2

Where may classified information be discussed between authorized persons? Select all that apply.

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

Lesson Conclusion

In this lesson, you learned about the requirements for properly safeguarding classified information when it is being used and discussed.

Answer Key

Question 1

An authorized person:	True	False
May lock classified information in his or her desk drawer while he or she goes down the hall to get a cup of coffee	○	●
May turn classified information over on his or her desk when an unauthorized person is present	●	○
Is responsible for safeguarding classified information in a restricted area	●	○
Must escort or control the activities of their classified visitor	●	○

Question 2

Classified information may be discussed between authorized persons **in a restricted area** and **on secure telephones**.

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Reproducing Classified Information

Lesson Introduction

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

.

The lesson objectives are:

- Identify when a proposed reproduction requires prior authorization of the contracting officer or other government authority
- Identify when classified information may be reproduced without obtaining authorization
- Identify the security procedures for reproducing classified information

Authorizations

1. 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.

Procedures

1. 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.

a. 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).

2. Equipment Requirements

Most modern copy machines 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, or ISSP, to determine what approvals or accreditations are needed for a particular piece of equipment and what procedures need to be followed.

3. 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.

Here are some other best practices for reproducing classified information:

- The *location* of the equipment is important. Use only equipment that is located within a controlled area.
- Post the rules for using the designated equipment on or near the equipment so users know exactly what procedures to follow.

- 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.
- Ensure that the security markings on the original appear on all of the copies and has not been cut off.
- 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.
- Be aware of equipment vulnerabilities. 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.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

In which of these cases may classified information be reproduced without obtaining GCA authorization? Select all that apply.

☐ 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

Question 2

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

- ○ Permissible
- ○ Problematic

Lesson Conclusion

In this lesson, you learned about the authorization requirements for reproducing classified information as well as the copy and equipment requirements.

Answer Key

Question 1

The marked cases are those in which classified information may be reproduced without obtaining GCA authorization.

- ☒ 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

Question 2

You are along making classified copies and the machine jams. If you leave to go down the hall to as for help, this action is **problematic**. You cannot leave the classified material behind.

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Disposition of Classified Information

Lesson Introduction

Classified information that is no longer needed must be processed for appropriate disposition. Disposition is relevant during all stages of a contract. While contractors should dispose of material they no longer need throughout the contract period, special emphasis is placed on disposing of classified information at the contract's conclusion. The three modes of disposition are retaining, returning, and destroying classified information. In this lesson, you will learn about the requirements for making proper disposition of classified information.

The lesson objectives are:

- Identify the requirements for retaining classified information
- Identify the requirements for returning classified information to the Government Contracting Authority (GCA)
- Identify the requirements for destroying classified information

Retention

1. 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 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, you must request retention authority from the GCA in a certain format, depending on the level of classified material involved, and you must include a statement of justification.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

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

Disposition Schedule

1. 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

1. 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.

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

TOP SECRET destruction records:

- Can be combined with other control records
- Must be retained for 2 years

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

2. Methods

According to the NISPOM, the method of destruction must preclude recognition or reconstruction of the classified information. Classified information may be destroyed by various methods such as burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing. 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.

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.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 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. Select True or False for each statement.

	True	False
WW can request retention authority from the Navy.	○	○
If WW requests retention authority, they would need to do it within 180 days.	○	○
The Navy would need to issue a final DD Form 254 indicating the final retention period and final disposition instructions.	○	○
The Army would need to issue a final DD Form 254 or a letter indicating the final retention period and final disposition instructions.	○	○

Question 2

In which of the following cases must classified information be returned or destroyed? Select all that apply.

- ☐ 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

Question 3

Select True or False for each statement.

	True	False
Classified information in the form of regular paper may be burned.	○	○
Destruction of classified information must ensure the information cannot be recognized or reconstructed.	○	○
When destroying classified information through a shredder, shred size is not important.	○	○
Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL information.	○	○

Lesson Conclusion

In this lesson, you learned about the requirements for making proper disposition of classified information which includes retention of classified information, the disposition schedule for returning classified information to the GCA or destroying it, as well as the requirements and methods for the destruction of classified information.

.

Answer Key

Question 1

	True	False
WW can request retention authority from the Navy.	○	●
If WW requests retention authority, they would need to do it within 180 days.	○	●
The Navy would need to issue a final DD Form 254 indicating the final retention period and final disposition instructions.	○	●
The Army would need to issue a final DD Form 254 or a letter indicating the final retention period and final disposition instructions.	●	○

Question 2

In all of the marked cases, classified information must be returned or destroyed.

- ☒ 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

Question 3

	True	False
Classified information in the form of regular paper may be burned.	●	○
Destruction of classified information must ensure the information cannot be recognized or reconstructed.	●	○
When destroying classified information through a shredder, shred size is not important.	○	●
Two authorized personnel must be present for the destruction of SECRET and CONFIDENTIAL information.	○	●

Student Guide

Course: Safeguarding Classified Information in the NISP

Lesson: Safeguarding Challenge

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

1. Visitor's Desk

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

a. 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 material if necessary
- Refused if an authorized person is not available to receive the package

b. Package

Any time 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

c. Drawer in an 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

d. 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

2. Handling Classified Information

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

a. 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

b. 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
- PDAs

c. 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 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

d. Safe with an open 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

e. 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

f. Information Management System

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:
- 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)

g. 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

h. 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

3. Copy Room

Now look around this copy room. What elements have implications for safeguarding classified information?

a. 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

b. 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

c. Shredder

Be sure to destroy classified material appropriately! A shredder may be used for destroying paper products and water-repellant paper products. Cross-cut shredders must satisfy NISPOM 5-705.

Manner of destroying classified information:
- Must prevent recognition or reconstruction of information
- Residue must not contain any traces of classified information

d. SECRET document for reproduction

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

When making copies of classified information:
- Determine exact number of copies needed
- Consider how to minimize number of copies
- Allow only authorized personnel to make copies

e. 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.

What to destroy:
- Multiple copies
- Obsolete material
- Classified waste

How to destroy:
- Top Secret information requires two individuals
- Secret/Confidential information requires one individual

f. 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

Conclusion

Congratulations! You have completed the Safeguarding Challenge. Being aware of your surroundings and knowing the policies and procedures you need to apply will help you and your organization properly safeguard classified information.