SEC301: Module One

1. Module One

1.1 Opening Slide

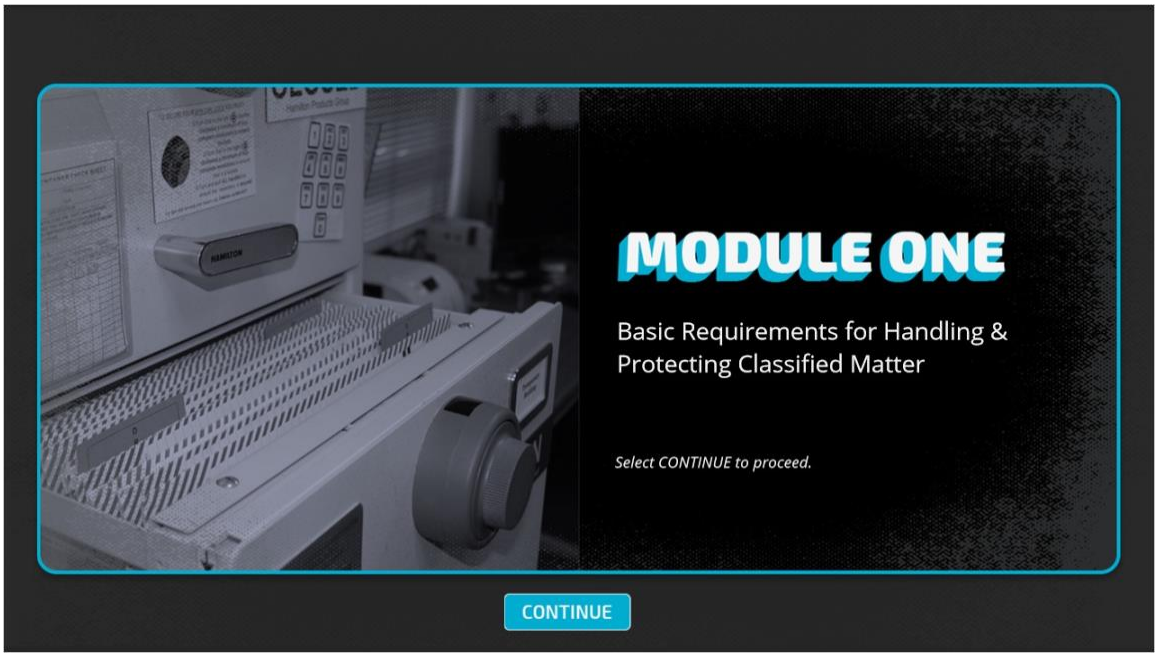


Notes:

SEC301, Classified Matter Training.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2026-26281O.

1.2 Module Introduction



Notes:

Module one: Basic Requirements for Handling & Protecting Classified Matter

Select continue to proceed.

1.3 How to use this course



Notes:

How to use this course.

Welcome to SEC301, Classified Matter Training. We've made changes to this course to better fit your training needs based on how much your position requires you to directly work with or support classified operations.

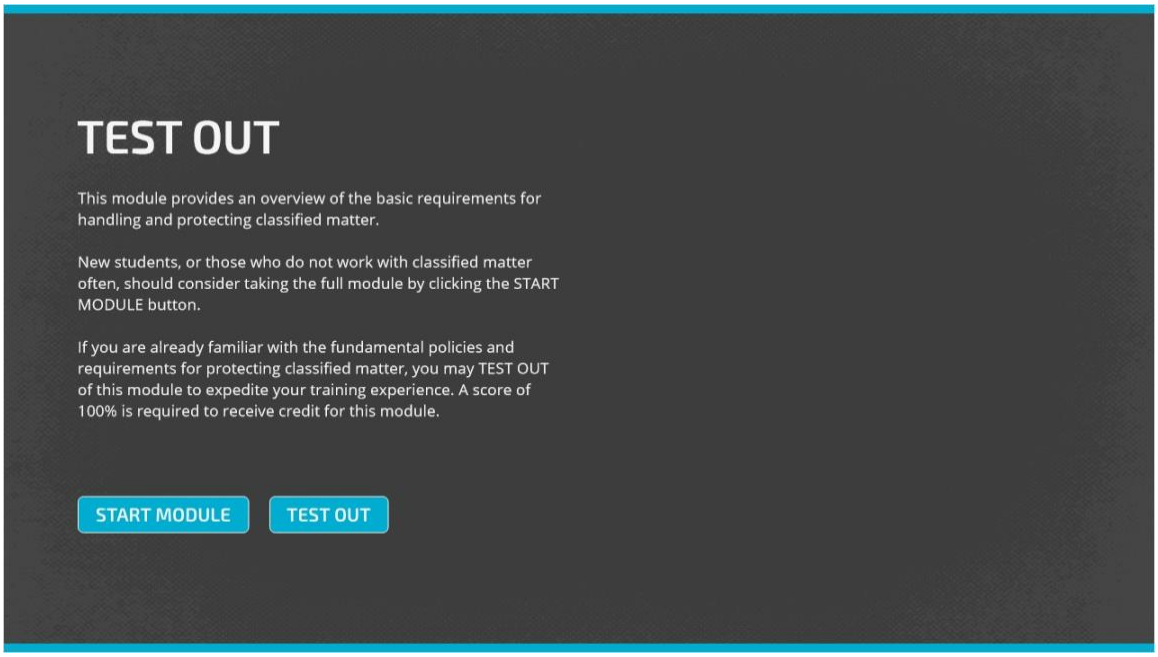
This course consists of several modules, each of which presents the policy and requirements related to classified matter during different stages of its lifecycle. To customize your training experience, we've included a survey question at the beginning of each module so that you can determine if the content is relevant to your position, as well as a test out option so that you can expedite your training, as needed.

As a reminder, the classified matter resources, available under the Resources tab, can be accessed at any time to provide additional information on each topic presented in this training.

We've included a glossary and links to course resources for every module. This is located in the upper right of the course player.

Use the forward and backward buttons to navigate from slide to slide.

1.4 Test Out Option



Notes:

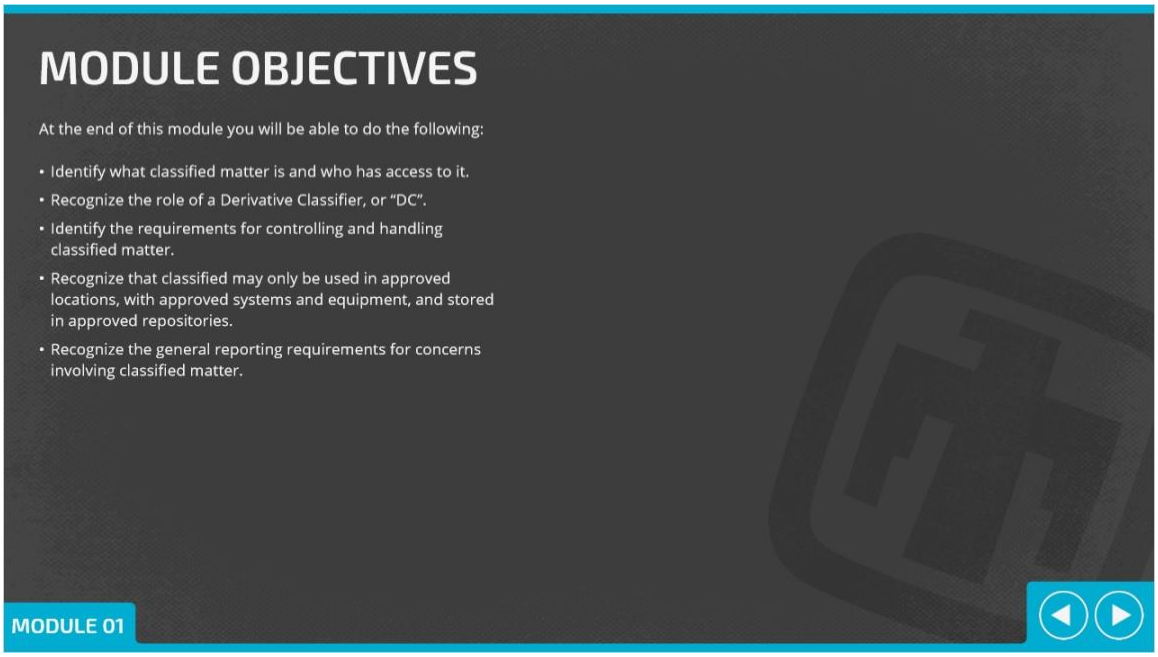
Test out

This module provides an overview of the basic requirements for handling and protecting classified matter.

New students, or those who do not work with classified matter often, should consider taking the full module by clicking the START MODULE button.

If you are already familiar with the fundamental policies and requirements for protecting classified matter, you may TEST OUT of this module to expedite your training experience. A score of 100% is required to receive credit for this module.

1.5 Objectives



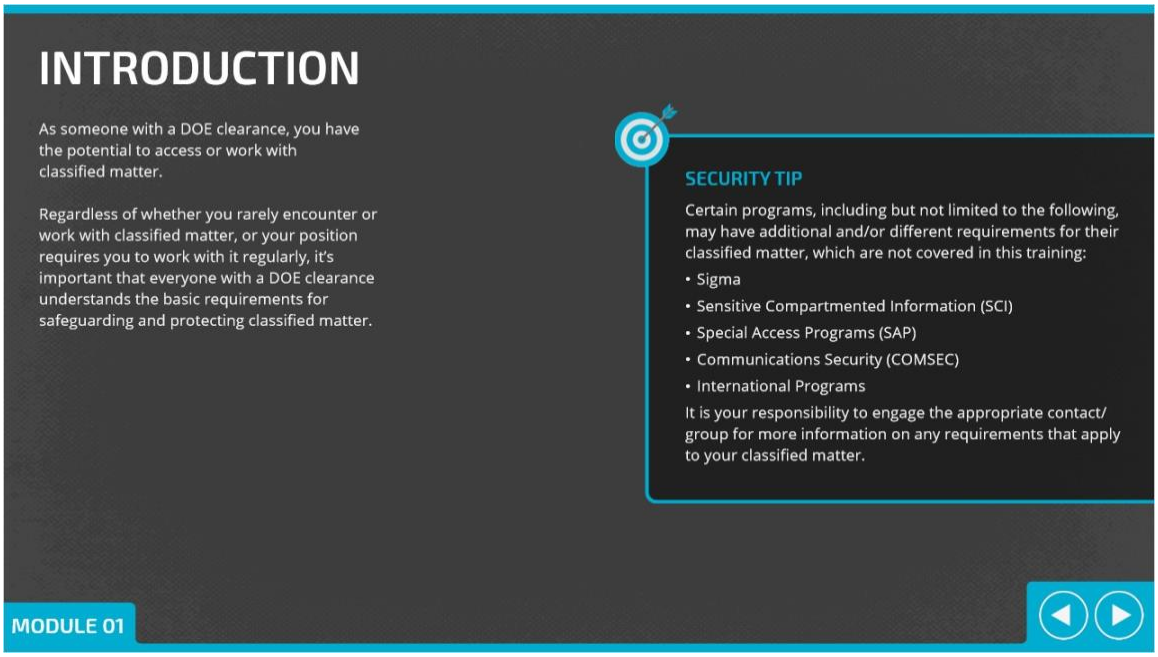
Notes:

Module objectives

At the end of this module you will be able to do the following:

- Identify what classified matter is and who has access to it.
- Recognize the role of a Derivative Classifier, or (DC).
- Identify the requirements for controlling and handling classified matter.
- Recognize that classified may only be used in approved locations, with approved systems and equipment, and stored in approved repositories.
- Recognize the general reporting requirements for concerns involving classified matter.

1.6 Introduction



Notes:

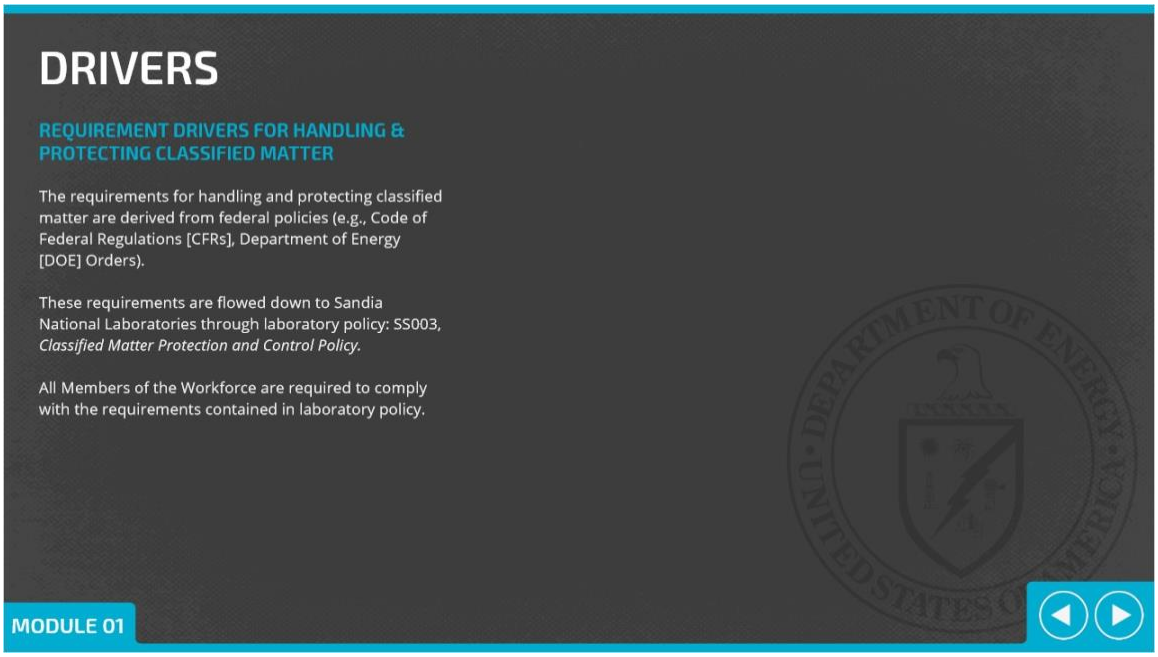
Introduction

As someone with a DOE clearance, you have the potential to access or work with classified matter.

Regardless of whether you rarely encounter or work with classified matter, or your position requires you to work with it regularly, it's important that everyone with a DOE clearance understands the basic requirements for safeguarding and protecting classified matter.

Certain programs, including but not limited to the following, may have additional and/or different requirements for their classified matter, which are not covered in this training:
· Sigma
· Sensitive Compartmented Information (SCI)
· Special Access Programs (SAP)
· Communications Security (COMSEC)
· International Programs
It is your responsibility to engage the appropriate contact/group for more information on any requirements that apply to your classified matter.

1.7 Drivers



Notes:

Drivers

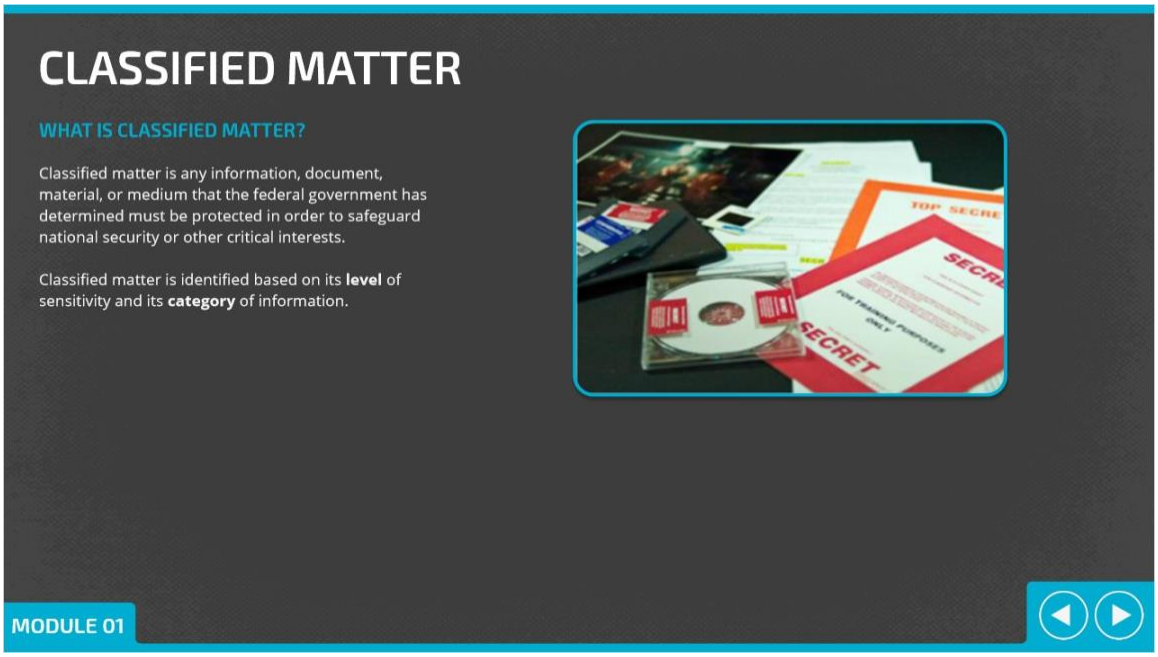
REQUIREMENT DRIVERS FOR HANDLING & PROTECTING CLASSIFIED MATTER

The requirements for handling and protecting classified matter are derived from federal policies (e.g., Code of Federal Regulations [CFRs], Department of Energy [DOE] Orders).

These requirements are flowed down to Sandia National Laboratories through laboratory policy: SS003, Classified Matter Protection and Control Policy.

All Members of the Workforce are required to comply with the requirements contained in laboratory policy.

1.8 Classified Matter

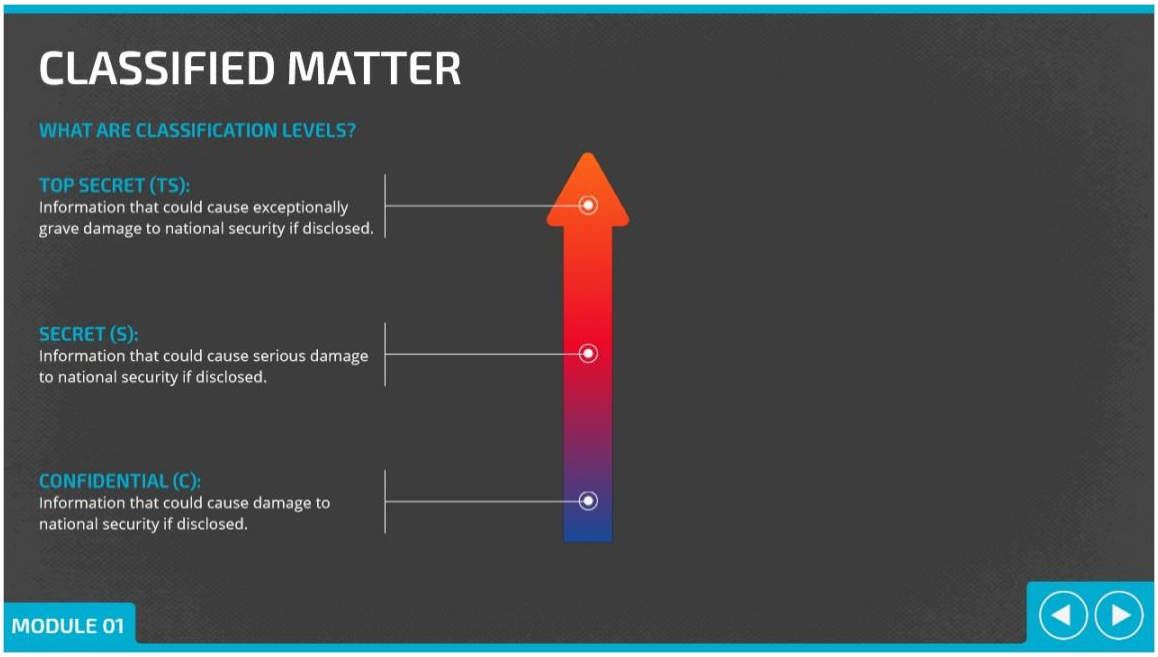


Notes:

Classified Matter

WHAT IS CLASSIFIED MATTER?
Classified matter is any information, document, material, or medium that the federal government has determined must be protected in order to safeguard national security or other critical interests. Classified matter is identified based on its level of sensitivity and its category of information.

1.9 Classified Matter



Notes:

Classified Matter

WHAT ARE CLASSIFICATION LEVELS?

TOP SECRET (TS):
Information that could cause exceptionally grave damage to national security if disclosed.

SECRET (S):
Information that could cause serious damage to national security if disclosed.

CONFIDENTIAL (C):
Information that could cause damage to national security if disclosed.

1.10 Classified Matter



Notes:

Classified Matter

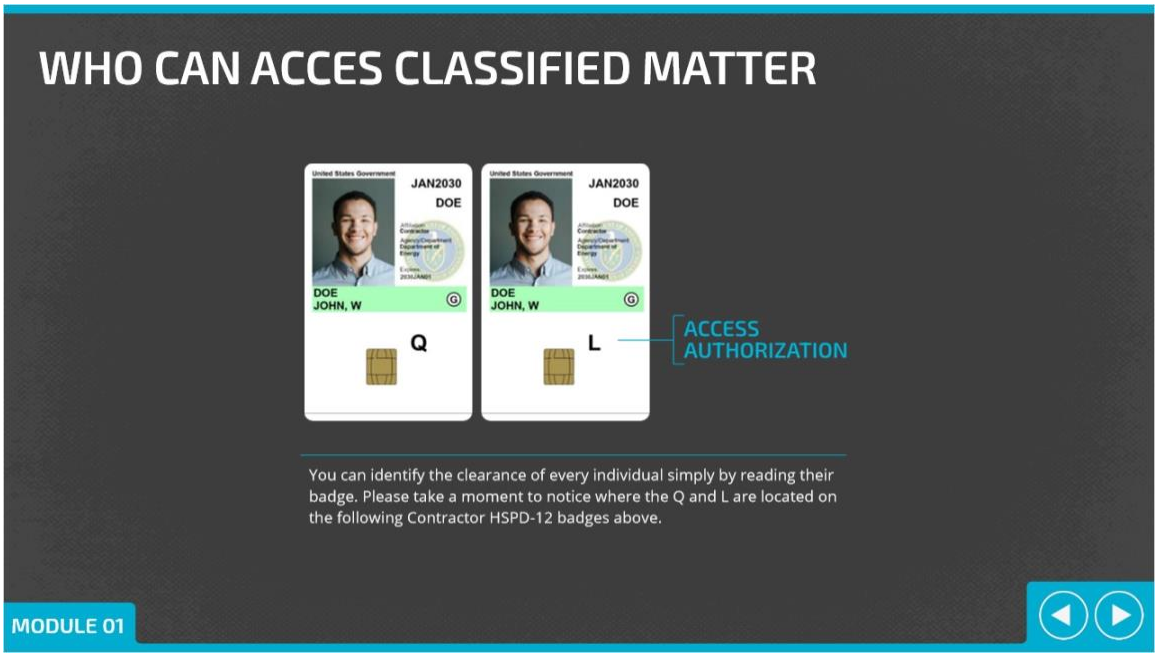
CLASSIFICATION CATEGORIES

RESTRICTED DATA (RD):
RD includes data related to the design, manufacture or utilization of atomic weapons as well as the production of special nuclear material (SNM) or the use of special nuclear material in production of energy.

FORMERLY RESTRICTED DATA (RD):
FRD is information that was removed from the RD category after the Department of Energy and Department of Defense jointly determined that the information related primarily to the military use of atomic weapons. The term "formerly" does not mean it is unclassified.

NATIONAL SECURITY INFORMATION (NSI):
NSI is information that is important to national security for reasons other than those in the RD and FRD categories. Examples of NSI include information related to military operations, foreign government information, intelligence-related activities, and economic or scientific information associated with national security.

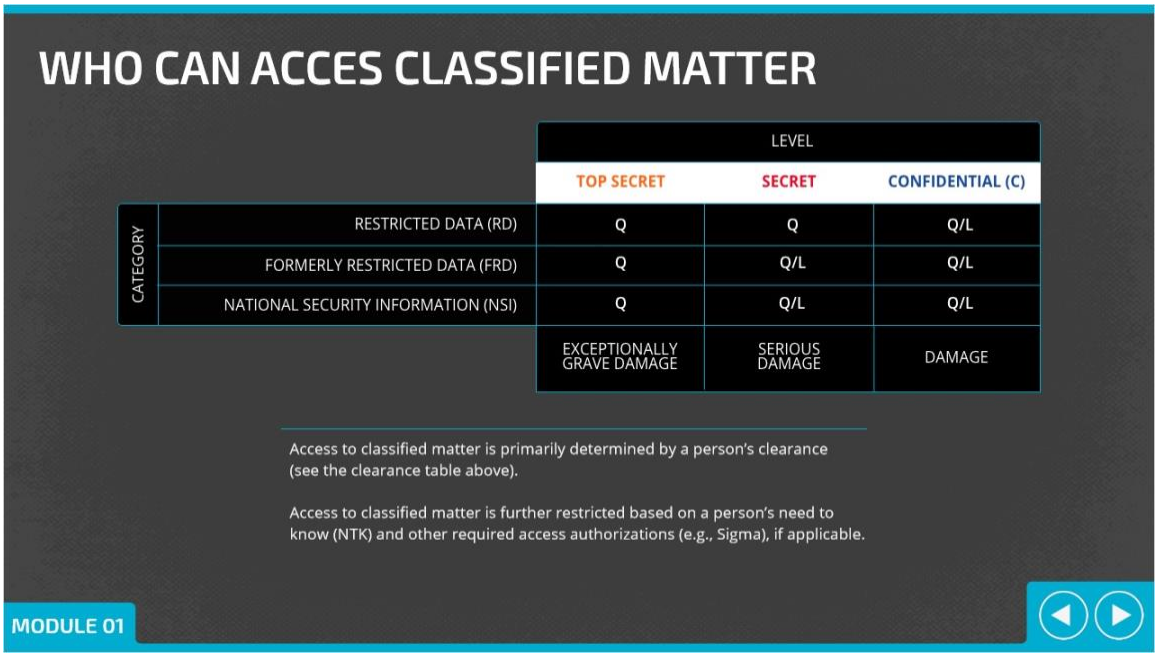
1.11 Classified Matter



Notes:

WHO CAN ACCESS CLASSIFIED MATTER?
You can identify the clearance of every individual simply by reading their badge. Please take a moment to notice where the Q and L are located on the following Contractor HSPD-12 badges above.

1.12 Classified Matter



Notes:

WHO CAN ACCESS CLASSIFIED MATTER?
Access to classified matter is primarily determined by a person's clearance (see the clearance table above).
Access to classified matter is further restricted based on a person's need to know (NTK) and other required access authorizations (e.g., Sigma), if applicable.

1.13 Classified Matter



Notes:

HOW IS CLASSIFIED MATTER IDENTIFIED?

Classified matter is identified by a Derivative Classifier (DC) who is authorized to determine the classification of an item.

Classified matter MUST also be marked to:
- Alert individuals to the presence of classified.
- Inform users how to control/protect that type of classified matter in accordance with SS003, Classified Matter Protection and Control (CMPC) Policy.

1.14 Protection Requirements



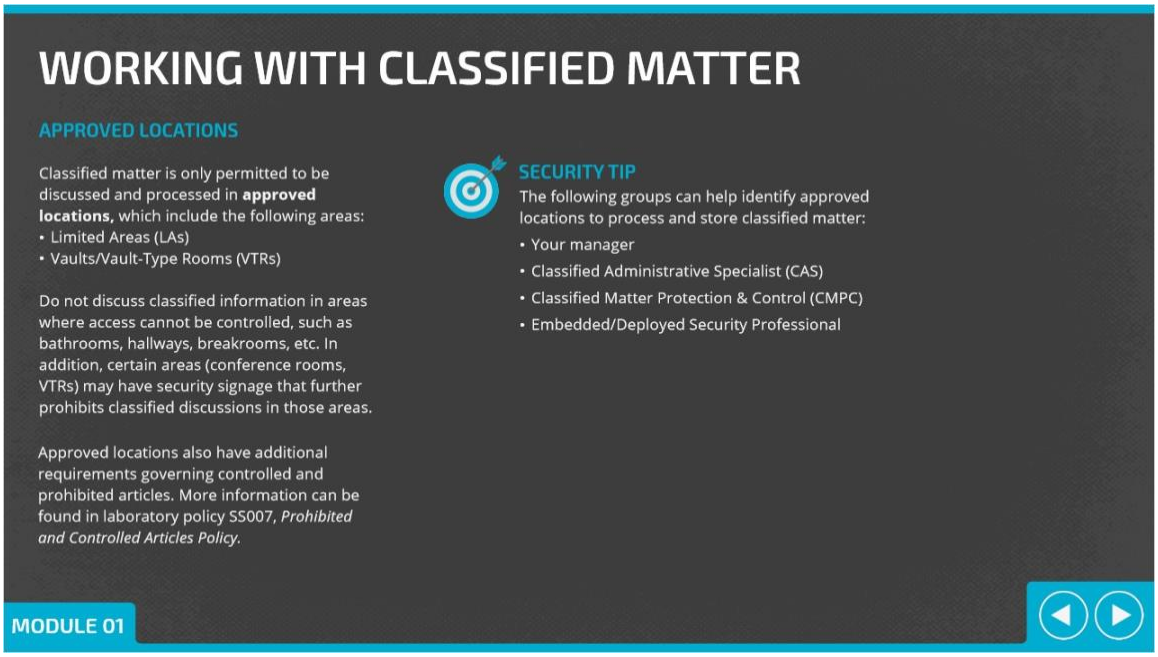
Notes:

REQUIREMENTS FOR PROTECTING CLASSIFIED MATTER
All classified matter must be under the direct control of an appropriately cleared individual when in use and removed from storage.

Classified matter must be protected from the following means of unauthorized access:
- Visual
- Aural
- Physical
- Cyber
- Other inadvertent access

Security Tip: Anyone with a security clearance is responsible for ensuring classified matter is appropriately safeguarded and reporting situations where classified is not protected or stored properly.

1.15 Working with Classified Matter



Notes:

APPROVED LOCATIONS
Classified matter is only permitted to be discussed and processed in approved locations which include the following areas:
- Limited Areas (LAs)
- Vaults/Vault-Type Rooms (VTRs)

Do not discuss classified information in areas where access cannot be controlled, such as bathrooms, hallways, breakrooms, etc. In addition, certain areas (conference rooms, VTRs) may have security signage that further prohibits classified discussions in those areas.

Approved locations also have additional requirements governing controlled and prohibited articles. More information can be found in laboratory policy SS007, Prohibited
and Controlled Articles Policy.

Security Tip: The following groups can help identify approved locations to process and store classified matter:
- Your manager
- Classified Administrative Specialist (CAS)
- Classified Matter Protection & Control (CMPC)
- Embedded/Deployed Security Professional

1.16 Working with Classified Matter



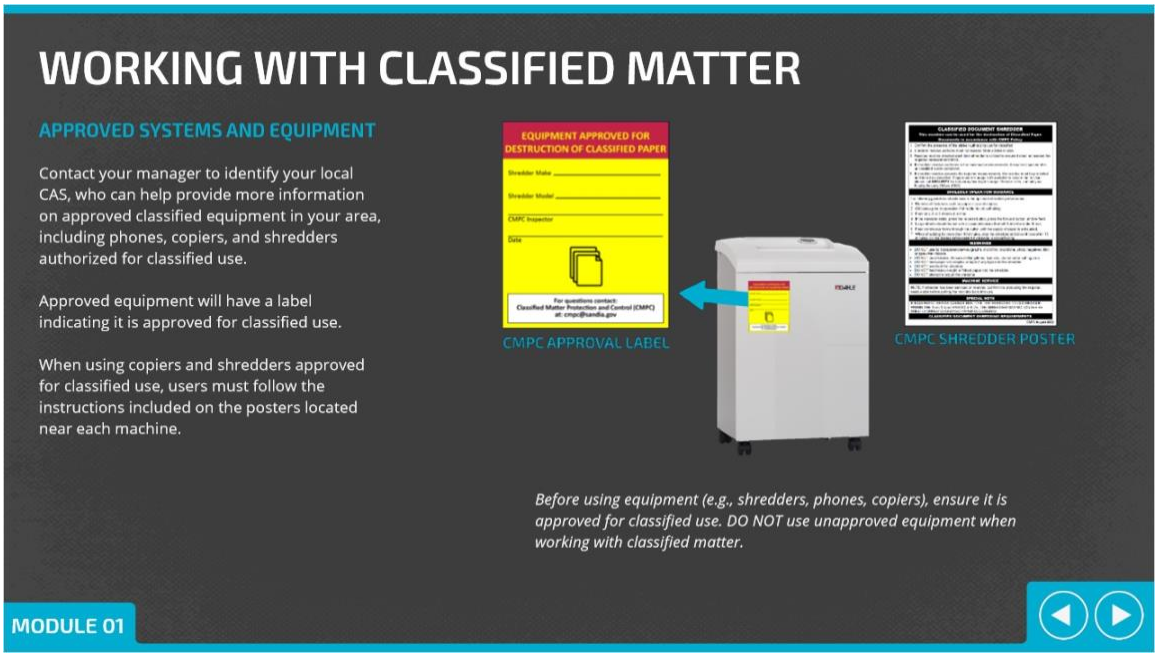
Notes:

APPROVED SYSTEMS AND EQUIPMENT
Classified information must only be processed on computing systems and equipment that have been approved for classified use.

Contact your Cyber Liaison, Corporate Computing Help Desk (CCHD), or Classified Computing Continual Service Improvement (3CSI) for more information on approved classified computing networks/systems.

Reminder: The term "system high" refers to the highest classification level and category a computing system is authorized to process. "System high" for Sandia's Classified Network (SCN) is Secret/Restricted Data (SRD).

1.17 Working with Classified Matter



Notes:

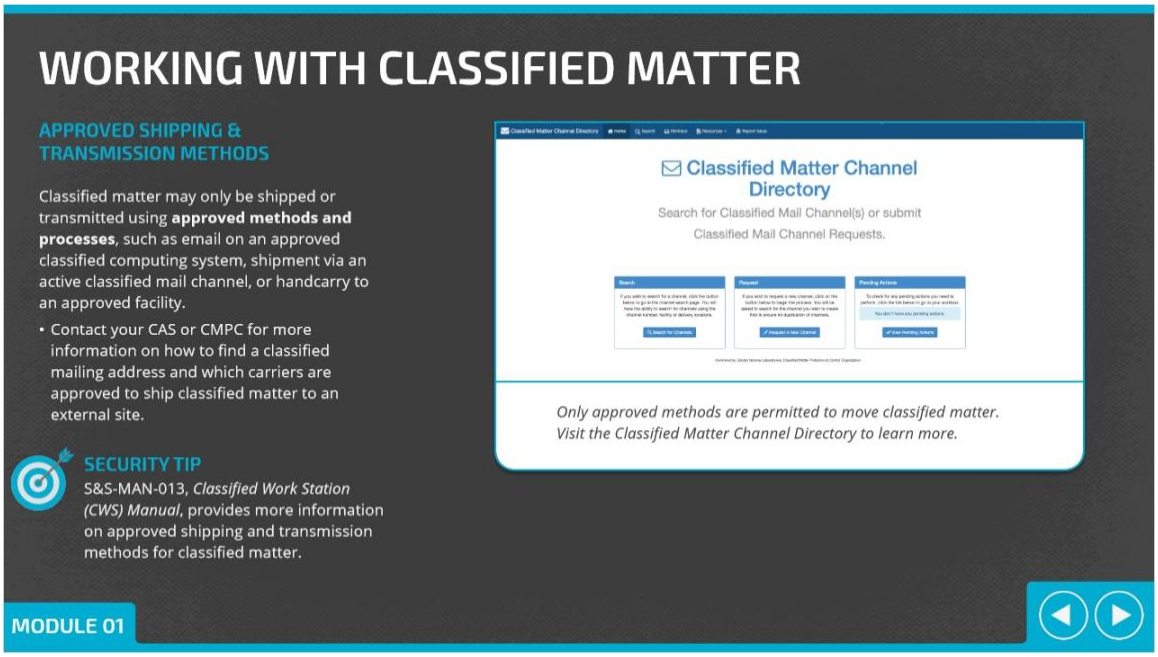
APPROVED SYSTEMS AND EQUIPMENT
Contact your manager to identify your local CAS, who can help provide more information on approved classified equipment in your area, including phones, copiers, and shredders authorized for classified use.

Approved equipment will have a label indicating it is approved for classified use.

When using copiers and shredders approved for classified use, users must follow the instructions included on the posters located near each machine.

Before using equipment (e.g., shredders, phones, copiers), ensure it is approved for classified use. DO NOT use unapproved equipment when working with classified matter.

1.18 Working with Classified Matter



Notes:

APPROVED SHIPPING & TRANSMISSION METHODS

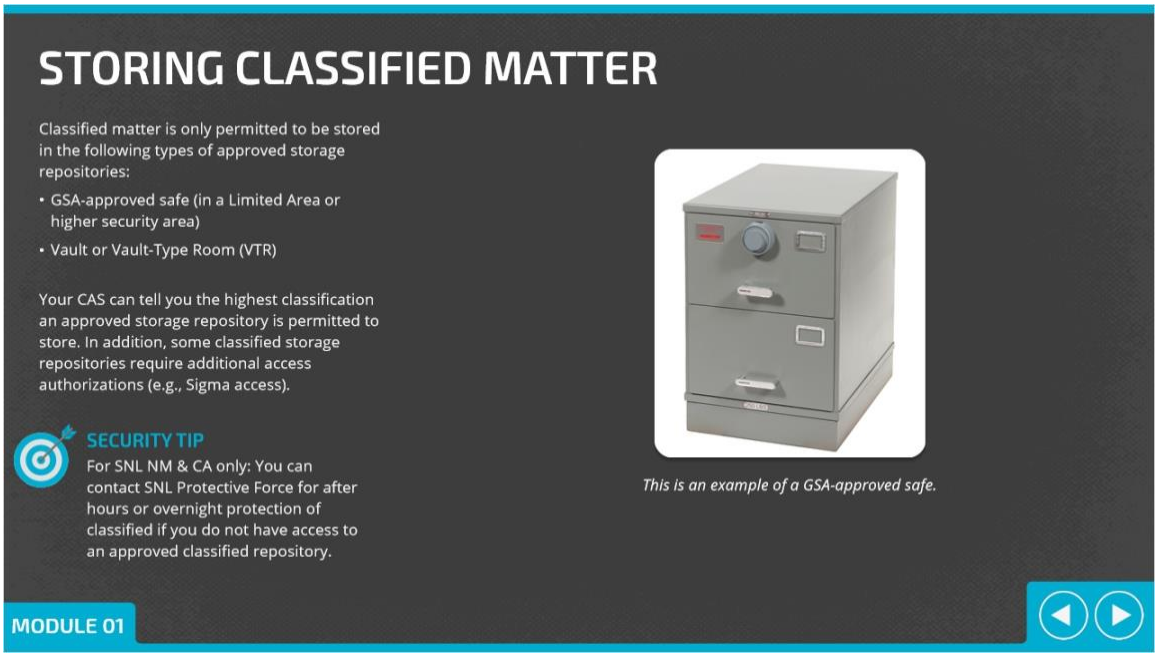
Classified matter may only be shipped or transmitted using approved methods and processes, such as email on an approved classified computing system, shipment via an active classified mail channel, or handcarry to an approved facility.

Contact your CAS or CMPC for more information on how to find a classified mailing address and which carriers are approved to ship classified matter to an external site.

SECURITY TIP:
S&S-MAN-013, Classified Work Station (CWS) Manual, provides more information on approved shipping and transmission methods for classified matter.

Only approved methods are permitted to move classified matter. Visit the Classified Matter Channel Directory to learn more.

1.19 Working with Classified Matter



Notes:

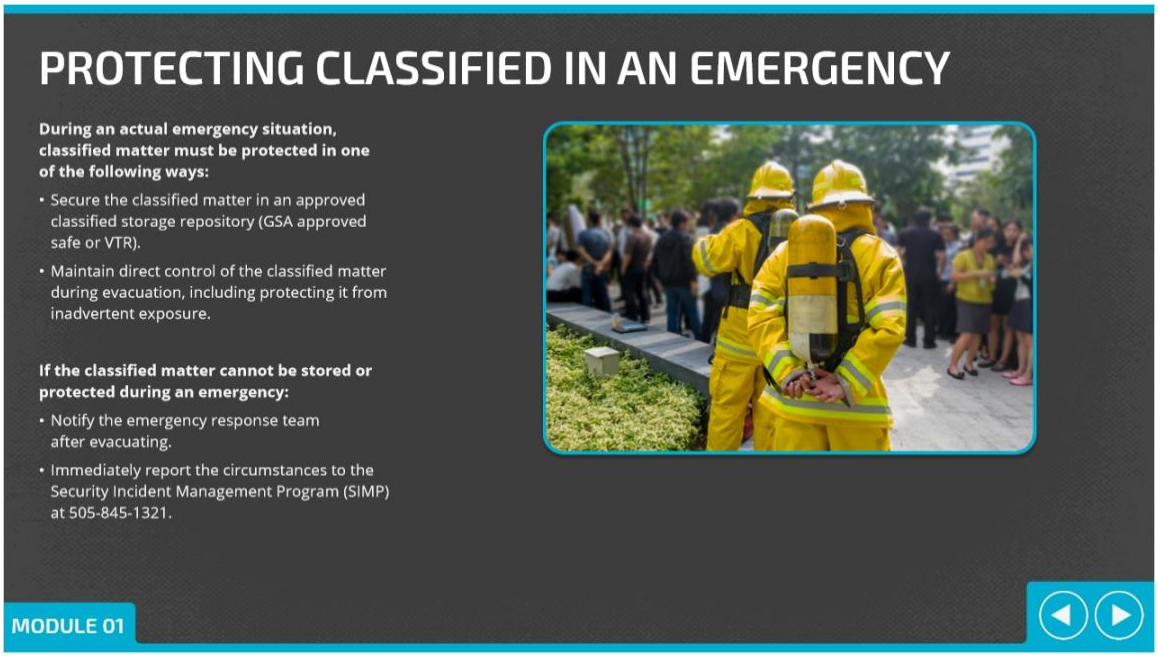
REQUIREMENTS FOR STORING CLASSIFIED MATTER
Classified matter is only permitted to be stored in the following types of approved storage repositories:

- GSA-approved safe (in a Limited Area or higher security area)
- Vault or VTR

Note: Your CAS can tell you the highest classification an approved storage repository is permitted to store. In addition, some classified storage repositories require additional access authorizations (e.g., Sigma access).

For SNL NM & CA only: You can contact SNL Protective Force for after hours or overnight protection of classified if you do not have access to an approved classified repository.

1.20 Handling Classified Matter in an Emergency



Notes:

Protecting classified matter in an emergency.

If an emergency is life threatening, the health and safety of personnel takes precedence over the need to secure classified matter.

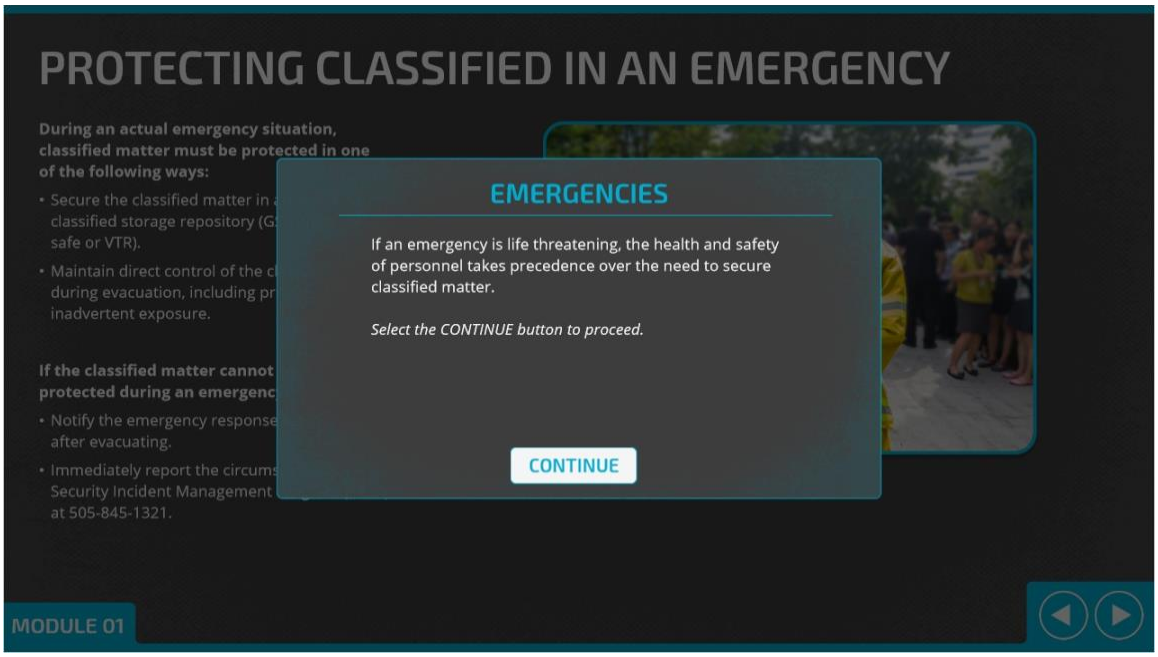
During an actual emergency situation, classified matter must be protected in one of the following ways:

- Secure the classified matter in an approved classified storage repository (GSA approved safe or VTR).
- Maintain direct control of the classified matter during evacuation, including protecting it from inadvertent exposure.

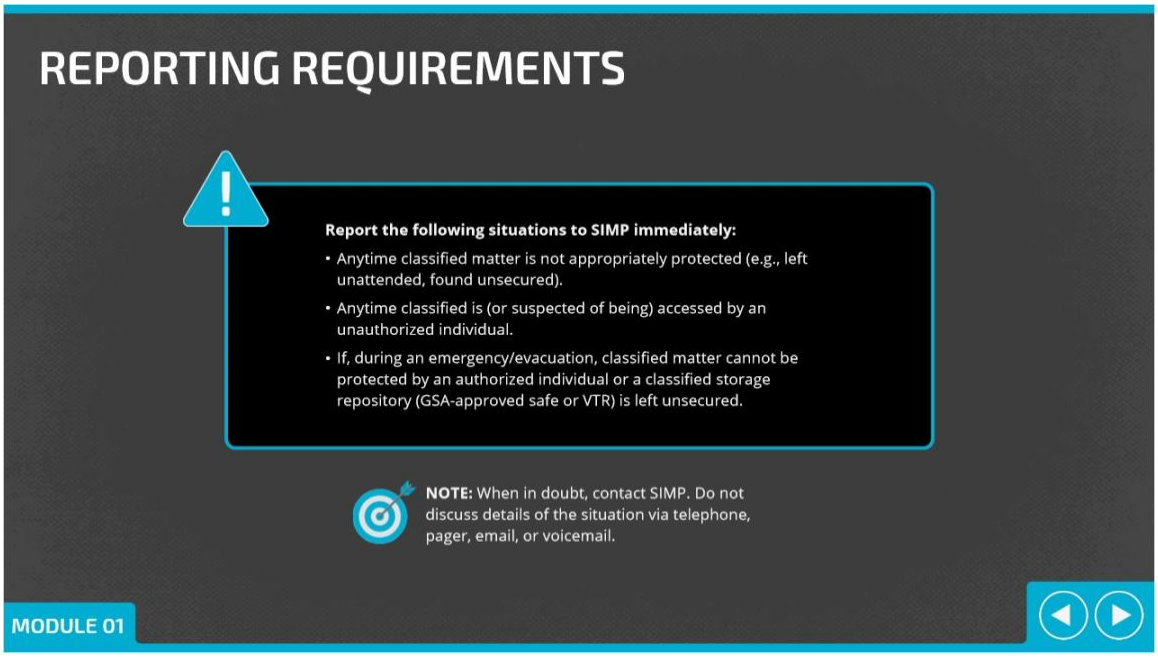
If the classified matter cannot be stored or protected during an emergency:

- Notify the emergency response team after evacuating.
- Immediately report the circumstances to the Security Incident Management Program (SIMP) at 505-845-1321.

EMERGENCIES (Slide Layer)



1.21 Reporting Requirements



Notes:

Reporting Requirements

Report the following situations to SIMP immediately:
- Anytime classified matter is not appropriately protected (e.g., left unattended, found unsecured).
- Anytime classified is (or suspected of being) accessed by an unauthorized individual.
- If, during an emergency/evacuation, classified matter cannot be protected by an authorized individual or a classified storage repository (GSA-approved safe or VTR) is left unsecured.

NOTE: When in doubt, contact SIMP. Do not discuss details of the situation via telephone, pager, email, or voicemail.

1.22 Key Takeaways



Notes:

Final Takeaways

Everyone with a security clearance has an obligation to ensure classified matter is appropriately safeguarded and protected.

When working with classified matter, always protect it from unauthorized physical, visual, aural, cyber, and other inadvertent access.

Classified matter may only be processed and stored in approved locations at SNL (Limited Area or higher security area).

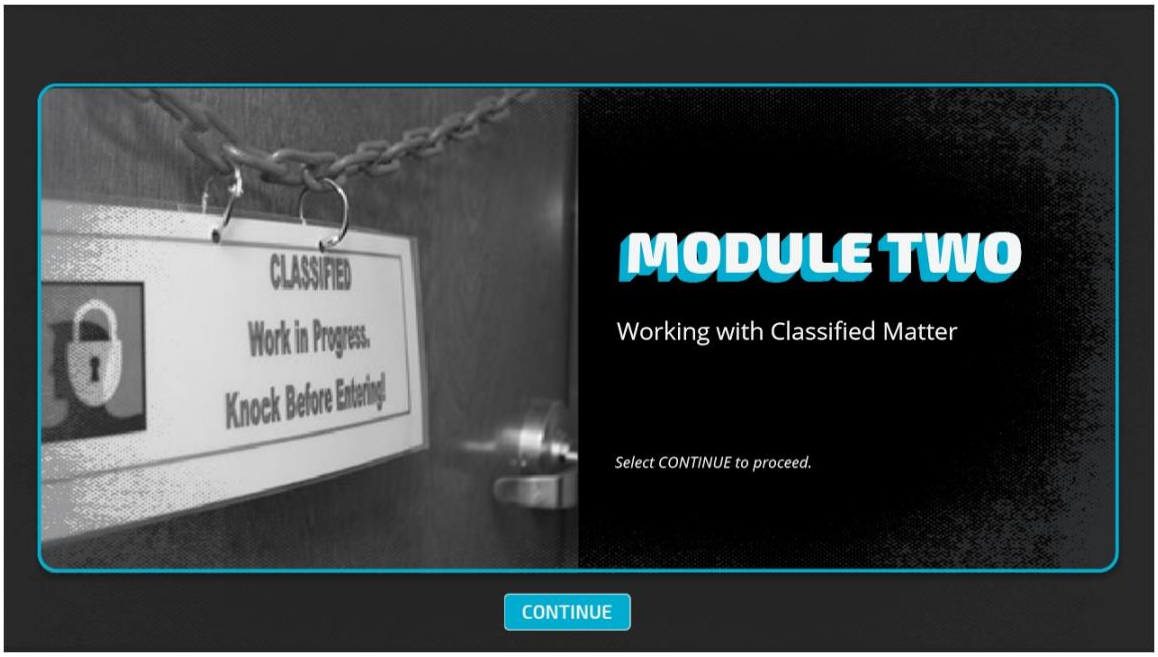
Only approved computing systems, equipment, and processes are authorized for classified use.

If you have additional questions about classified matter, talk to your manager or contact Security Connection at 321 (505-845-1321).

SEC301: Module Two

1. Module Two

1.1 Module Introduction

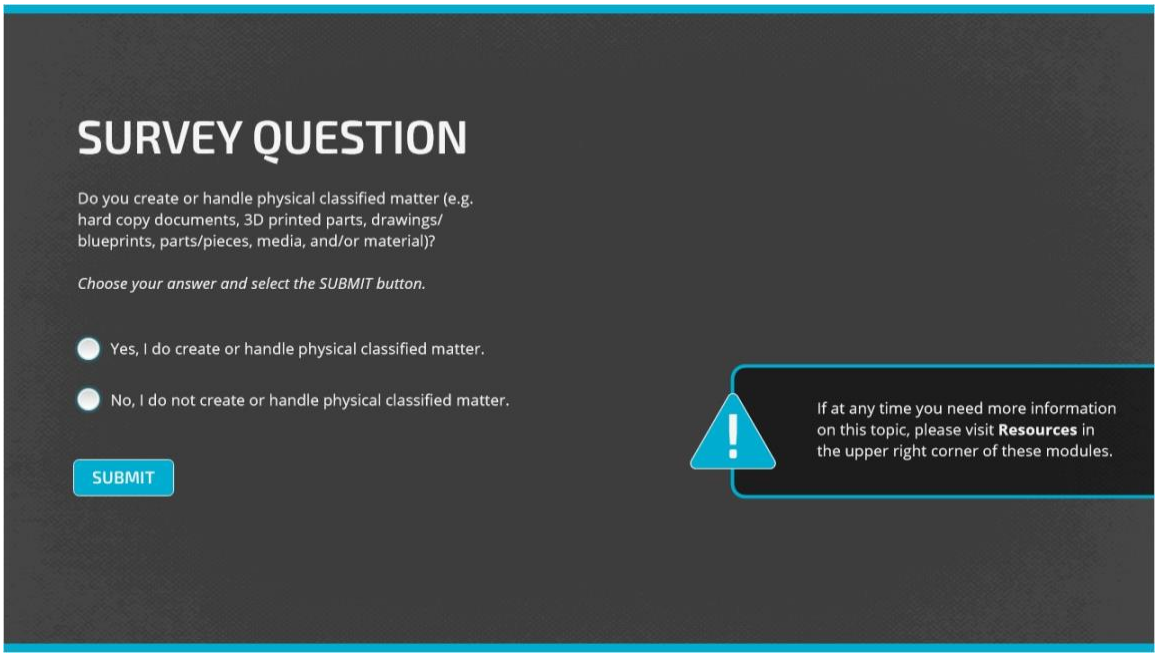


Notes:

MODULE TWO

Working with Classified Matter

1.2 Survey



Notes:

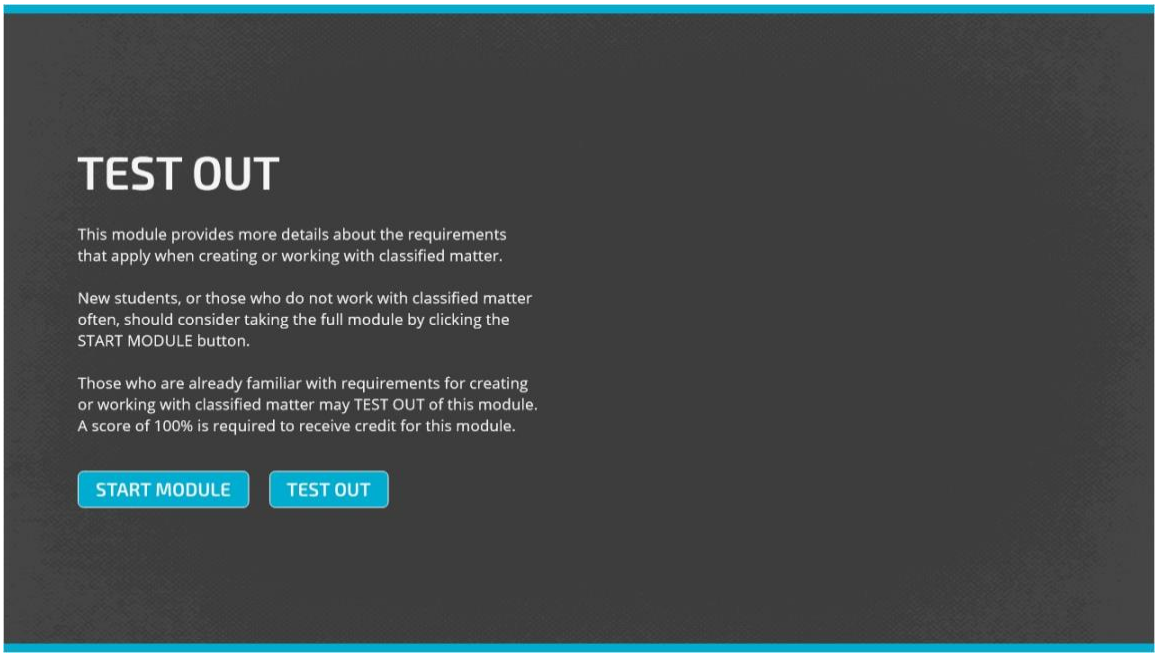
SURVEY QUESTION

Do you create or handle physical classified matter (e.g. hard copy documents, 3D printed parts, drawings/blueprints, parts/pieces, media, and/or material)?

Choose your answer and select the SUBMIT button.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option



Notes:

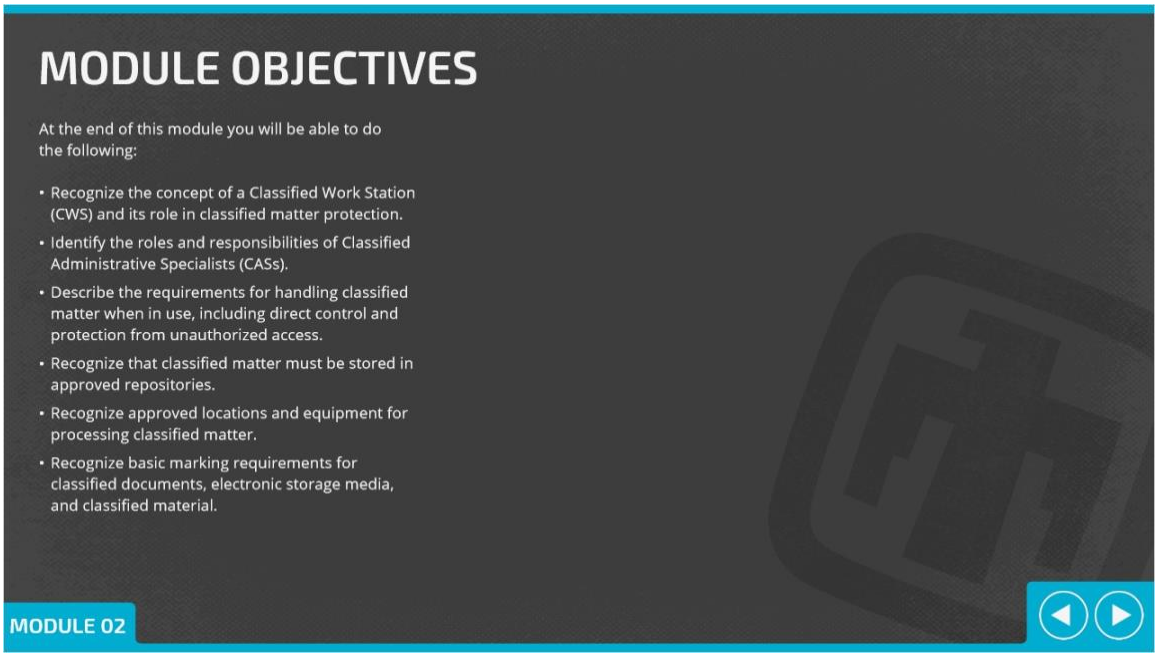
TEST OUT

This module provides more details about the requirements that apply when creating or working with classified matter.

New students, or those who do not work with classified matter often, should consider taking the full module by clicking the START MODULE button.

Those who are already familiar with requirements for creating or working with classified matter may TEST OUT of this module. A score of 100% is required to receive credit for this module.

1.4 Objectives



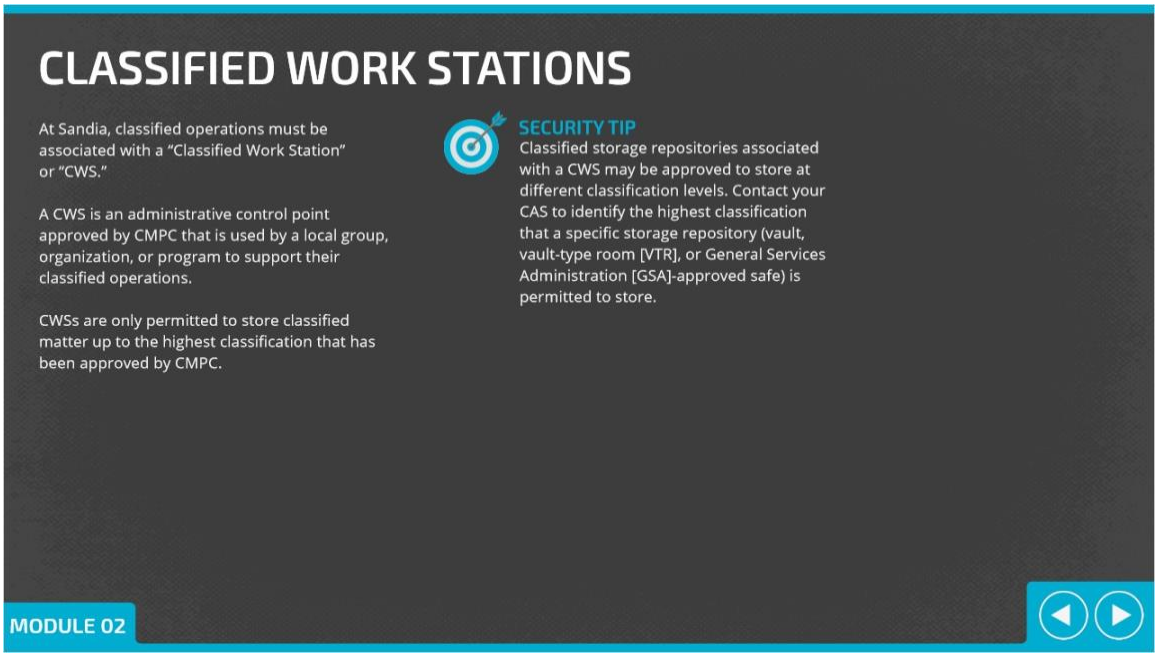
Notes:

Module Objectives

At the end of this module you will be able to do the following:

- Recognize the concept of a Classified Work Station (CWS) and its role in classified matter protection.
- Identify the roles and responsibilities of Classified Administrative Specialists (CASs).
- Describe the requirements for handling classified matter when in use, including direct control and protection from unauthorized access.
- Recognize that classified matter must be stored in approved repositories.
- Recognize approved locations and equipment for processing classified matter.
- Recognize basic marking requirements for classified documents, electronic storage media, and classified material.

1.5 Classified Work Stations



Notes:

CLASSIFIED WORK STATIONS

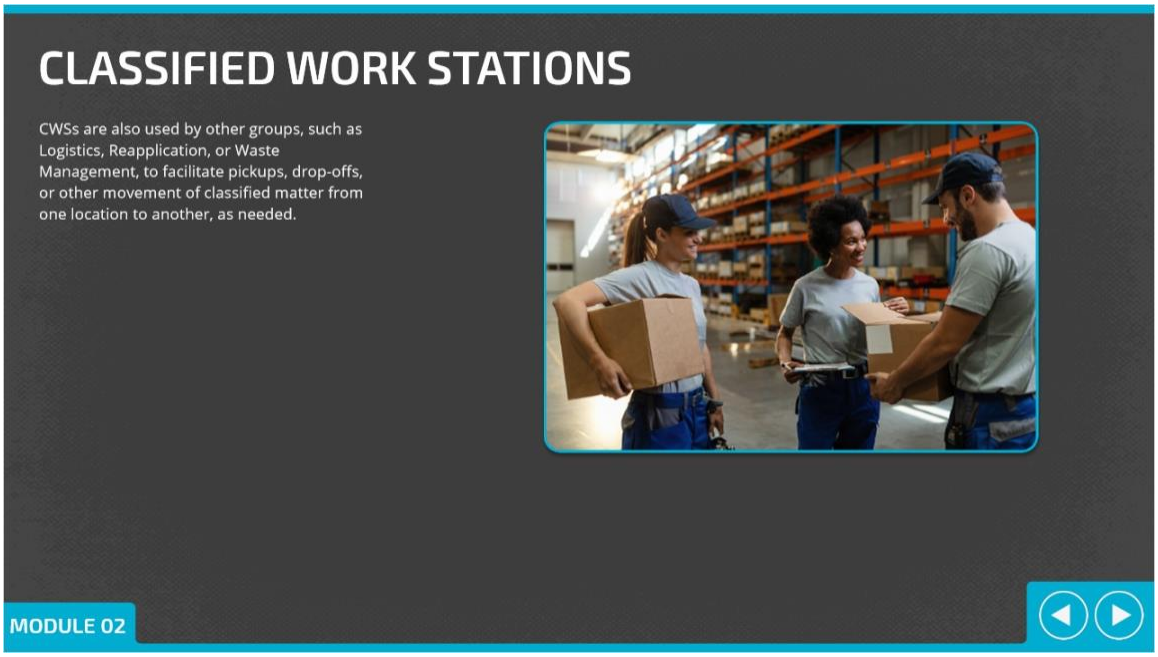
At Sandia, classified operations must be associated with a "Classified Work Station" or "CWS."

A CWS is an administrative control point approved by CMPC that is used by a local group, organization, or program to support their classified operations.

CWSs are only permitted to store classified matter up to the highest classification that has been approved by CMPC.

Security Tip: Classified storage repositories associated with a CWS may be approved to store at different classification levels. Contact your CAS to identify the highest classification that a specific storage repository (vault, vault-type room [VTR], or General Services Administration [GSA]-approved safe) is permitted to store.

1.6 Classified Work Stations



Notes:

CLASSIFIED WORK STATIONS

CWSs are also used by other groups, such as Logistics, Reapplication, or Waste Management, to facilitate pickups, drop-offs, or other movement of classified matter from one location to another, as needed.

1.7 Classified Administrative Specialist



Notes:

Classified Administrative Specialist

All CWSs are managed by a CWS Manager, a Primary Classified Administrative Specialist (CAS), and at least one Alternate CAS. CASs serve as local POCs and liaisons for their CWS's operations.

CASs are responsible for managing their CWS's approved storage repositories and authorized equipment for classified use.

CASs can also assist CWS users with marking, storing, moving, and destroying classified matter.

1.8 Classified Administrative Specialist



Notes:

Classified Administrative Specialist

Your CAS can tell you more about your CWS's classified storage locations, the highest classification your CWS is authorized to store, and any local equipment approved for classified use.

CMPC's CWS Authorization List provides a list of all CASs at each SNL site. The list can be searched by organization or location. If you are unsure who your CAS is, talk to your manager or use the CWS Authorization List to find a local CAS.

1.9 Classified Matter in Use



Notes:

Classified Matter in Use

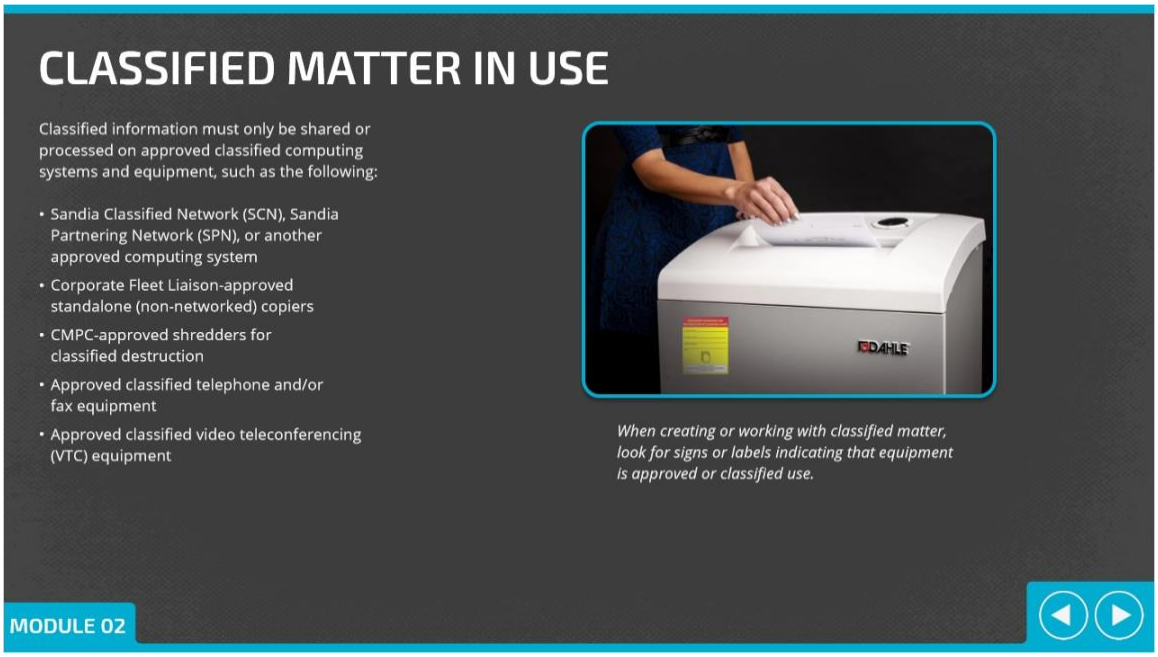
Classified matter is either in use or in storage.
When Classified Matter is in use:

Classified must be under the direct control of an appropriately cleared individual and be protected at the appropriate classification to prevent unauthorized physical, visual, aural, cyber, or other access.

Classified matter must only be used for official business purposes. Individuals are prohibited from taking classified matter to non-official business locations (e.g., offsite for lunch, personal appointments).

Any classified information that will be shared outside of Sandia or an ad-hoc working group must first be submitted through Sandia's Information Release (IR) process.

1.10 Classified Matter in Use



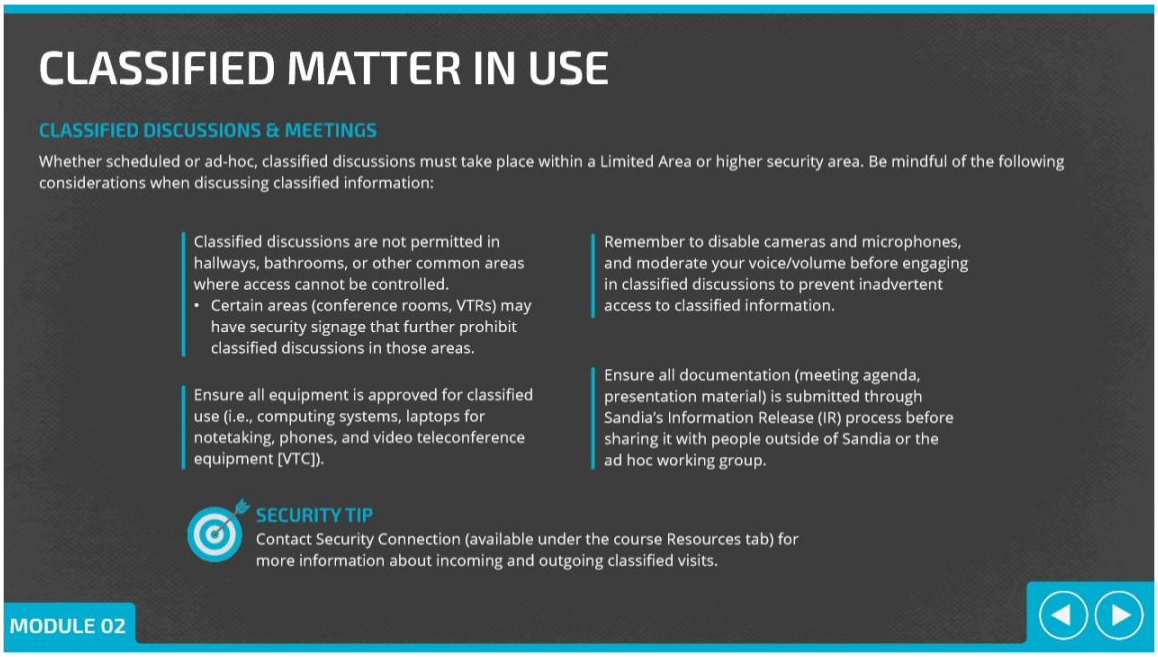
Notes:

Classified Matter in Use

Classified information must only be shared or processed on approved classified computing systems and equipment, such as the following:
Sandia Classified Network (SCN), Sandia Partnering Network (SPN), or another approved computing system
Corporate Fleet Liaison-approved standalone (non-networked) copiers
CMPC-approved shredders for classified destruction
Approved classified telephone and/or fax equipment
Approved classified video teleconferencing (VTC) equipment

When creating or working with classified matter, look for signs or labels indicating that equipment is approved or classified use.

1.11 Classified Matter in Use



Notes:

Classified Discussions and Meetings:
Whether scheduled or ad-hoc, classified discussions must take place within a Limited Area or higher security area. Be mindful of the following considerations when discussing classified information:

Classified discussions are not permitted in hallways, bathrooms, or other common areas where access cannot be controlled.
- Certain areas (conference rooms, VTRs) may have security signage that further prohibit classified discussions in those areas.

Ensure all equipment is approved for classified use (i.e., computing systems, laptops for notetaking, phones, and video teleconference equipment [VTC]).

Remember to disable cameras and microphones, and moderate your voice/volume before engaging in classified discussions to prevent inadvertent access to classified information.

Ensure all documentation (meeting agenda, presentation material) is submitted through Sandia's Information Release (IR) process before sharing it with people outside of Sandia or the ad hoc working group.

SECURITY TIP: Contact Security Connection (available under the course Resources tab) for more information about incoming and outgoing classified visits.

1.12 Classified Matter in Use



Notes:

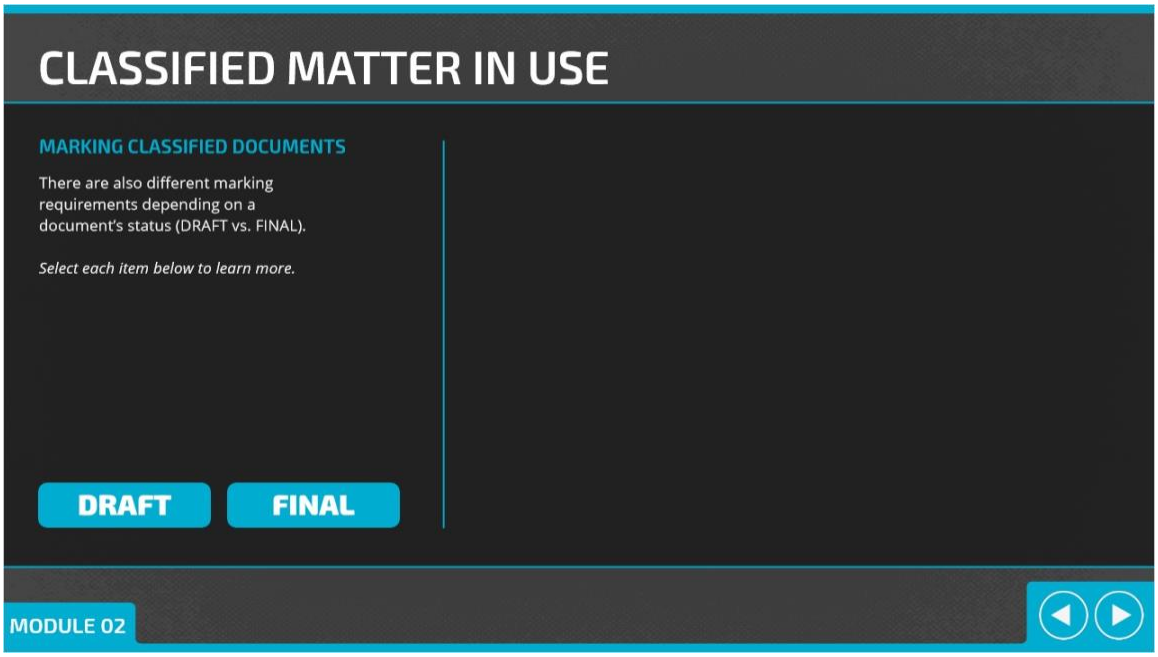
Classified Matter in Use

MARKING CLASSIFIED DOCUMENTS
Classified matter must be marked to alert individuals to its sensitivity and ensure the appropriate level of protection.
There are different requirements for marking classified documents, depending on the category of information it contains (NSI vs. RD/FRD).
National Security Information (NSI) documents are required to be portion marked, while Restricted Data/Formerly Restricted Data (RD/FRD) documents are not.

When removed from storage, all classified documents must have the appropriate cover and backing sheet that matches the classification of the document.

Document originators are responsible for marking their classified documents to ensure proper handling, protection, and storage.

1.13 Classified Matter in Use



Notes:

Classified Matter in Use

MARKING CLASSIFIED DOCUMENTS
There are also different marking requirements depending on a document's status (DRAFT vs. FINAL).

Select each item below to learn more.

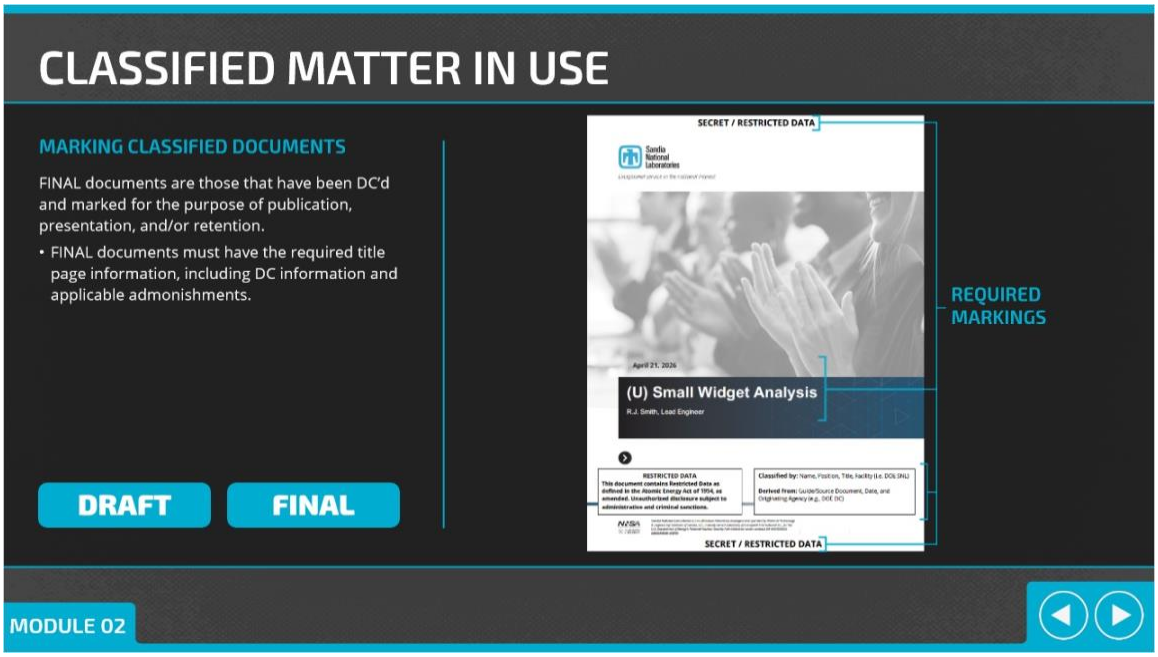
- DRAFT documents include living/working documents (e.g., meeting, conference, or handwritten notes) and anything else that has not been reviewed by an authorized Derivative Classifier (DC).
  DRAFT documents are required to have a title page with specific information (e.g., "Draft/Working Paper" annotation, highest potential classification marked on the top and bottom).
  DRAFT documents must include dated entries and be finalized (DC'd and re-marked) within 180 days from their creation or last update.

- FINAL documents are those that have been DC'd and marked for the purpose of publication, presentation, and/or retention.
  FINAL documents must have the required title page information, including DC information and applicable admonishments.

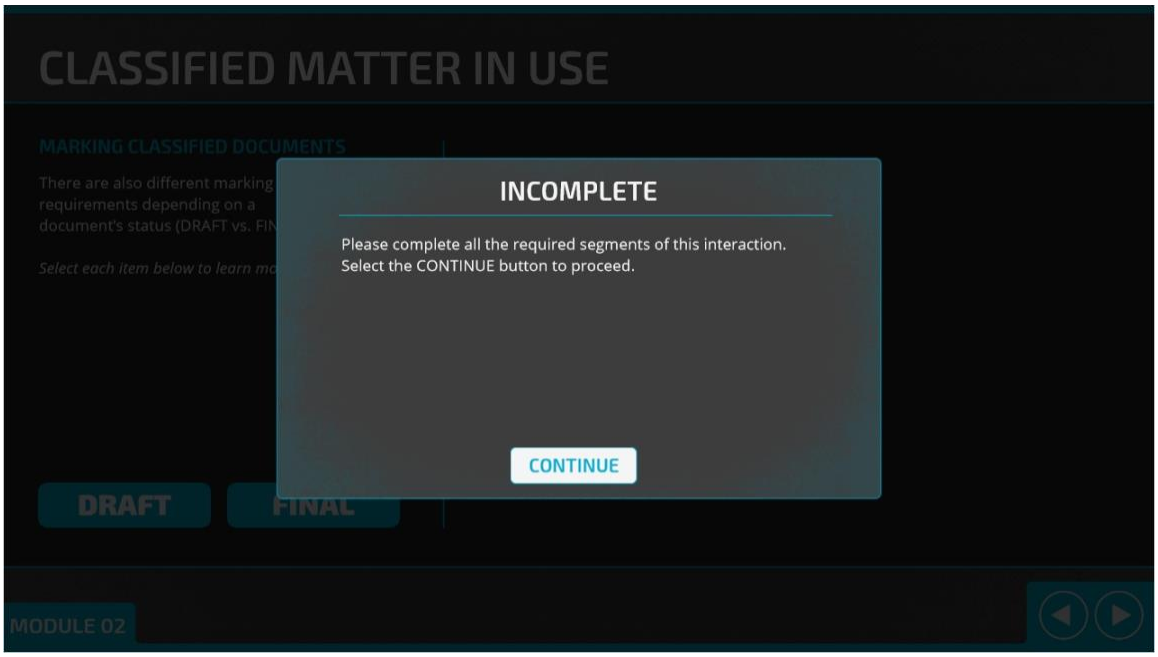
Draft (Slide Layer)



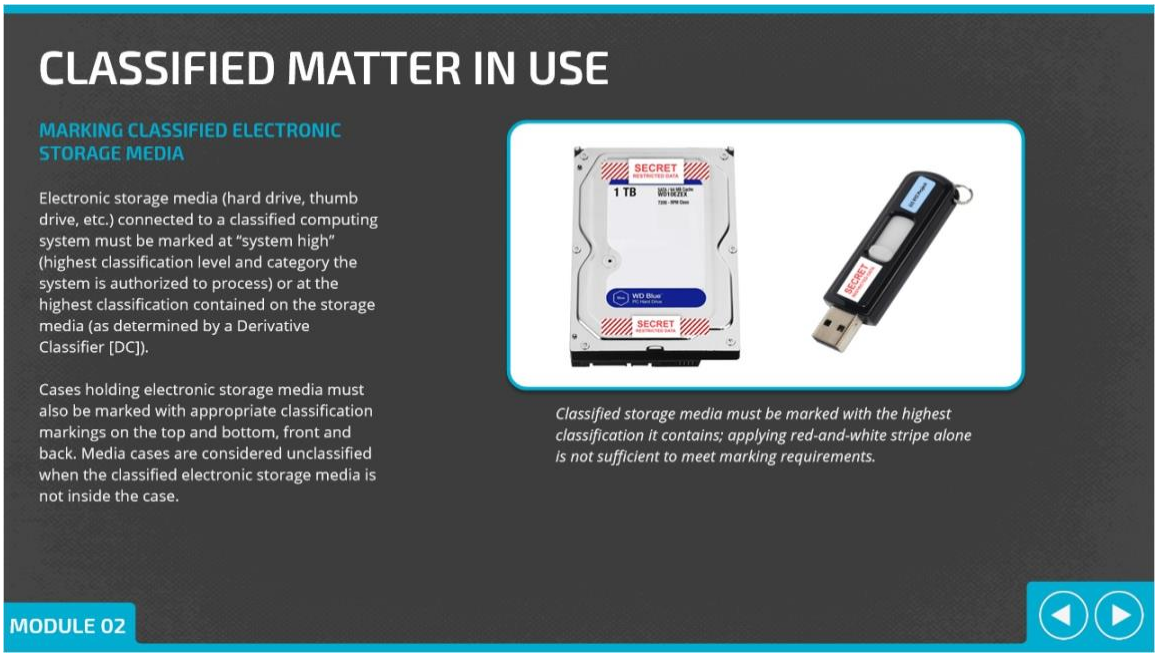
Final (Slide Layer)



Incomplete (Slide Layer)



1.14 Classified Matter in Use



Notes:

CLASSIFIED MATTER IN USE

MARKING CLASSIFIED ELECTRONIC STORAGE MEDIA
Electronic storage media (hard drive, thumb drive, etc.) connected to a classified computing system must be marked at "system high" (highest classification level and category the system is authorized to process) or at the highest classification contained on the storage media (as determined by a Derivative Classifier [DC]).

Cases holding electronic storage media must also be marked with appropriate classification markings on the top and bottom, front and back. Media cases are considered unclassified when the classified electronic storage media is not inside the case.

SECURITY TIP: Classified storage media must be marked with the highest classification it contains; applying red-and-white stripe alone is not sufficient to meet marking requirements.

1.15 Classified Matter in Use



Notes:

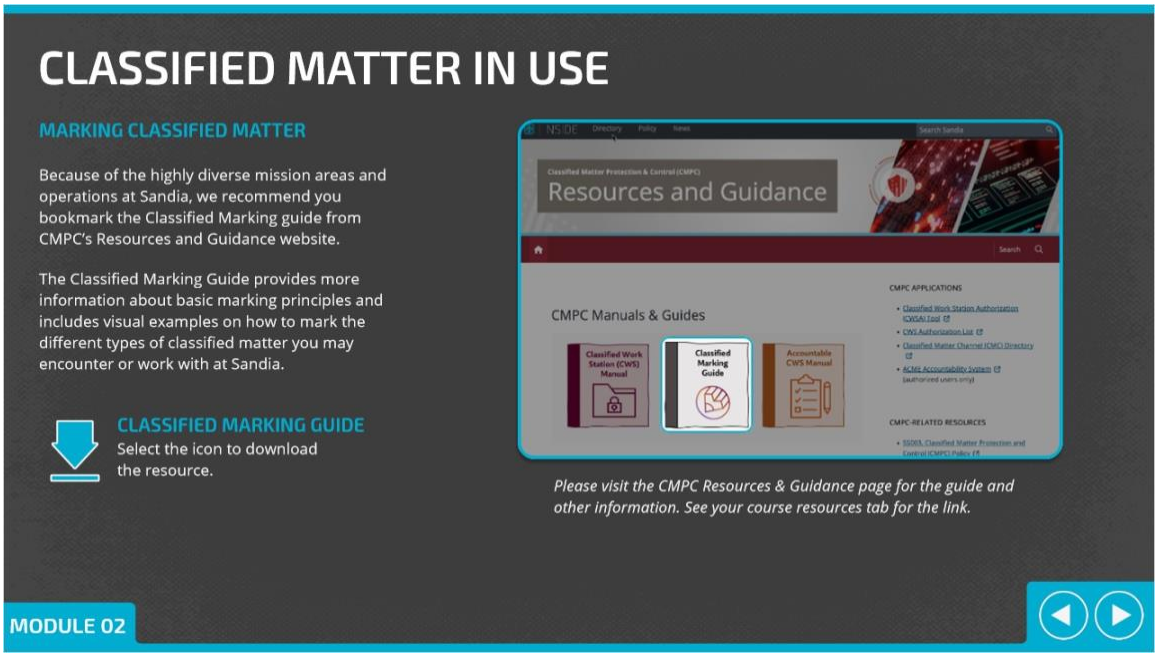
Classified Matter in Use

MARKING CLASSIFIED MATERIAL
Classified material must have the classification level and category (if RD or FRD) stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device.

NOTE: If items cannot be marked (e.g.; very small items), the container holding them must be marked with the item's classification.
Markings on Classified material must be visible, regardless of the angle or positioning of the material.

Classified material can be marked in different ways (as shown in the examples above), but it must always include the classification level and category (if RD or FRD).

1.16 Classified Matter in Use



Notes:

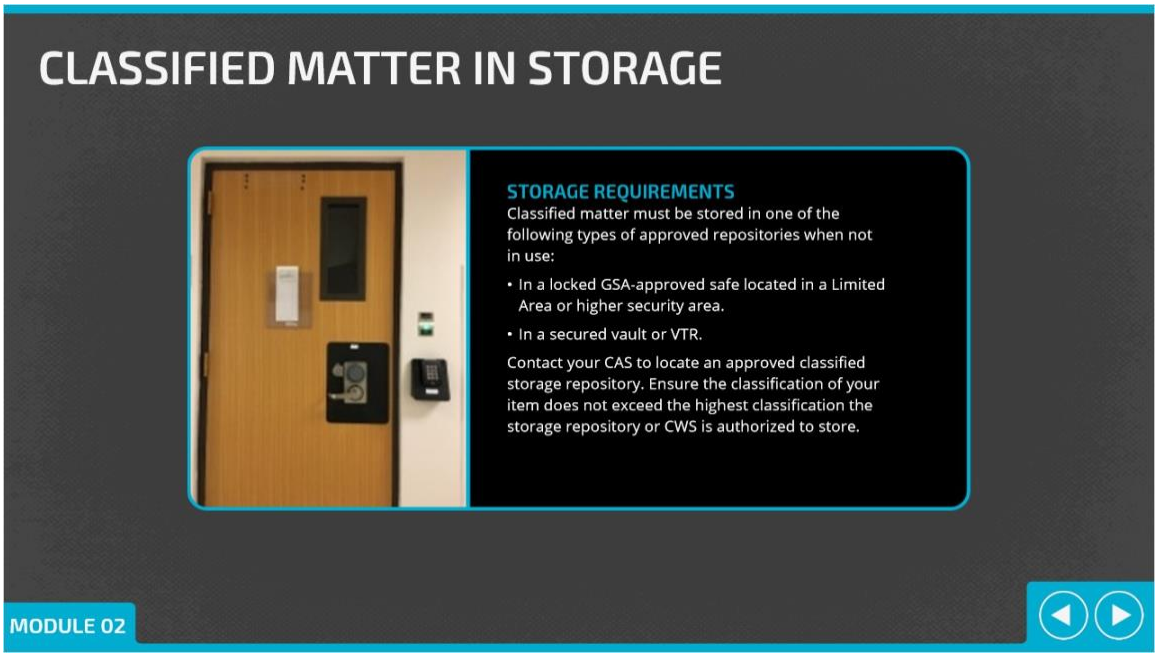
Classified Matter in Use

MARKING CLASSIFIED MATTER
Because of the highly diverse mission areas and operations at Sandia, we recommend you bookmark the Classified Marking guide from CMPC's resources and Guidance website.

The Classified Marking Guide provides more information about basic marking principles and includes visual examples on how to mark the different types of classified matter you may encounter or work with at Sandia.

Please visit the CMPC Resources & Guidance page for the guide and other information. See your course resources tab for the link.

1.17 Classified Matter in Storage



Notes:

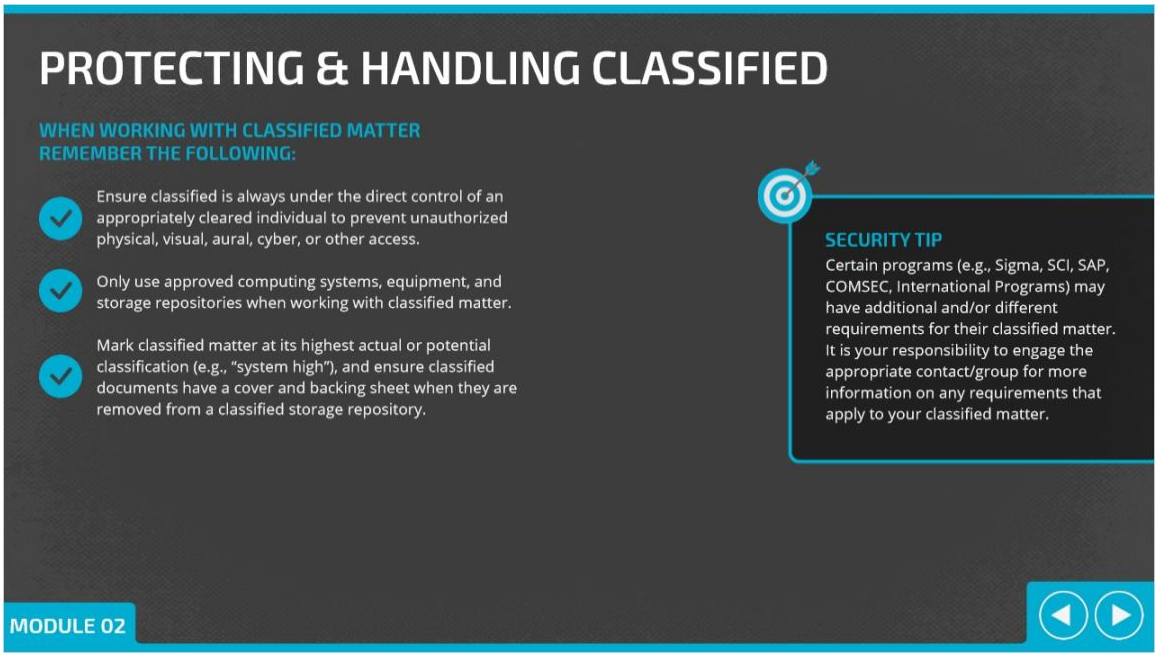
CLASSIFIED MATTER IN USE

STORAGE REQUIREMENTS
Classified matter must be stored in one of the following types of approved repositories when not in use:

- In a locked GSA-approved safe located in a Limited Area or higher security area.
- In a secured vault or VTR.

Contact your CAS to locate an approved classified storage repository. Ensure the classification of your item does not exceed the highest classification the storage repository or CWS is authorized to store.

1.18 Protecting & Handling Classified



Notes:

PROTECTING & HANDLING CLASSIFIED

When working with classified matter remember the following:

Ensure classified is always under the direct control of an appropriately cleared individual to prevent unauthorized physical, visual, aural, cyber, or other access.
Only use approved computing systems, equipment, and storage repositories when working with classified matter.

Mark classified matter at its highest actual or potential classification (e.g., "system high"), and ensure classified documents have a cover and backing sheet when they are removed from a classified storage repository.

SECURITY TIP: Certain programs (e.g.; Sigma, SCI, SAP, International Programs) may have additional and/or different requirements for their classified matter. It is your responsibility to engage the appropriate contact/group for more information on any requirements that apply to your classified matter.

1.19 Reporting Requirements



Notes:

REPORTING REQUIREMENTS

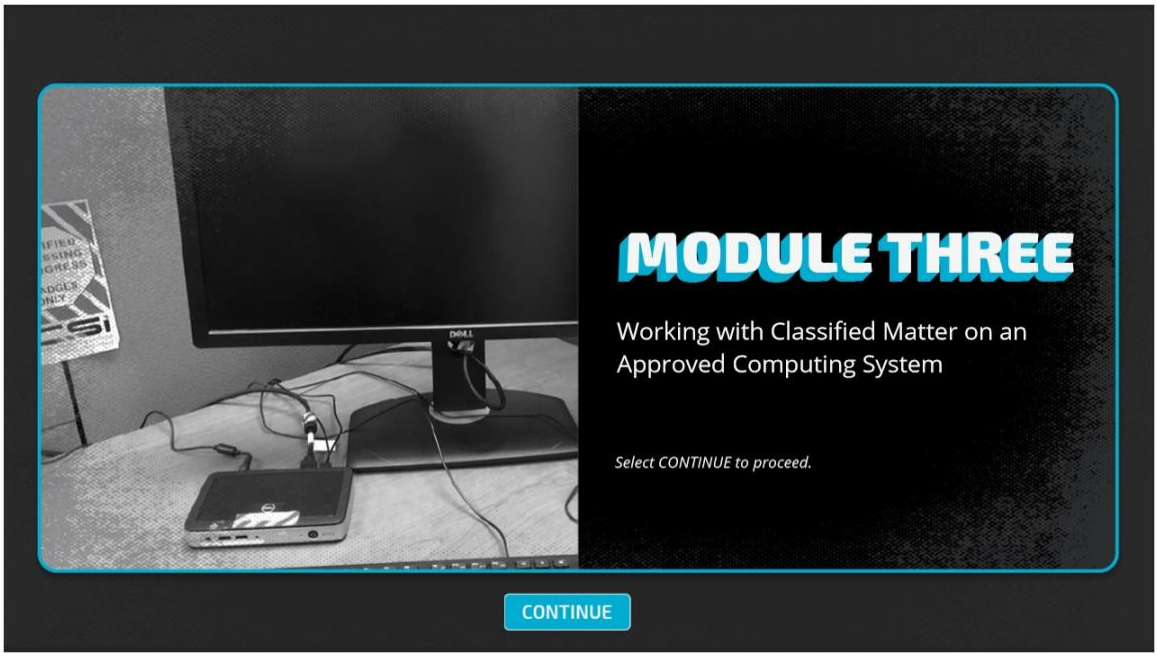
Report the following situations to the Security Incident Management Program (SIMP) immediately:

If there is a loss, compromise, or suspected loss/compromise of classified matter.
Anytime a classified storage repository is found unsecured and unattended.
If, during an emergency/evacuation, classified matter cannot be protected by an authorized individual or a classified storage repository is left unsecured.

SEC301: Module Three

1. Module Three

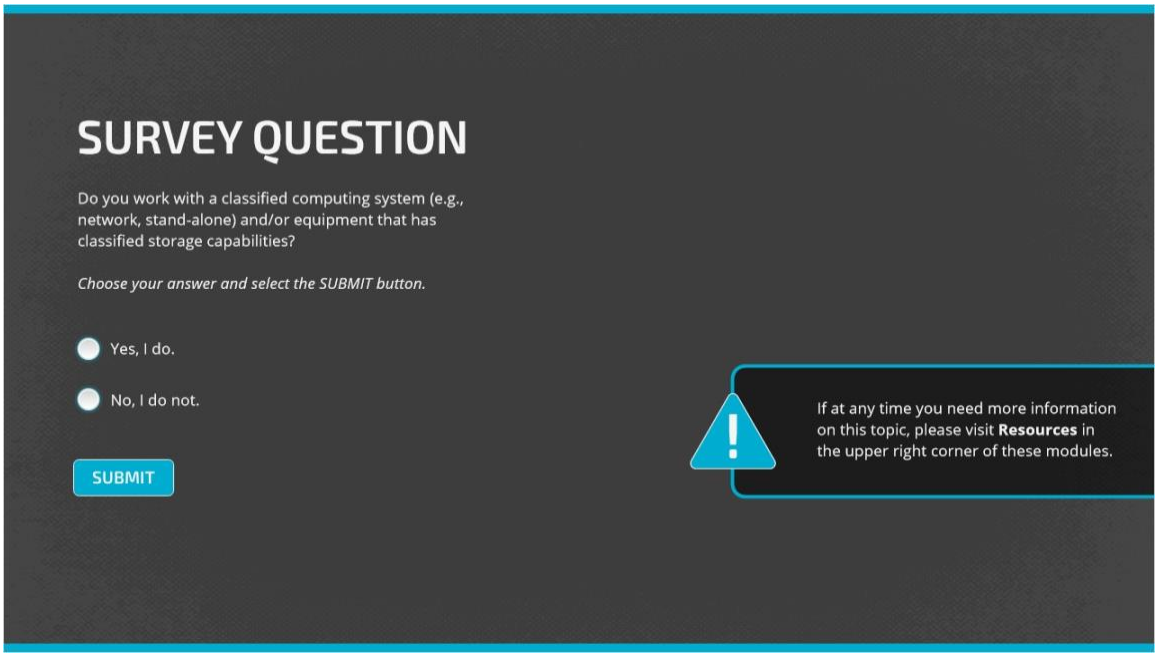
1.1 Module Introduction



Notes:

Module Three: Working with Classified Matter on an Approved Computing System

1.2 Survey Question



Notes:

Survey Question

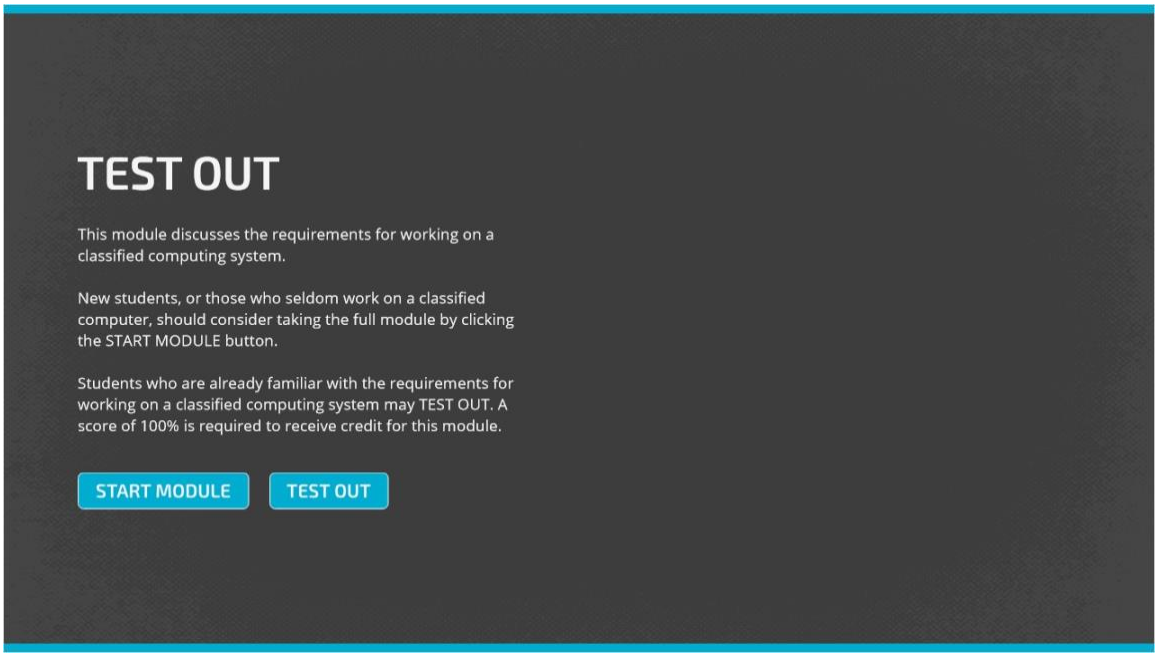
Do you work with a classified computing system (e.g., network, stand-alone) and/or equipment that has classified storage capabilities?

Choose your answer and select the SUBMIT button.

Yes, I do.
No, I do not.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option

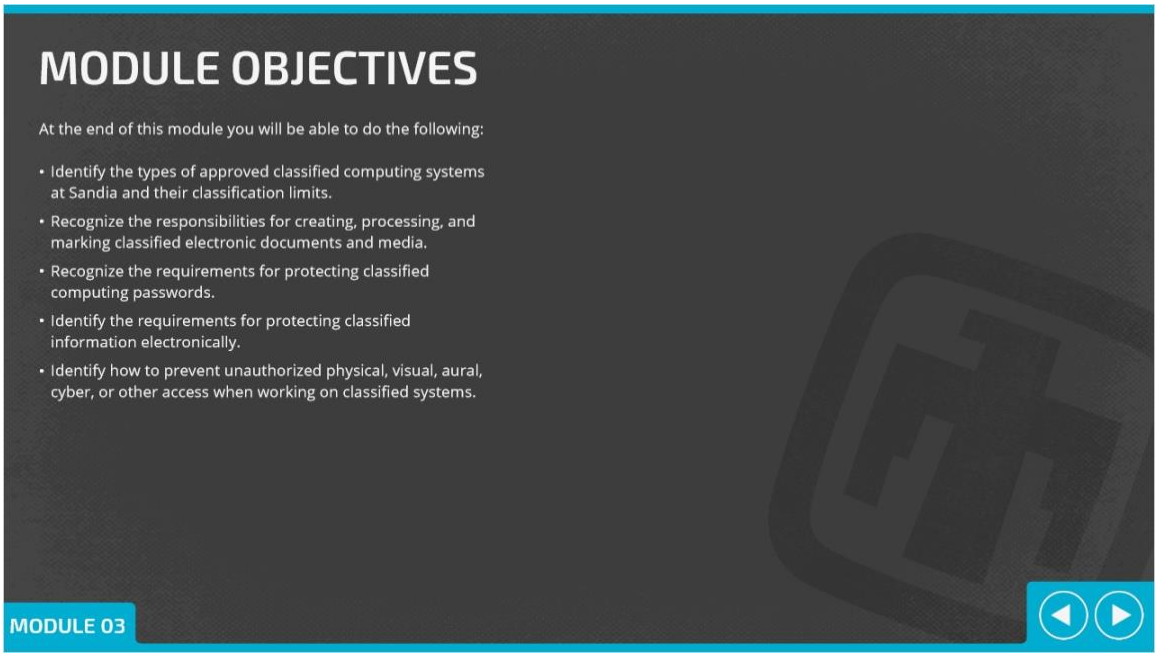


Notes:

Test Out

This module discusses the requirements for working on a classified computing system.
New students, or those who seldom work on a classified computer, should consider taking the full module by clicking the START MODULE button.
Students who are already familiar with the requirements for working on a classified computing system may TEST OUT. A score of 100% is required to receive credit for this module.

1.4 Objectives



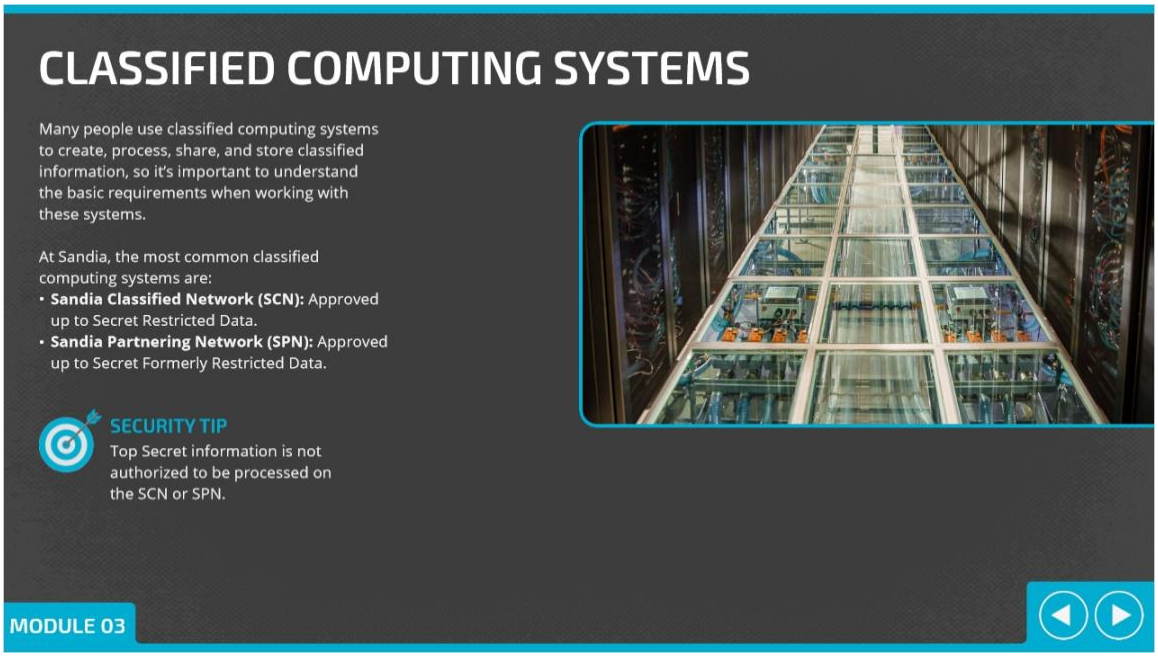
Notes:

Module Objectives

At the end of this module you will be able to do the following:

- Identify the types of approved classified computing systems at Sandia and their classification limits.
- Recognize the responsibilities for creating, processing, and marking classified electronic documents and media.
- Recognize the requirements for protecting classified computing passwords.
- Identify the requirements for protecting classified information electronically.
- Identify how to prevent unauthorized physical, visual, aural, cyber, or other access when working on classified systems.

1.5 Classified Computing Systems



Notes:

Classified Computing Systems

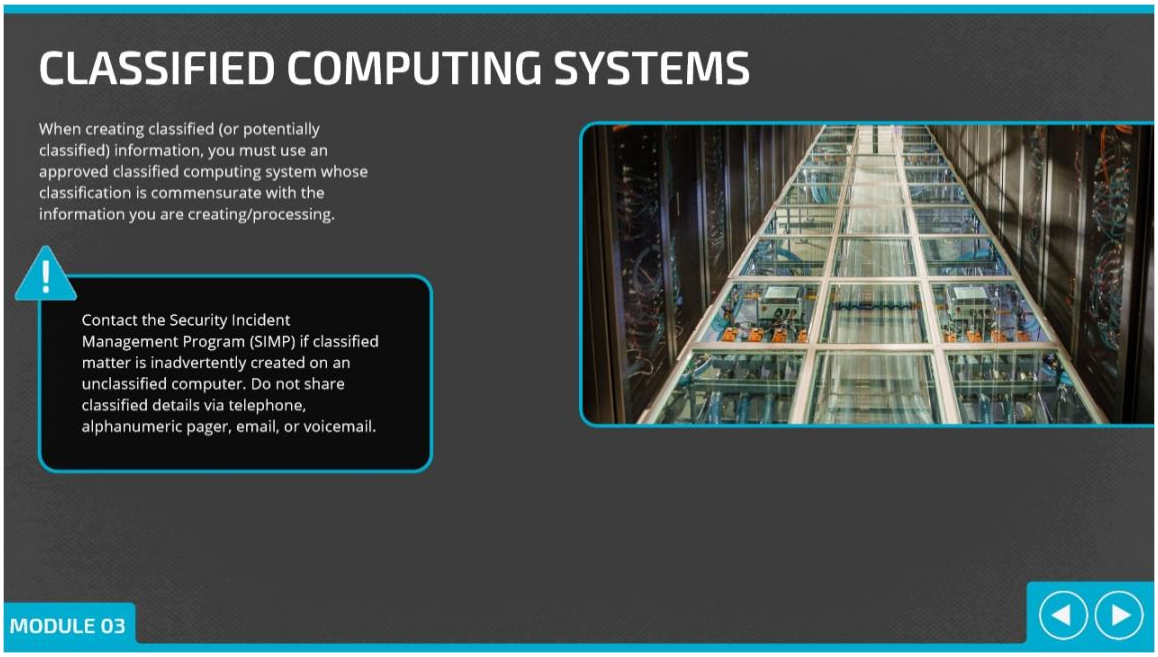
Many people use classified computing systems to create, process, share, and store classified information, so it's important to understand the basic requirements when working with these systems.

At Sandia, the most common classified computing systems are:

- Sandia Classified Network (SCN): Approved up to Secret Restricted Data.
- Sandia Partnering Network (SPN): Approved up to Secret Formerly Restricted Data.

Security Tip: Top Secret information is not authorized to be processed on the SCN or SPN.

1.6 Classified Computing Systems



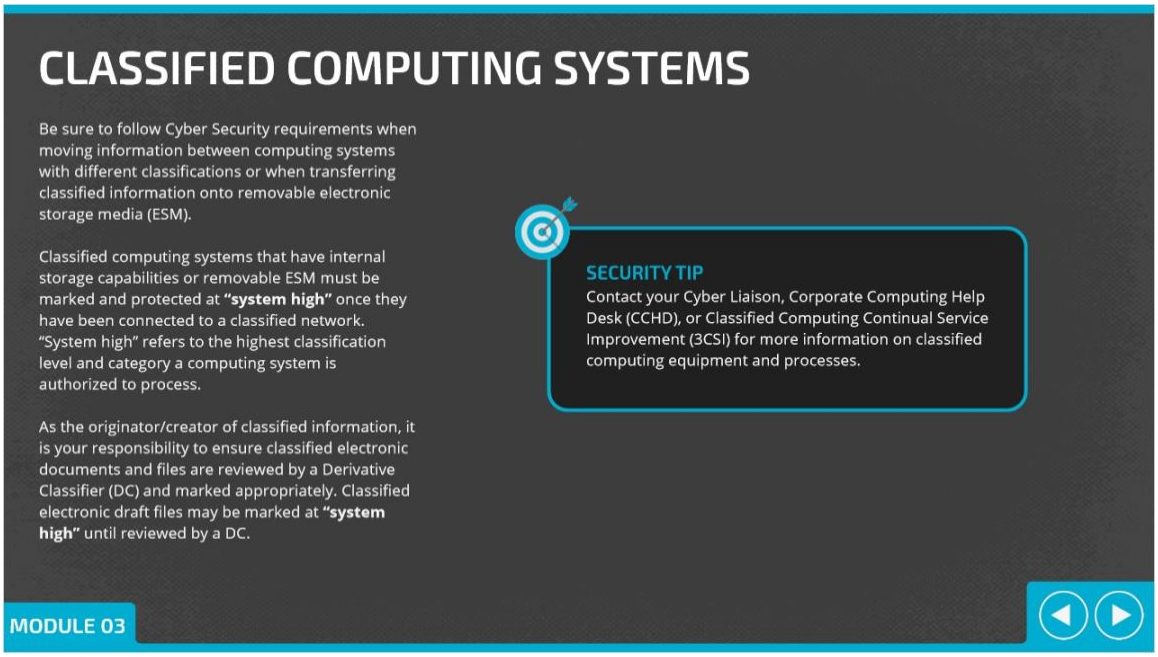
Notes:

Classified Computing Systems

When creating classified (or potentially classified) information, you must use an approved classified computing system whose classification is commensurate with the information you are creating/processing.

Contact the Security Incident Management Program (SIMP) if classified matter is inadvertently created on an unclassified computer. Do not share classified details via telephone, alphanumeric pager, email, or voicemail.

1.7 Classified Computing Systems



Notes:

Classified Computing Systems

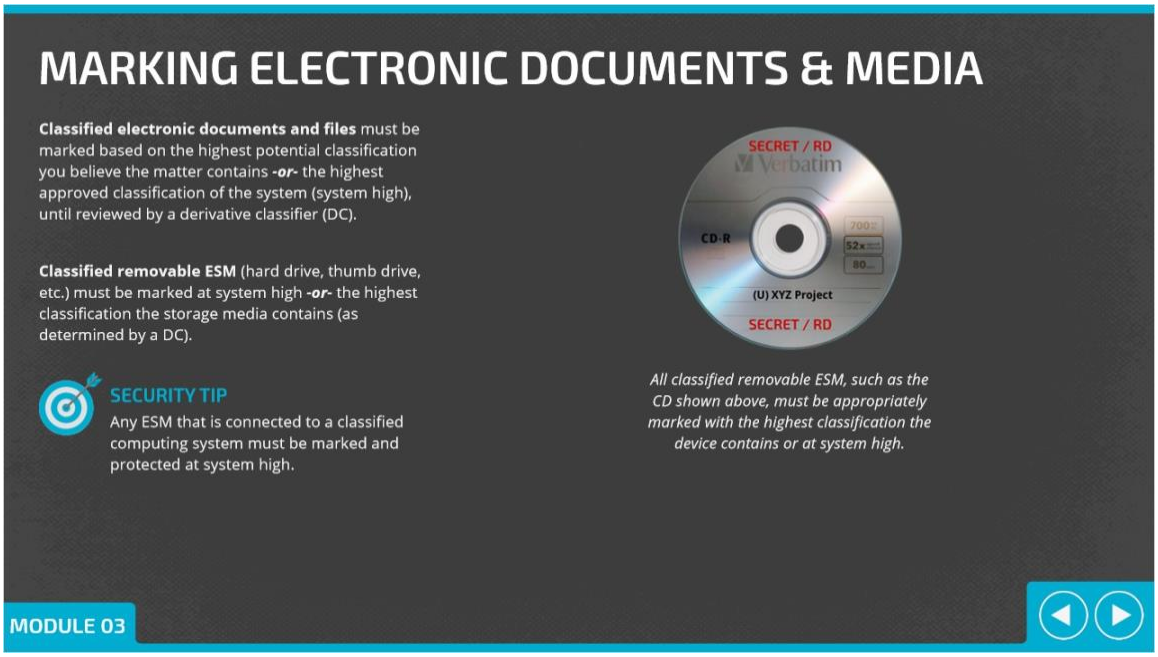
Be sure to follow Cyber Security requirements when moving information between computing systems with different classifications or when transferring classified information onto removable electronic storage media (ESM).

Classified computing systems that have internal storage capabilities or removable ESM must be marked and protected at "system high" once they have been connected to a classified network.
"System high" refers to the highest classification level and category a computing system is authorized to process.

As the originator/creator of classified information, it is your responsibility to ensure classified electronic documents and files are reviewed by a Derivative Classifier (DC) and marked appropriately. Classified electronic draft files may be marked at "system high" until reviewed by a DC.

SECURITY TIP: Contact your Cyber Liaison, Corporate Computing Help Desk (CCHD), or Classified Computing Continual Service Improvement (3CSI) for more information on classified computing equipment and processes.

1.8 Marking Electronic Documents and Media



Notes:

Marking Electronic Documents and Media

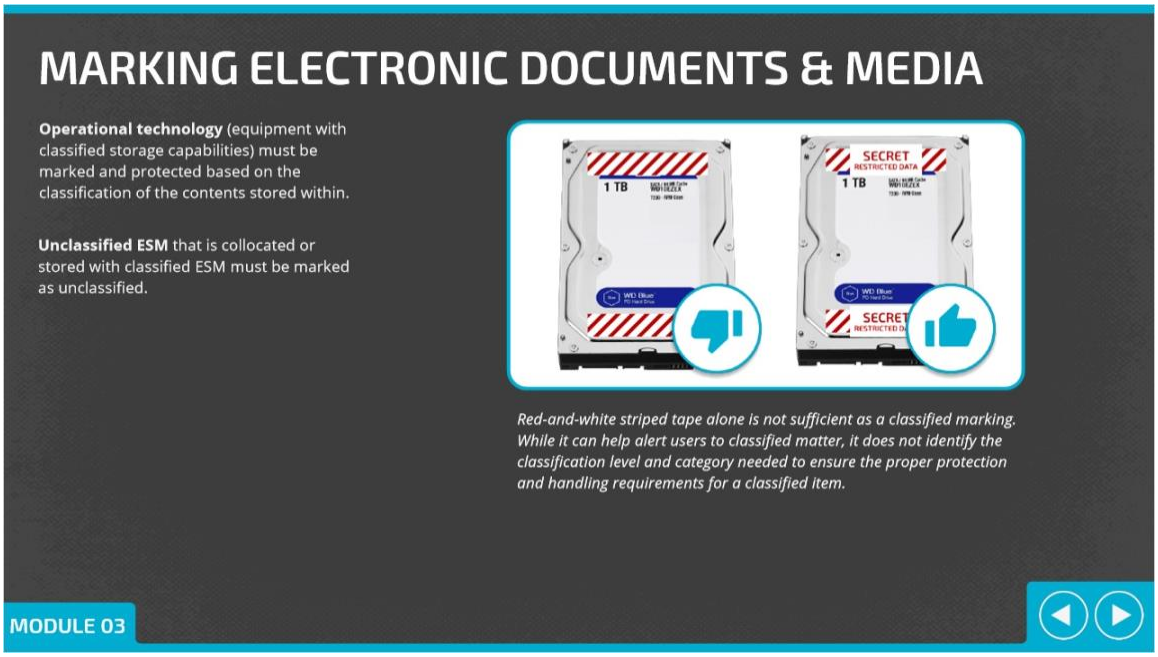
Classified electronic documents and files must be marked based on the highest potential classification you believe the matter contains -or- the highest approved classification of the system (system high), until reviewed by a derivative classifier (DC).

Classified removable ESM (hard drive, thumb drive, etc.) must be marked at system high -or- the highest classification the storage media contains (as determined by a DC).

SECURITY TIP: Any ESM that is connected to a classified computing system must be marked and protected at system high.

All classified removable ESM, such as the CD shown above, must be appropriately marked with the highest classification the device contains or at system high.

1.9 Marking Electronic Documents and Media



Notes:

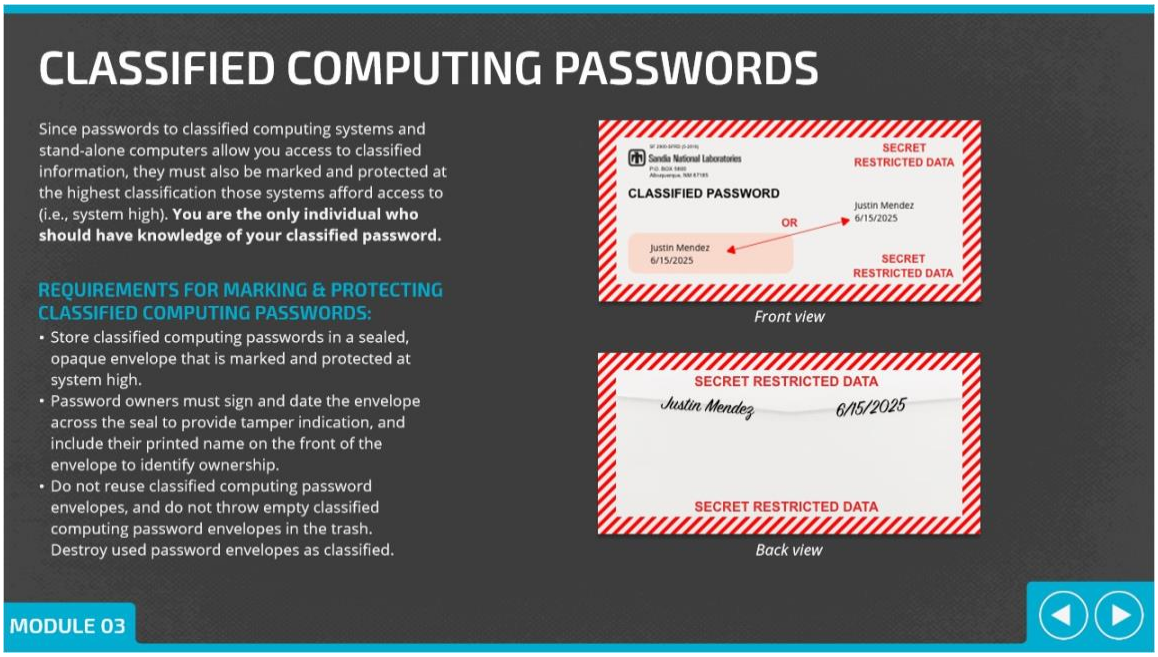
Marking Electronic Documents and Media

Operational technology (equipment with classified storage capabilities) must be marked and protected based on the classification of the contents stored within.

Unclassified ESM that is collocated or stored with classified ESM must be marked as unclassified.

Red-and-white striped tape alone is not sufficient as a classified marking. While it can help alert users to classified matter, it does not identify the classification level and category needed to ensure the proper protection and handling requirements for a classified item.

1.10 Classified Computing Passwords



Notes:

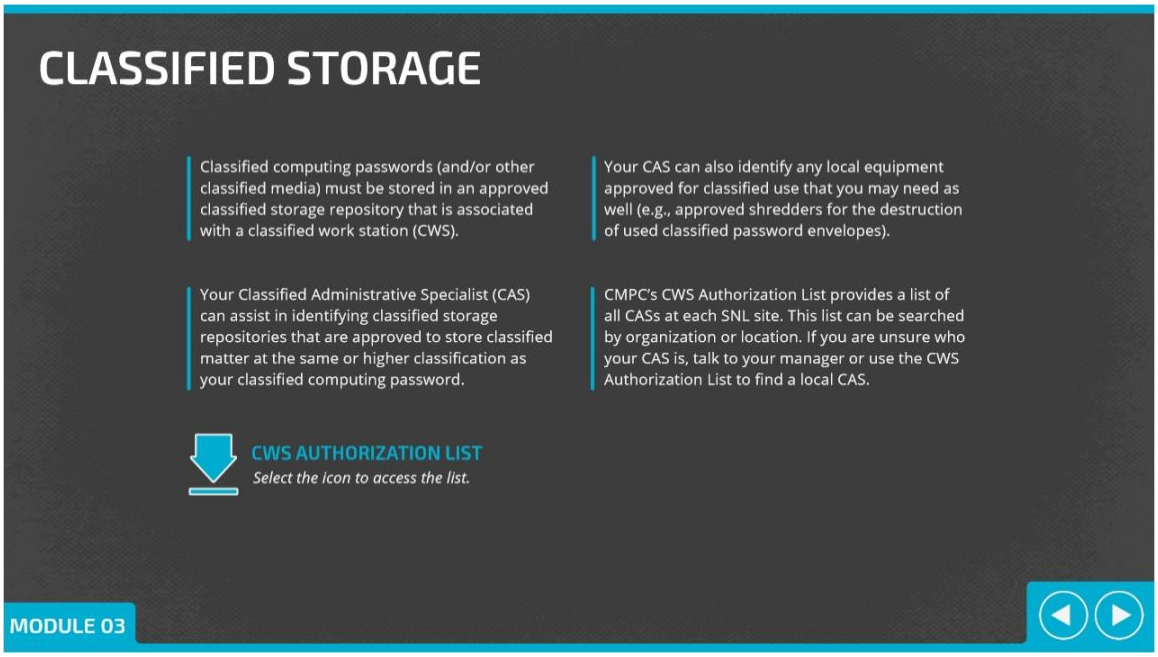
Classified Computing Passwords

Since passwords to classified computing systems and stand-alone computers allow you access to classified information, they must also be marked and protected at the highest classification those systems afford access to (i.e., system high).
You are the only individual who should have knowledge of your classified password.

REQUIREMENTS FOR MARKING & PROTECTING CLASSIFIED COMPUTING PASSWORDS:

- Store classified computing passwords in a sealed, opaque envelope that is marked and protected at system high.
- Password owners must sign and date the envelope across the seal to provide tamper indication, and include their printed name on the front of the envelope to identify ownership.
- Do not reuse classified computing password envelopes, and do not throw empty classified computing password envelopes in the trash. Destroy used password envelopes as classified.

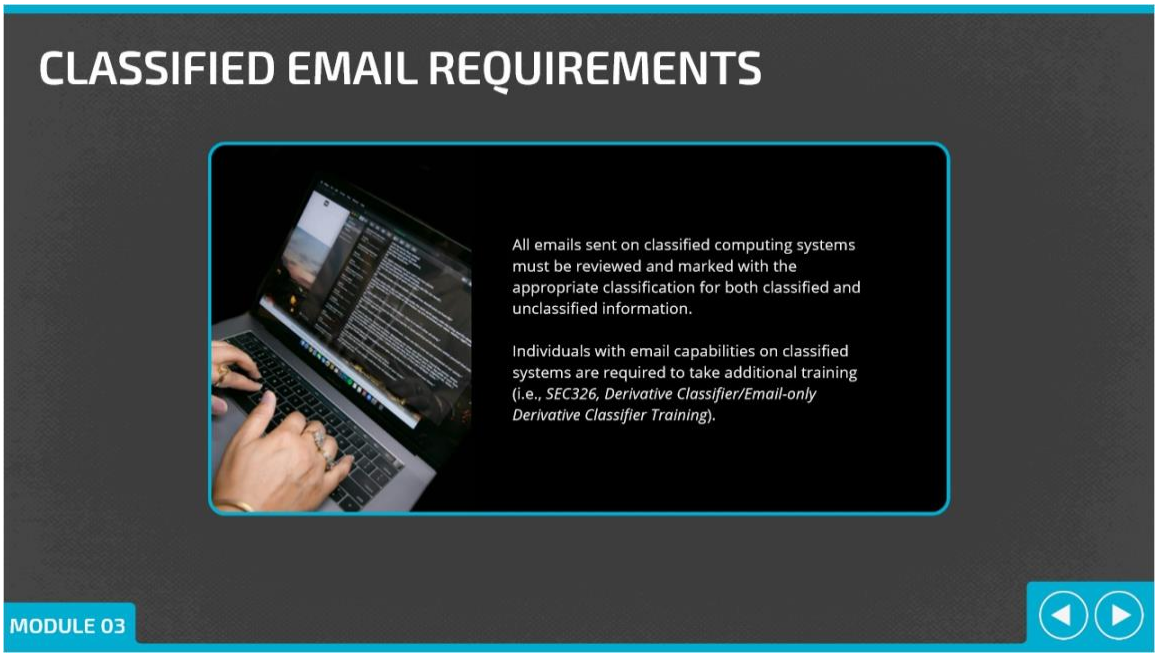
1.11 Classified Storage



Notes:

CLASSIFIED STORAGE
Classified computing passwords (and/or other classified media) must be stored in an approved classified storage repository that is associated with a classified work station (CWS).
Your Classified Administrative Specialist (CAS) can assist in identifying classified storage repositories that are approved to store classified matter at the same or higher classification as your classified computing password.
Your CAS can also identify any local equipment approved for classified use that you may need as well (e.g., approved shredders for the destruction of used classified password envelopes).
CMPC's CWS Authorization List provides a list of all CASs at each SNL site. This list can be searched by organization or location. If you are unsure who your CAS is, talk to your manager or use the CWS Authorization List to find a local CAS.

1.12 Classified Email Requirements



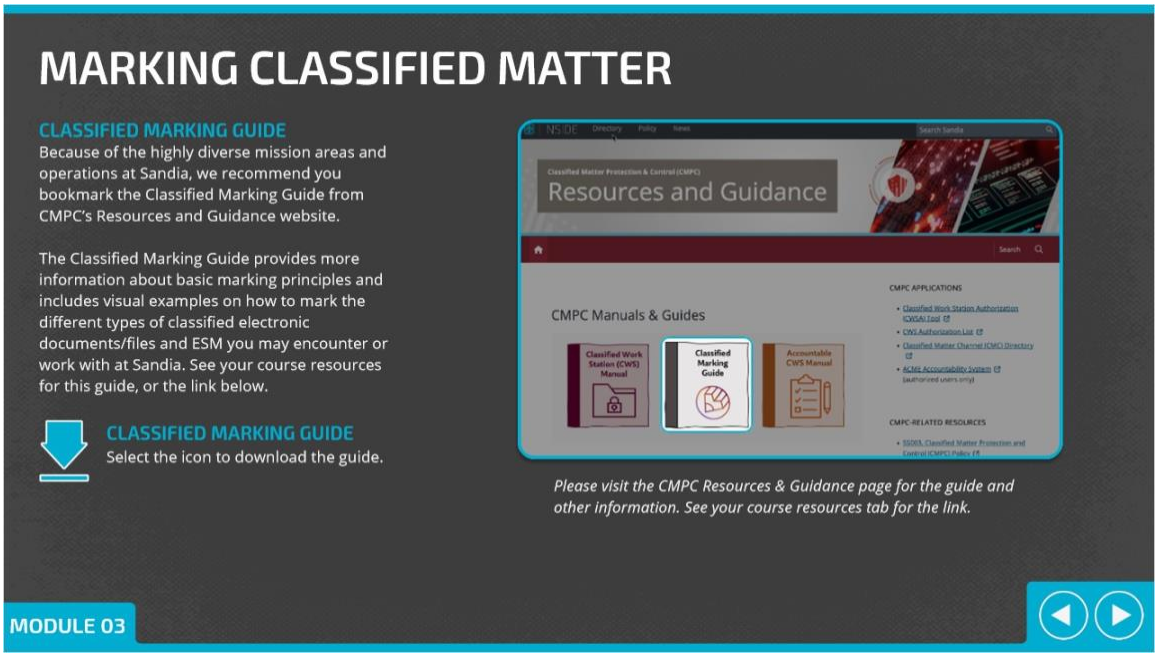
Notes:

Classified Email Requirements

All emails sent on classified computing systems must be reviewed and marked with the appropriate classification for both classified and unclassified information.

Individuals with email capabilities on classified systems are required to take additional training (i.e., SEC326, Derivative Classifier/Email-only Derivative Classifier Training).

1.13 Marking Classified Matter



Notes:

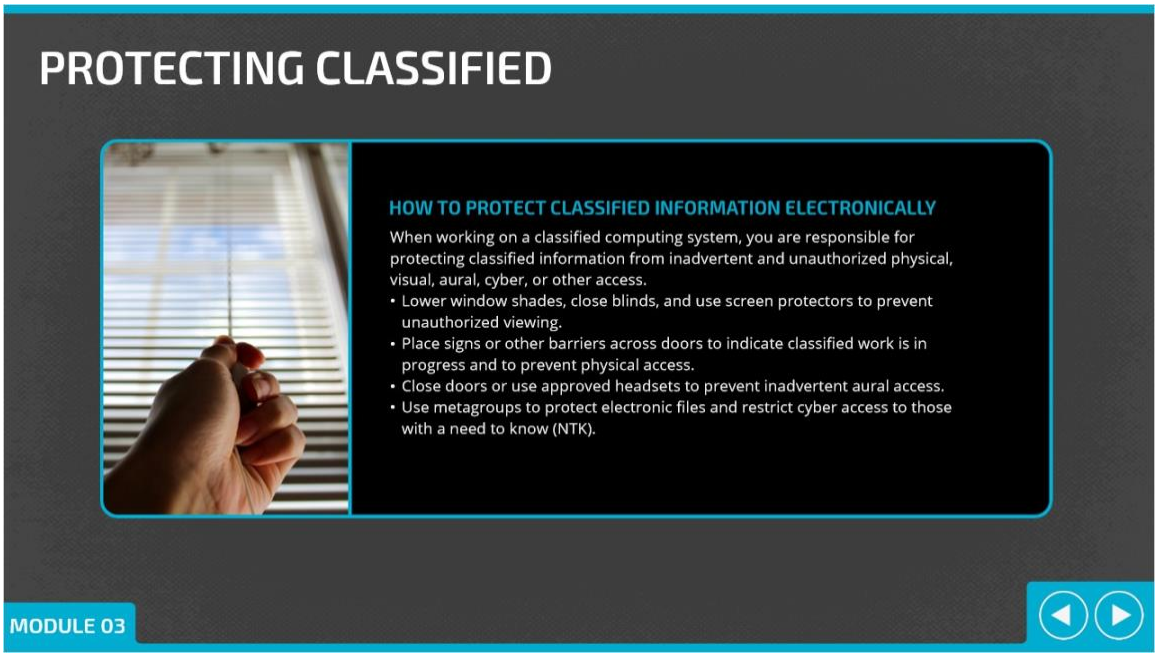
Marking Classified Matter

CLASSIFIED MARKING GUIDE
Because of the highly diverse mission areas and operations at Sandia, we recommend you bookmark the Classified Marking Guide from CMPC's Resources and Guidance website.

The Classified Marking Guide provides more information about basic marking principles and includes visual examples on how to mark the different types of classified electronic documents/files and ESM you may encounter or work with at Sandia. See your course resources for this guide, or the link below.

Please visit the CMPC Resources & Guidance page for the guide and other information. See your course resources tab for the link.

1.14 Protecting Classified Electronically



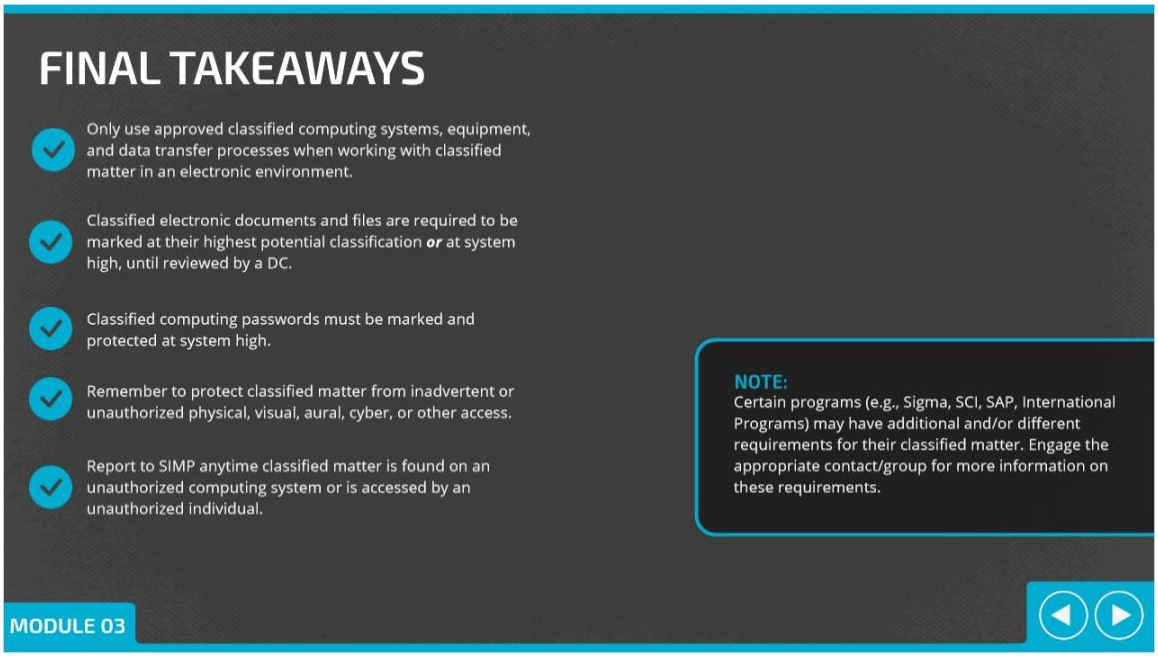
Notes:

Protecting Classified

HOW TO PROTECT CLASSIFIED INFORMATION ELECTRONICALLY
When working on a classified computing system, you are responsible for protecting classified information from inadvertent and unauthorized physical, visual, aural, cyber, or other access.

- Lower window shades, close blinds, and use screen protectors to prevent unauthorized viewing.
- Place signs or other barriers across doors to indicate classified work is in progress and to prevent physical access.
- Close doors or use approved headsets to prevent inadvertent aural access.
- Use metagroups to protect electronic files and restrict cyber access to those with a need to know (NTK).

1.15 Final Takeaways



Notes:

Final Takeaways

• Only use approved classified computing systems, equipment, and data transfer processes when working with classified matter in an electronic environment.
• Classified electronic documents and files are required to be marked at their highest potential classification or at system high, until reviewed by a DC.
• Classified computing passwords must be marked and protected at system high.
• Remember to protect classified matter from inadvertent or unauthorized physical, visual, aural, cyber, or other access.
• Report to SIMP anytime classified matter is found on an unauthorized computing system or is accessed by an unauthorized individual.
Note: Certain programs (e.g., Sigma, SCI, SAP, International Programs) may have additional and/or different requirements for their classified matter. Engage the appropriate contact/group for more information on these requirements.

SEC301: Module Four

1. Module Four

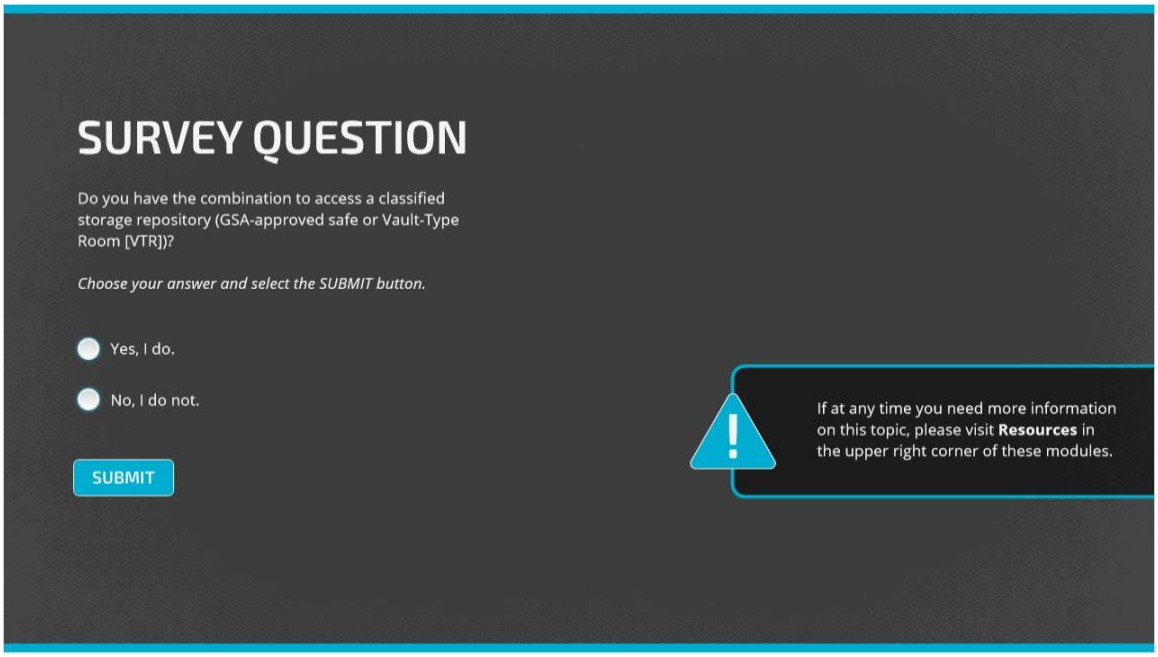
1.1 Module Introduction



Notes:

Module Four: Storing Classified Matter

1.2 Survey



Notes:

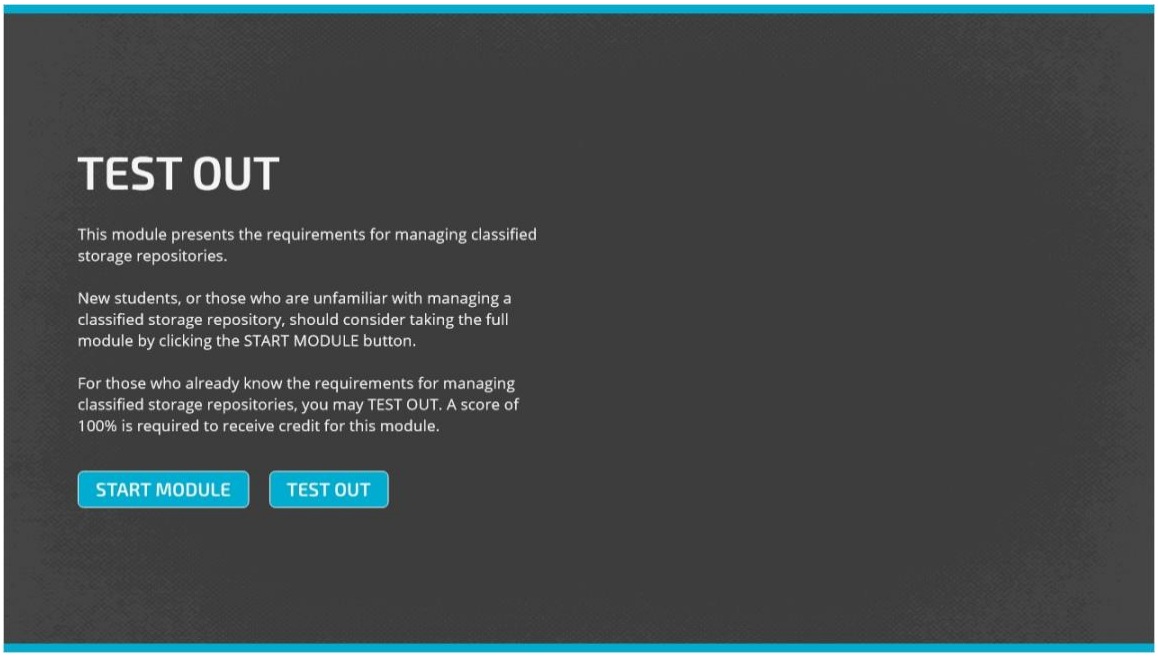
Survey Question

Do you have the combination to access a classified storage repository (GSA-approved safe or Vault-Type Room [VTR])?

Choose your answer and select the SUBMIT button.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option



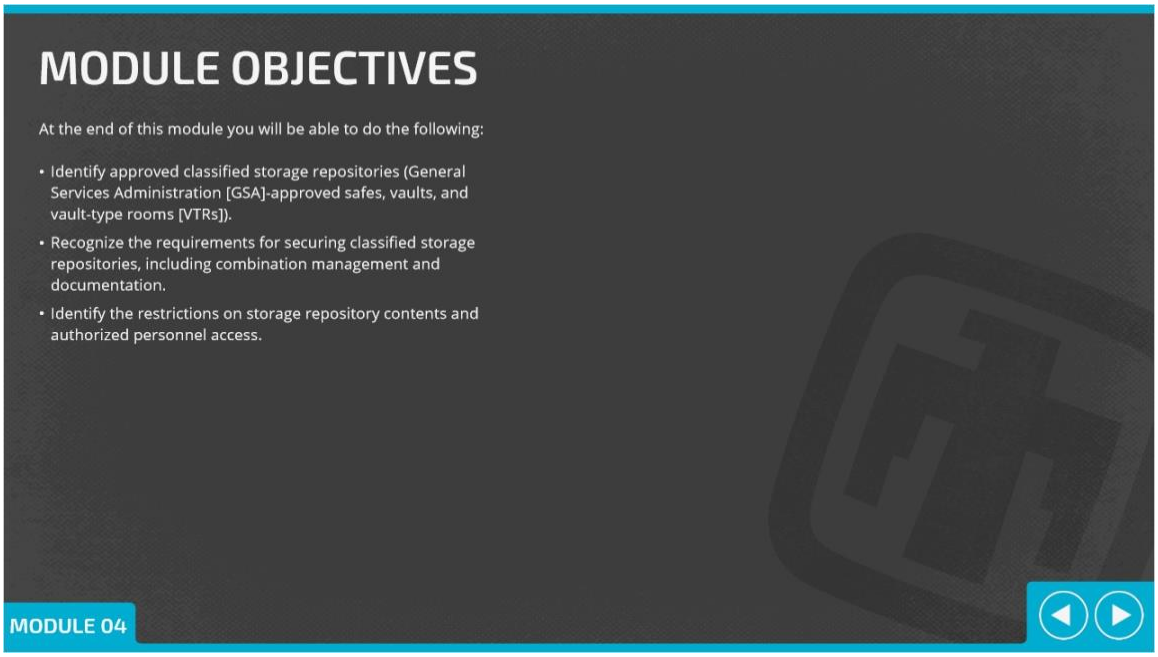
Notes:

Test Out
This module presents the requirements for managing classified storage repositories.

New students, or those who are unfamiliar with managing a classified storage repository, should consider taking the full module by clicking the START MODULE button.

For those who already know the requirements for managing classified storage repositories, you may TEST OUT. A score of 100% is required to receive credit for this module.

1.4 Objectives



Notes:

Module Objectives

At the end of this module you will be able to do the following:

- Identify approved classified storage repositories (General Services Administration [GSA]-approved safes, vaults, and vault-type rooms [VTRs]).
- Recognize the requirements for securing classified storage repositories, including combination management and documentation.
- Identify the restrictions on storage repository contents and authorized personnel access.

1.5 Storing Classified Matter



Notes:

STORING CLASSIFIED MATTER

APPROVED CLASSIFIED STORAGE REPOSITORIES

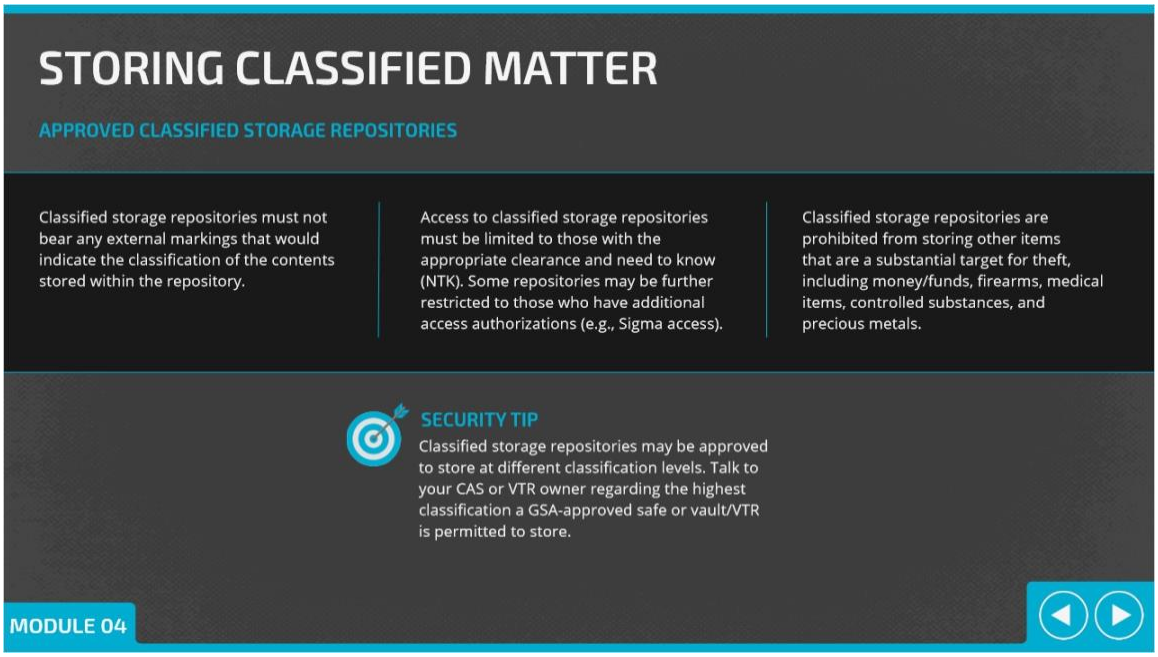
When not in use or under the direct control
of an appropriately cleared individual, classified matter must be stored in an approved repository.

Only GSA-approved safes, vaults, and vault-type rooms (VTRs) are permitted to store classified matter. All classified storage repositories must remain locked/secured when not under the supervision of an authorized individual.

All classified storage repositories must also be associated with a Classified Work Station (CWS) in the Classified Work Station Authorization (CWSA) tool.

SECURITY TIP:
Classified Matter Protection and Control's (CMPC) CWSA tool does not manage or track classified storage repositories located inside of Sensitive Compartmented Information Facilities (SCIFs) or Special Access Program Facilities (SAPFs). An alternate special security officer or program security officer can provide more information on classified storage

1.6 Storing Classified Matter



Notes:

Storing Classified Matter

APPROVED CLASSIFIED STORAGE REPOSITORIES

Classified storage repositories must not bear any external markings that would indicate the classification of the contents stored within the repository.

Access to classified storage repositories must be limited to those with the appropriate clearance and need to know (NTK). Some repositories may be further restricted to those who have additional access authorizations (e.g., Sigma access).

Classified storage repositories are prohibited from storing other items that are a substantial target for theft, including money/funds, firearms, medical items, controlled substances, and precious metals.

SECURITY TIP: Classified storage repositories may be approved to store at different classification levels. Talk to your CAS or VTR owner regarding the highest classification a GSA-approved safe or vault/VTR is permitted to store.

1.7 Storing Classified Matter



Notes:

STORING CLASSIFIED MATTER

GSA-APPROVED SAFES

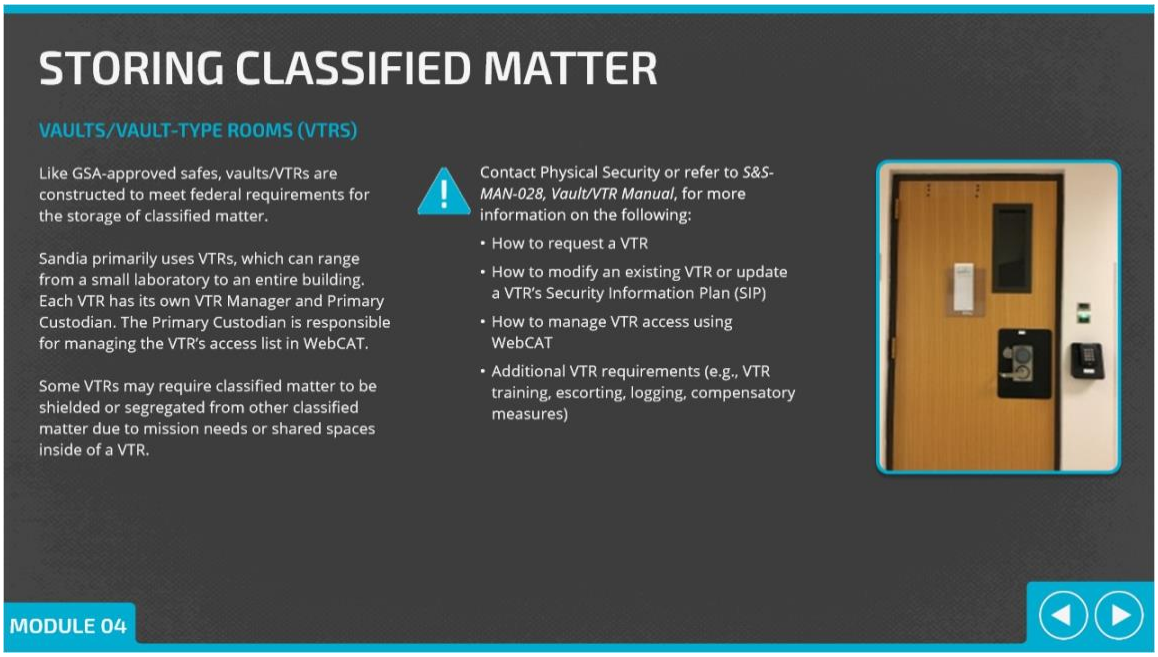
A GSA-approved safe is a fortified cabinet with at least one combination spin-dial lock that meets federal requirements for the storage of classified matter. Unauthorized modifications to the safe will void the safe's GSA approval.

All GSA-approved safes that store classified matter must be located in a Limited Area or higher security area.

Please refer to S&S-MAN-013, Classified Work Station (CWS) Manual, for specific information on the following:

- How to procure, move, or get rid of a GSA-approved safe
- How to add or remove a GSA-approved safe from a CWS
- How to manage a GSA-approved safe and its combination

1.8 Storing Classified Matter



Notes:

STORING CLASSIFIED MATTER

VAULTS/VAULT-TYPE ROOMS (VTRS)

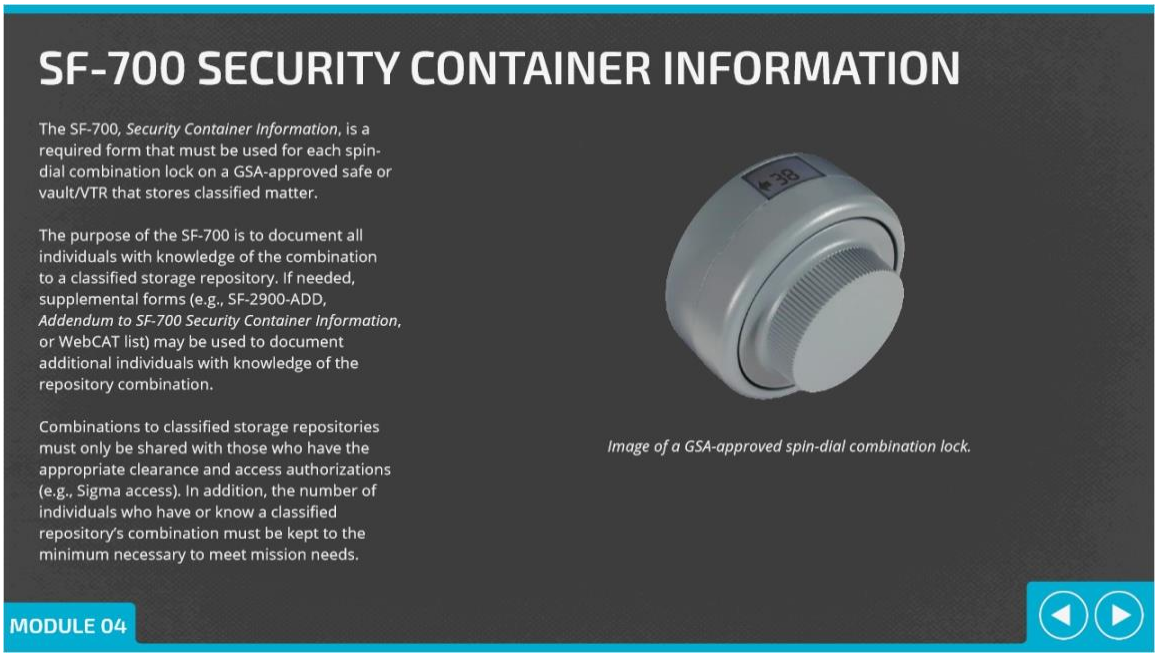
Like GSA-approved safes, vaults/VTRs are constructed to meet federal requirements for the storage of classified matter.

Sandia primarily uses VTRs, which can range from a small laboratory to an entire building. Each VTR has its own VTR Manager and Primary Custodian. The Primary Custodian is responsible for managing the VTR's access list in WebCAT.

Some VTRs may require classified matter to be shielded or segregated from other classified matter due to mission needs or shared spaces inside of a VTR.

Contact Physical Security or refer to S&S-MAN-028, Vault/VTR Manual, for more information on the following:
How to request a VTR
How to modify an existing VTR or update a VTR's Security Information Plan (SIP)
How to manage VTR access using WebCAT
Additional VTR requirements (e.g., VTR training, escorting, logging, compensatory measures)

1.9 SF-700 Security Container Information



Notes:

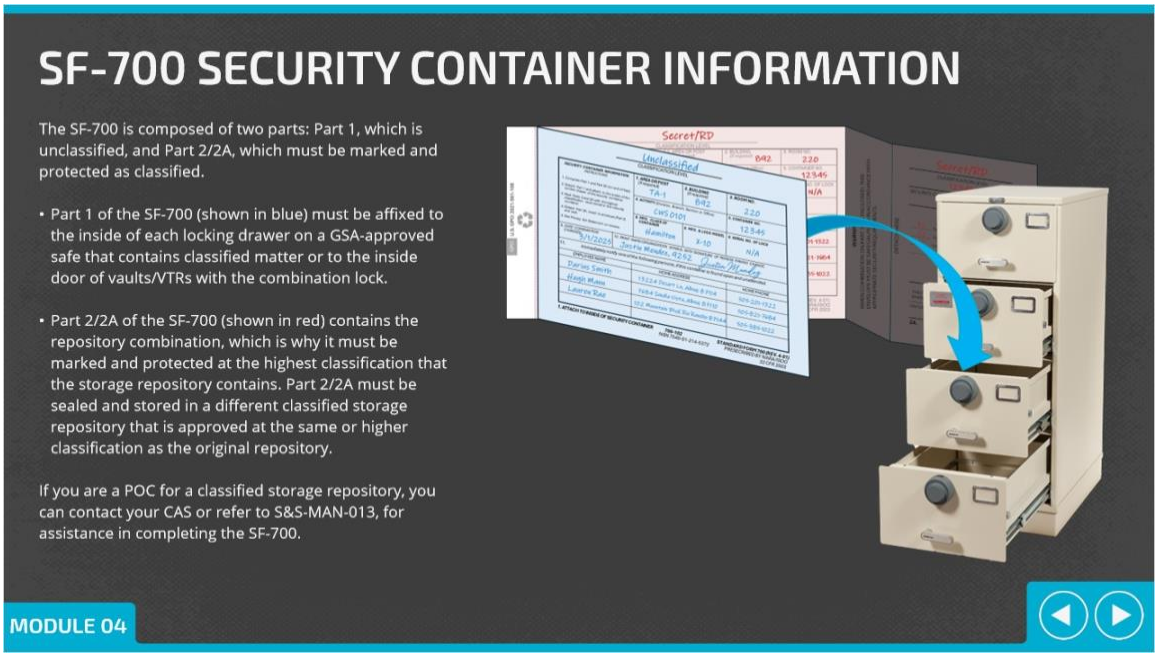
SF-700 SECURITY CONTAINER INFORMATION

The SF-700, Security Container Information, is a required form that must be used for each spin-dial combination lock on a GSA-approved safe or vault/VTR that stores classified matter.

The purpose of the SF-700 is to document all individuals with knowledge of the combination to a classified storage repository. If needed, supplemental forms (e.g., SF-2900-ADD, Addendum to SF-700 Security Container Information, or WebCAT list) may be used to document additional individuals with knowledge of the repository combination.

Combinations to classified storage repositories must only be shared with those who have the appropriate clearance and access authorizations (e.g., Sigma access). In addition, the number of individuals who have or know a classified repository's combination must be kept to the minimum necessary to meet mission needs.

1.10 SF-700 Security Container



Notes:

SF-700 SECURITY CONTAINER INFORMATION

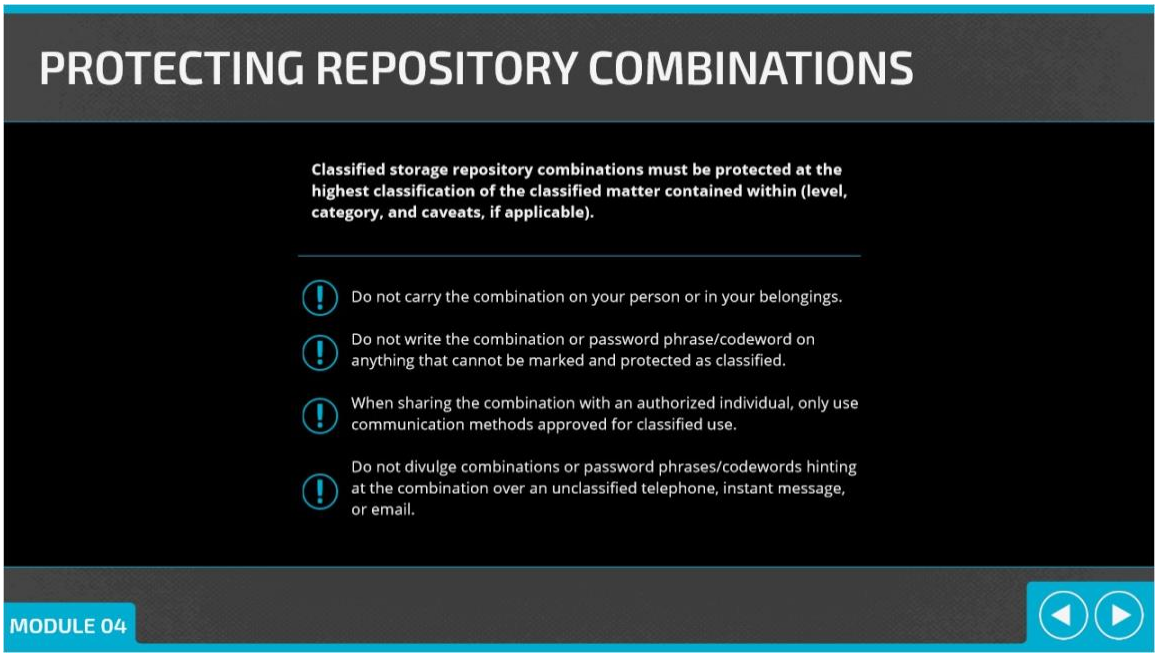
The SF-700 is composed of two parts: Part 1, which is unclassified, and Part 2/2A, which must be marked and protected as classified.

Part 1 of the SF-700 (shown in blue) must be affixed to the inside of each locking drawer on a GSA-approved safe that contains classified matter or to the inside door of vaults/VTRs with the combination lock.

Part 2/2A of the SF-700 (shown in red) contains the repository combination, which is why it must be marked and protected at the highest classification that the storage repository contains. Part 2/2A must be sealed and stored in a different classified storage repository that is approved at the same or higher classification as the original repository.

If you are a POC for a classified storage repository, you can contact your CAS or refer to S&S-MAN-013, for assistance in completing the SF-700.

1.11 Protecting Repository Combinations

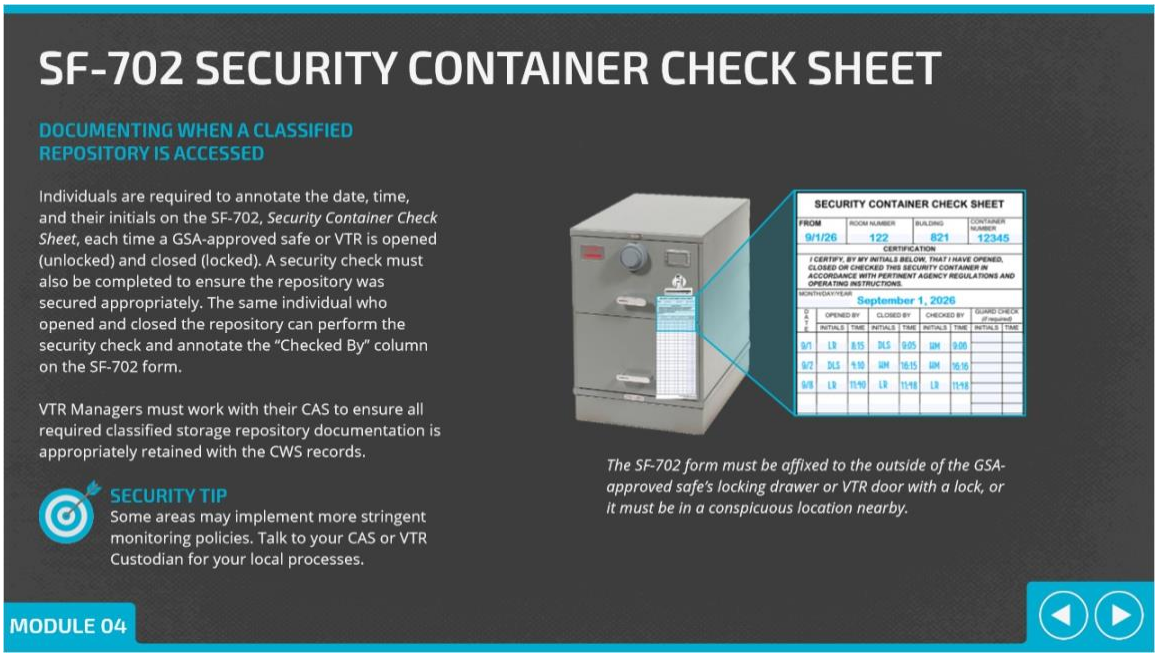


Notes:

PROTECTING REPOSITORY COMBINATIONS

Classified storage repository combinations must be protected at the highest classification of the classified matter contained within (level, category, and caveats, if applicable).
Do not carry the combination on your person or in your belongings.
Do not write the combination or password phrase/codeword on anything that cannot be marked and protected as classified.
When sharing the combination with an authorized individual, only use communication methods approved for classified use.
Do not divulge combinations or password phrases/codewords hinting at the combination over an unclassified telephone, instant message, or email.

1.12 SF-702 Security Container Check Sheet



Notes:

SF-700 Security Container Check Sheet

DOCUMENTING WHEN A CLASSIFIED REPOSITORY IS ACCESSED

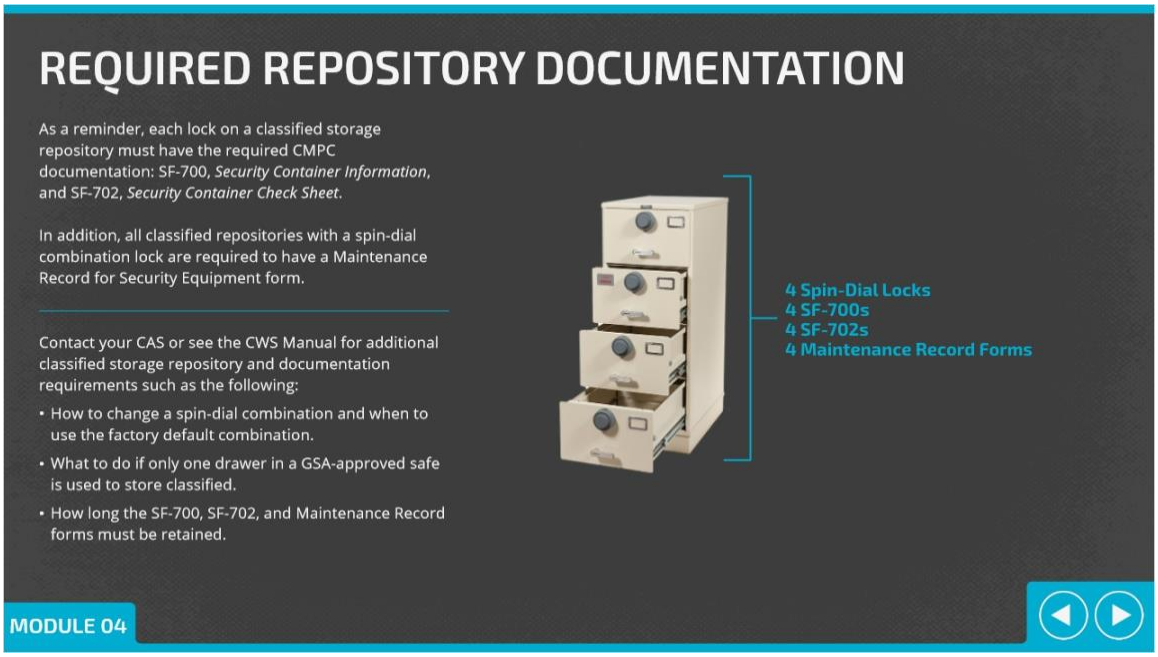
Individuals are required to annotate the date, time,
and their initials on the SF-702, Security Container Check Sheet, each time a GSA-approved safe or VTR is opened (unlocked) and closed (locked). A security check must also be completed to ensure the repository was secured appropriately. The same individual who opened and closed the repository can perform the security check and annotate the "checked by" column on the SF-702 form.

VTR Managers must work with their CAS to ensure all required classified storage repository documentation is appropriately retained with the CWS records.

SECURITY TIP: Some areas may implement more stringent monitoring policies. Talk to your CAS or VTR Custodian for your local processes.

The SF-702 form must be affixed to the outside of the GSA-approved safe's locking drawer or VTR door with a lock, or it must be in a conspicuous location nearby.

1.13 Required Repository Documentation



Notes:

REQUIRED REPOSITORY DOCUMENTATION

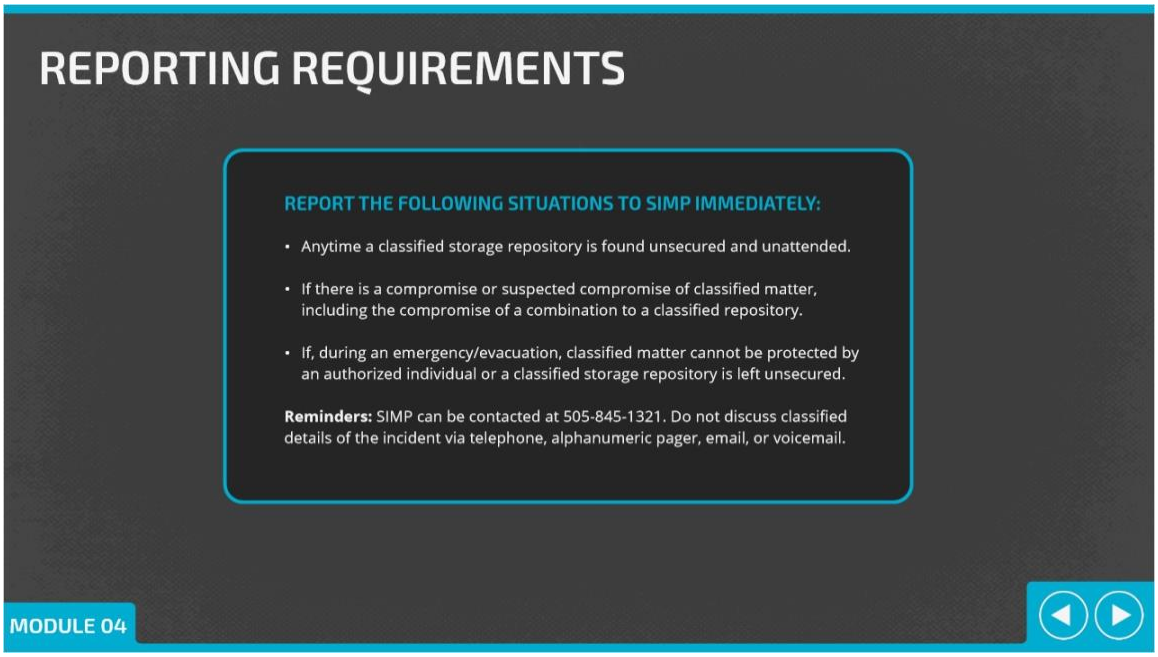
As a reminder, each lock on a classified storage repository must have the required CMPC documentation: SF-700, Security Container Information, and SF-702, Security Container Check Sheet.

In addition, all classified repositories with a spin-dial combination lock are required to have a Maintenance Record for Security Equipment form.

Contact your CAS or see the CWS Manual for additional classified storage repository and documentation requirements such as the following:

- How to change a spin-dial combination and when to use the factory default combination.
- What to do if only one drawer in a GSA-approved safe is used to store classified.
- How long the SF-700, SF-702, and Maintenance Record forms must be retained.

1.14 Reporting Requirements



Notes:

Reporting Requirements

REPORT THE FOLLOWING SITUATIONS TO SIMP IMMEDIATELY:

Anytime a classified storage repository is found unsecured and unattended.

If there is a compromise or suspected compromise of classified matter, including the compromise of a combination to a classified repository.

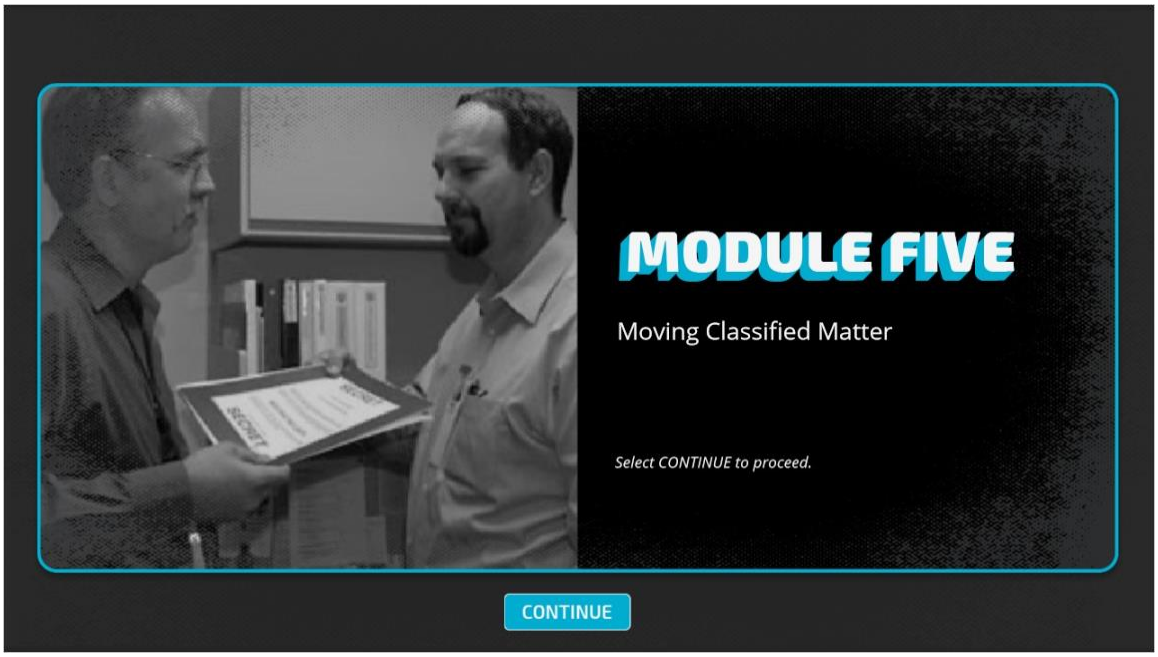
If, during an emergency/evacuation, classified matter cannot be protected by an authorized individual or a classified storage repository is left unsecured.

Reminders: SIMP can be contacted at 505-845-1321. Do not discuss classified details of the incident via telephone, alphanumeric pager, email, or voicemail.

SEC301: Module Five

1. Module Five

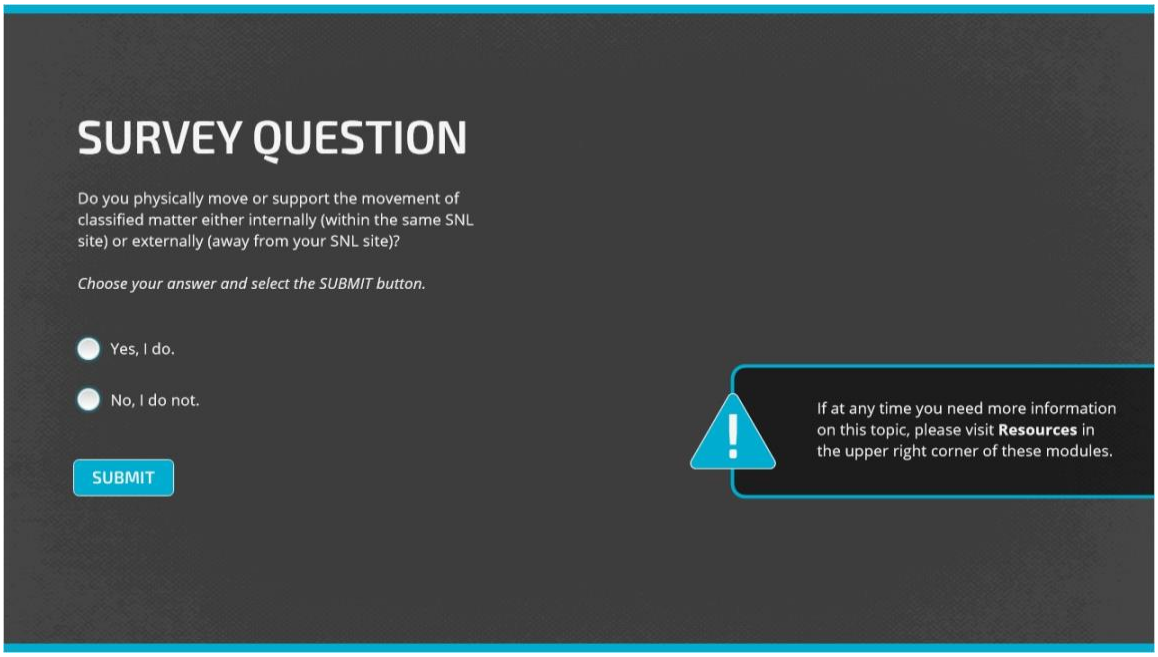
1.1 Module Introduction



Notes:

MODULE FIVE: Moving Classified Matter

1.2 Survey Question



Notes:

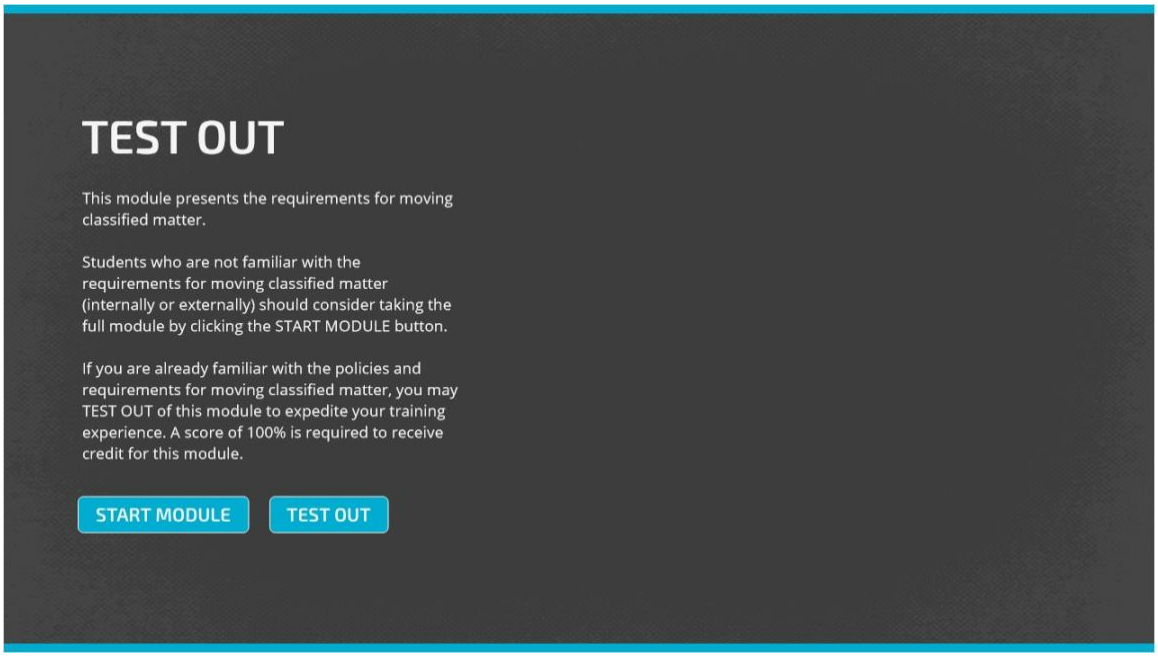
SURVEY QUESTION

Do you physically move or support the movement of classified matter either internally (within the same SNL site) or externally (away from your SNL site)?

Choose your answer and select the SUBMIT button.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option



Notes:

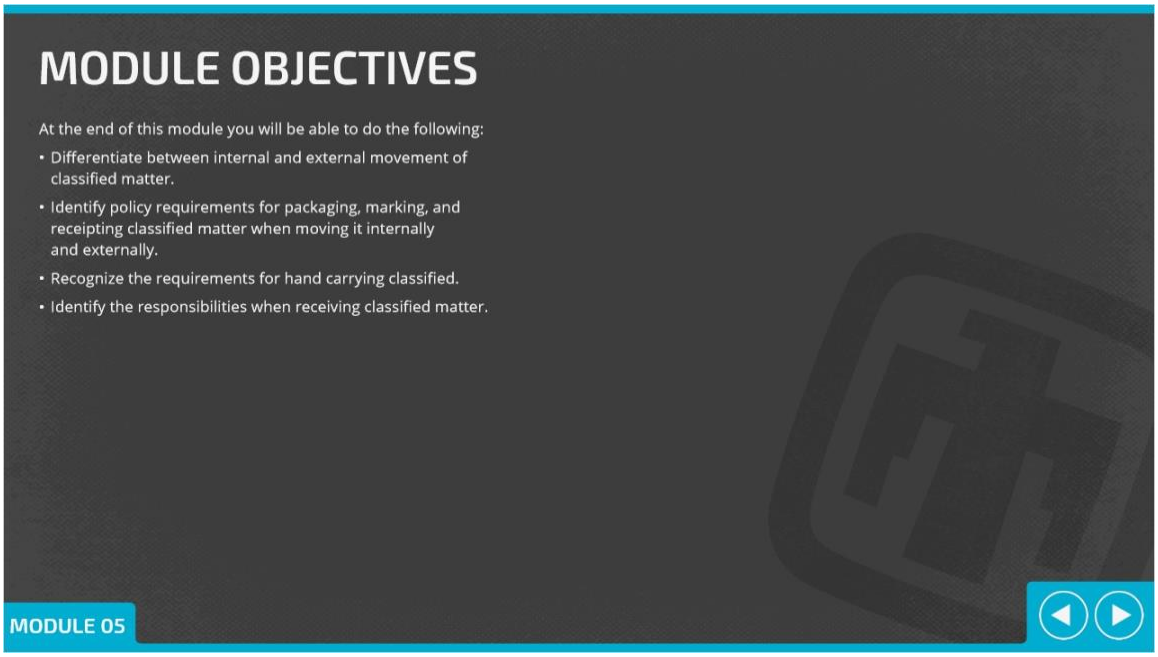
Test Out

This module presents the requirements for moving classified matter.

Students who are not familiar with the requirements for moving classified matter (internally or externally) should consider taking the full module by clicking the START MODULE button.

If you are already familiar with the policies and requirements for moving classified matter, you may TEST OUT of this module to expedite your training experience. A score of 100% is required to receive credit for this module.

1.4 Objectives

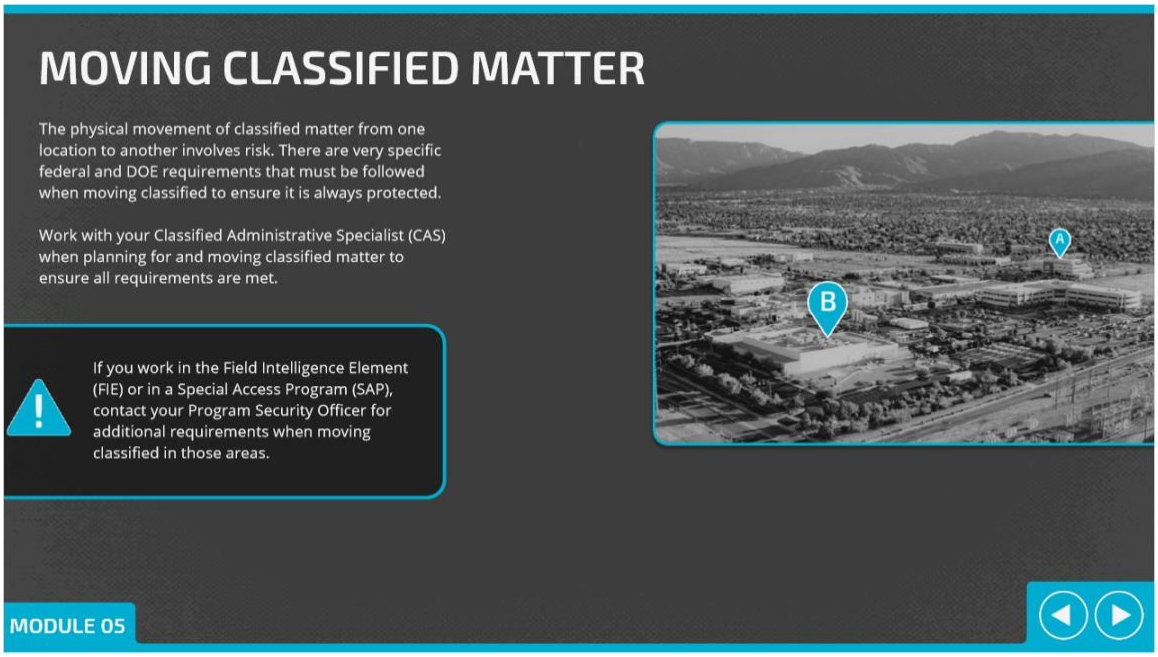


Notes:

Module Objectives

At the end of this module you will be able to do the following:
- Differentiate between internal and external movement of classified matter.
- Identify policy requirements for packaging, marking, and receipting classified matter when moving it internally and externally.
- Recognize the requirements for hand carrying classified.
- Identify the responsibilities when receiving classified matter.

1.5 Moving Classified Matter

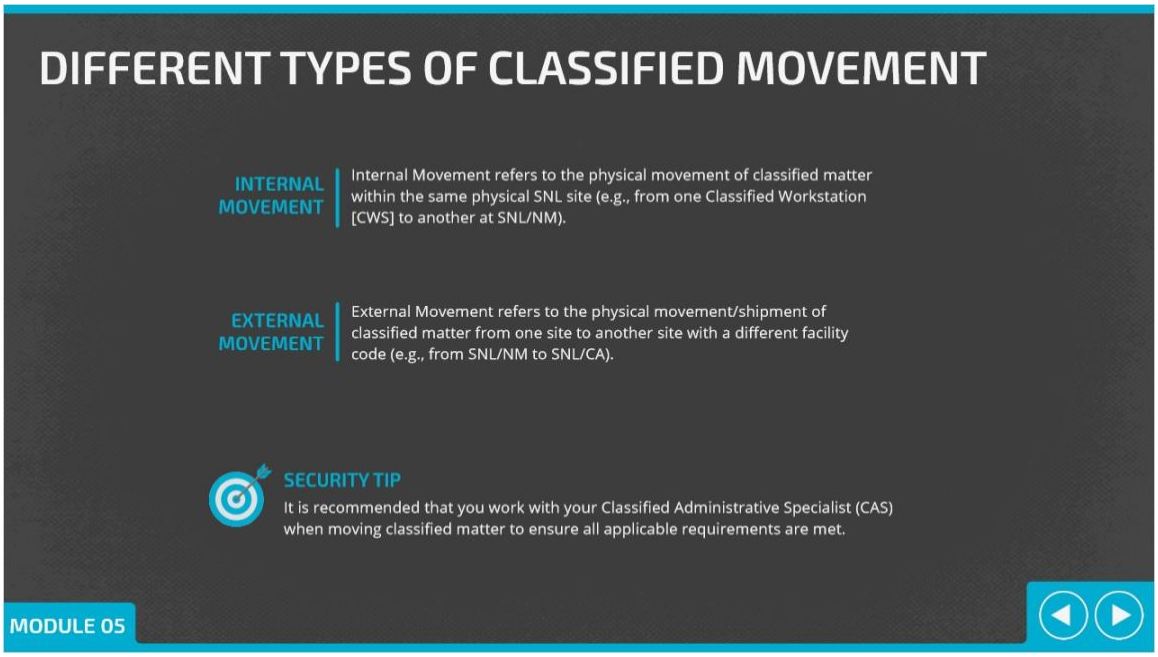


Notes:

MOVING CLASSIFIED MATTER

The physical movement of classified matter from one location to another involves risk. There are very specific federal and DOE requirements that must be followed when moving classified to ensure it is always protected.
Work with your Classified Administrative Specialist (CAS) when planning for and moving classified matter to ensure all requirements are met.
If you work in the Field Intelligence Element (FIE) or in a Special Access Program (SAP), contact your Program Security Officer for additional requirements when moving classified in those areas.

1.6 Different Types of Classified Matter



Notes:

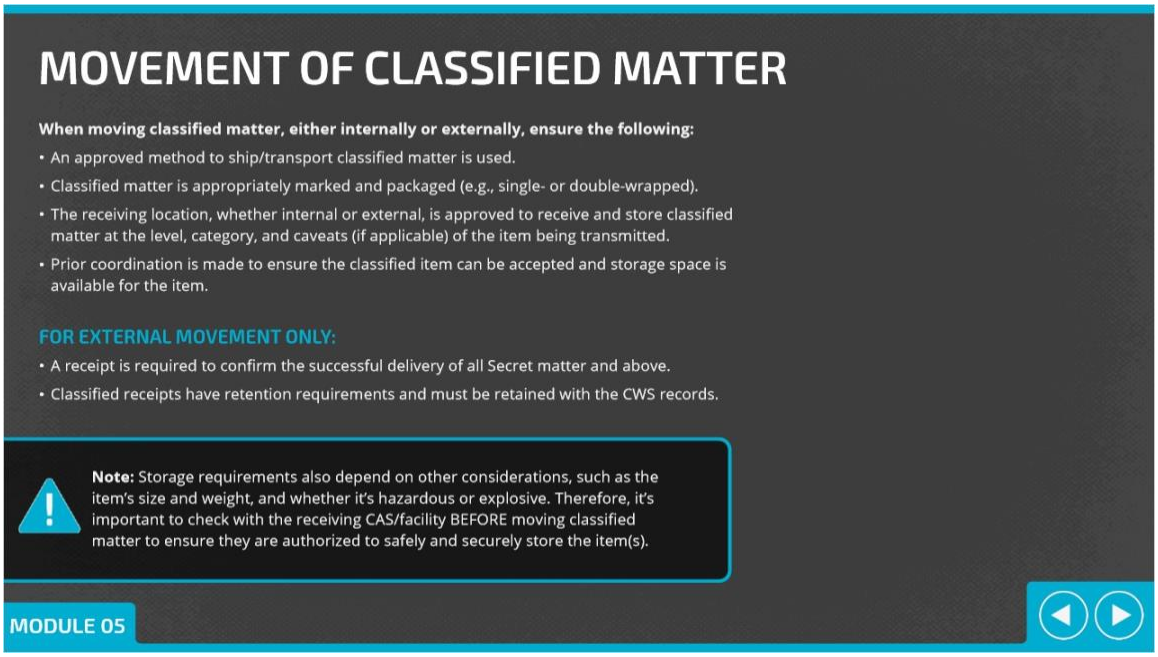
DIFFERENT TYPES OF CLASSIFIED MOVEMENT

Internal Movement refers to the physical movement of classified matter within the same physical SNL site (e.g., from one Classified Workstation [CWS] to another at SNL/NM).

External Movement refers to the physical movement/shipment of classified matter from one site to another site with a different facility code (e.g., from SNL/NM to SNL/CA).

SECURITY TIP: It is recommended that you work with your Classified Administrative Specialist (CAS) when moving classified matter to ensure all applicable requirements are met.

1.7 Movement of Classified Matter



Notes:

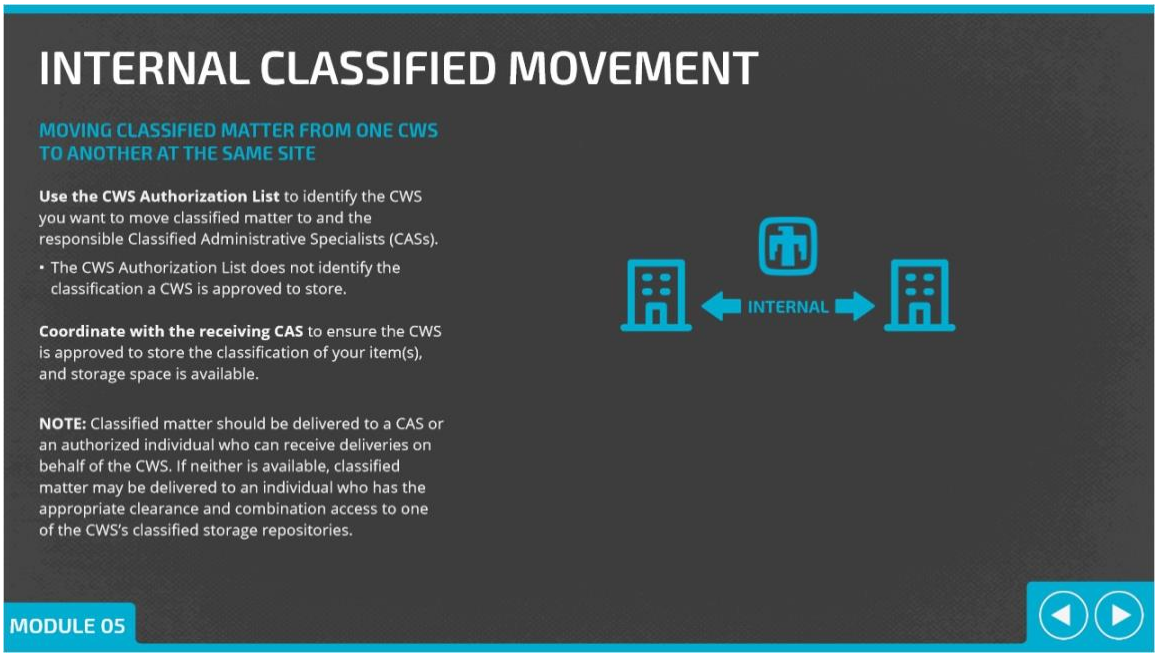
MOVEMENT OF CLASSIFIED MATTER

When moving classified matter, either internally or externally, ensure the following:
An approved method to ship/transport classified matter is used.
Classified matter is appropriately marked and packaged (e.g., single- or double-wrapped).
The receiving location, whether internal or external, is approved to receive and store classified matter at the level, category, and caveats (if applicable) of the item being transmitted.
Prior coordination is made to ensure the classified item can be accepted and storage space is available for the item.

For external movement only:
A receipt is required to confirm the successful delivery of all Secret matter and above.
Classified receipts have retention requirements and must be retained with the CWS records.

Note: Storage requirements also depend on other considerations, such as the item's size and weight, and whether it's hazardous or explosive. Therefore, it's important to check with the receiving CAS/facility BEFORE moving classified matter to ensure they are authorized to safely and securely store the item(s).

1.8 Internal Classified Movement



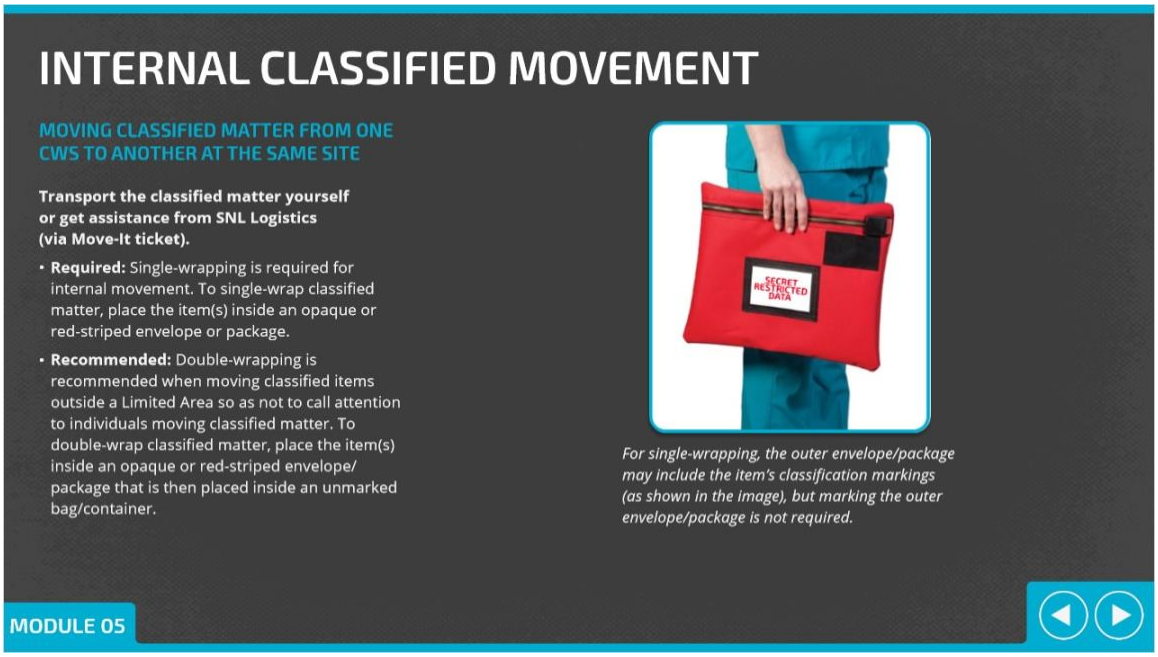
Notes:

INTERNAL CLASSIFIED MOVEMENT

MOVING CLASSIFIED MATTER FROM ONE CWS TO ANOTHER AT THE SAME SITE
Use the CWS Authorization List to identify the CWS you want to move classified matter to and the responsible Classified Administrative Specialists (CASs).
The CWS Authorization List does not identify the classification a CWS is approved to store.
Coordinate with the receiving CAS to ensure the CWS is approved to store the classification of your item(s), and storage space is available.

NOTE: Classified matter should be delivered to a CAS or an authorized individual who can receive deliveries on behalf of the CWS. If neither is available, classified matter may be delivered to an individual who has the appropriate clearance and combination access to one of the CWS's classified storage repositories.

1.9 Internal Classified Movement



Notes:

INTERNAL CLASSIFIED MOVEMENT

MOVING CLASSIFIED MATTER FROM ONE CWS TO ANOTHER AT THE SAME SITE

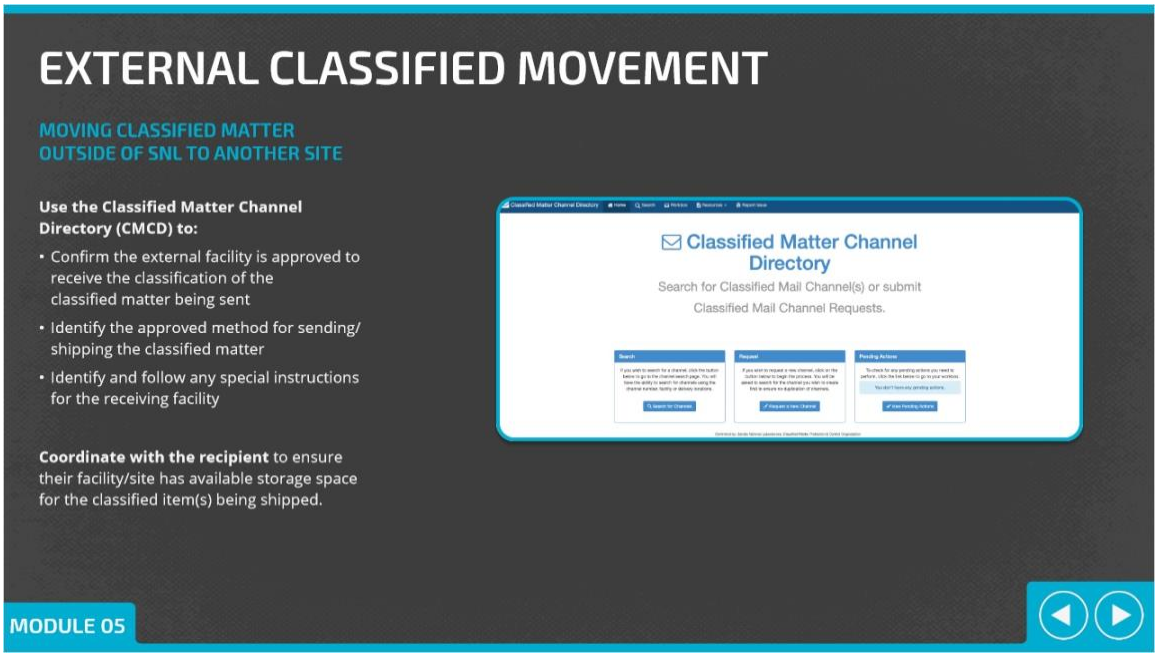
Transport the classified matter yourself or get assistance from SNL Logistics
(via Move-It ticket).

Required: Single-wrapping is required for internal movement. To single-wrap classified matter, place the item(s) inside an opaque or red-striped envelope or package.

Recommended: Double-wrapping is recommended when moving classified items outside a Limited Area so as not to call attention to individuals moving classified matter. To double-wrap classified matter, place the item(s) inside an opaque or red-striped envelope/package that is then placed inside an unmarked bag/container.

For single-wrapping, the outer envelope/package may include the item's classification markings (as shown in the image), but marking the outer envelope/package is not required.

1.10 External Classified Movement



Notes:

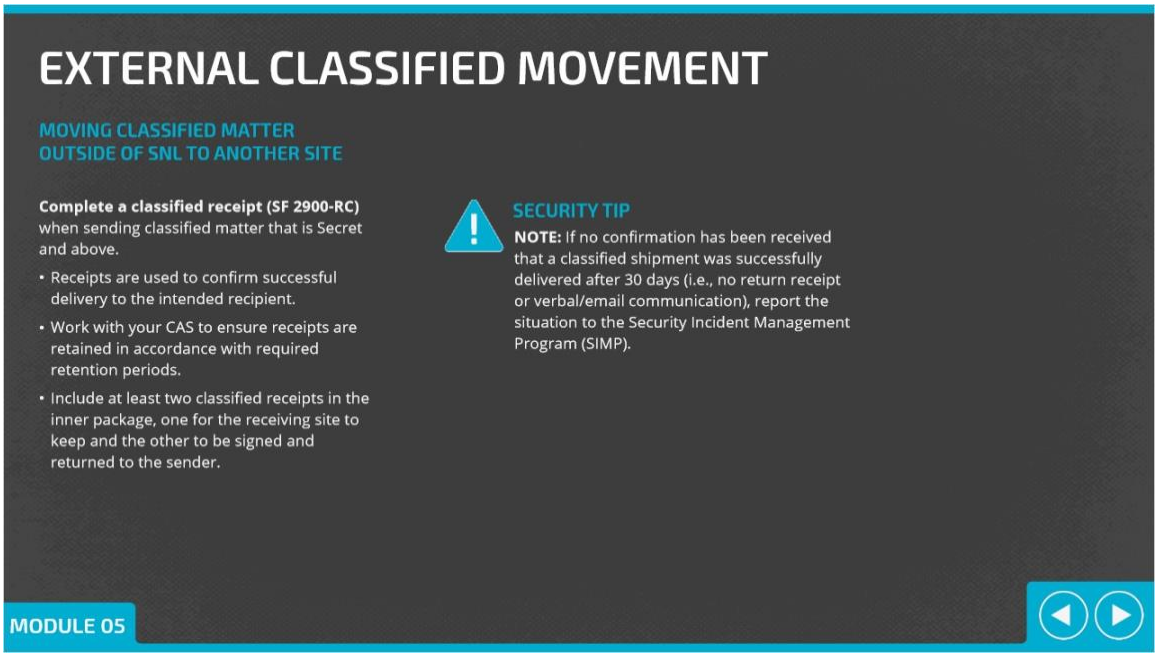
EXTERNAL CLASSIFIED MOVEMENT

MOVING CLASSIFIED MATTER OUTSIDE OF SNL TO ANOTHER SITE

Use the Classified Matter Channel Directory (CMCD) to:
- Confirm the external facility is approved to receive the classification of the classified matter being sent
- Identify the approved method for sending/shipping the classified matter
- Identify and follow any special instructions for the receiving facility

Coordinate with the recipient to ensure their facility/site has available storage space for the classified item(s) being shipped.

1.11 External Classified Movement



Notes:

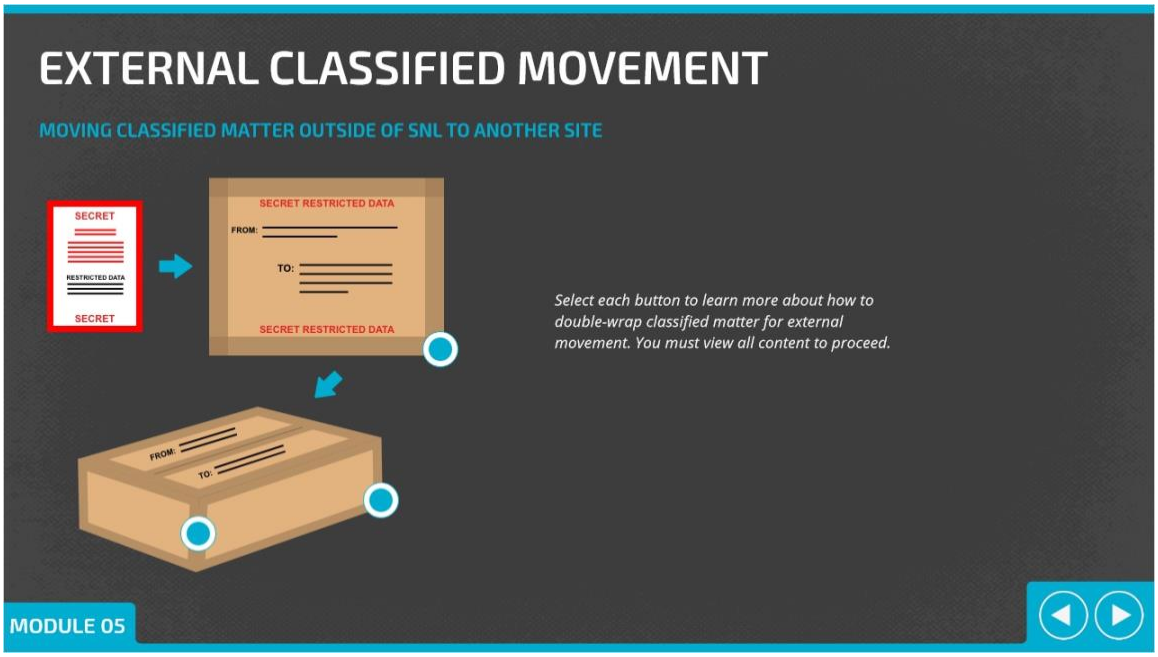
EXTERNAL CLASSIFIED MOVEMENT

MOVING CLASSIFIED MATTER OUTSIDE OF SNL TO ANOTHER SITE

Complete a classified receipt (SF 2900-RC) when sending classified matter that is Secret and above.
- Receipts are used to confirm successful delivery to the intended recipient.
- Work with your CAS to ensure receipts are retained in accordance with required retention periods.
- Include at least two classified receipts in the inner package, one for the receiving site to keep and the other to be signed and returned to the sender.

SECURITY TIP
NOTE: If no confirmation has been received that a classified shipment was successfully delivered after 30 days (i.e., no return receipt or verbal/email communication), report the situation to the Security Incident Management Program (SIMP).

1.12 External Classified Movement



Notes:

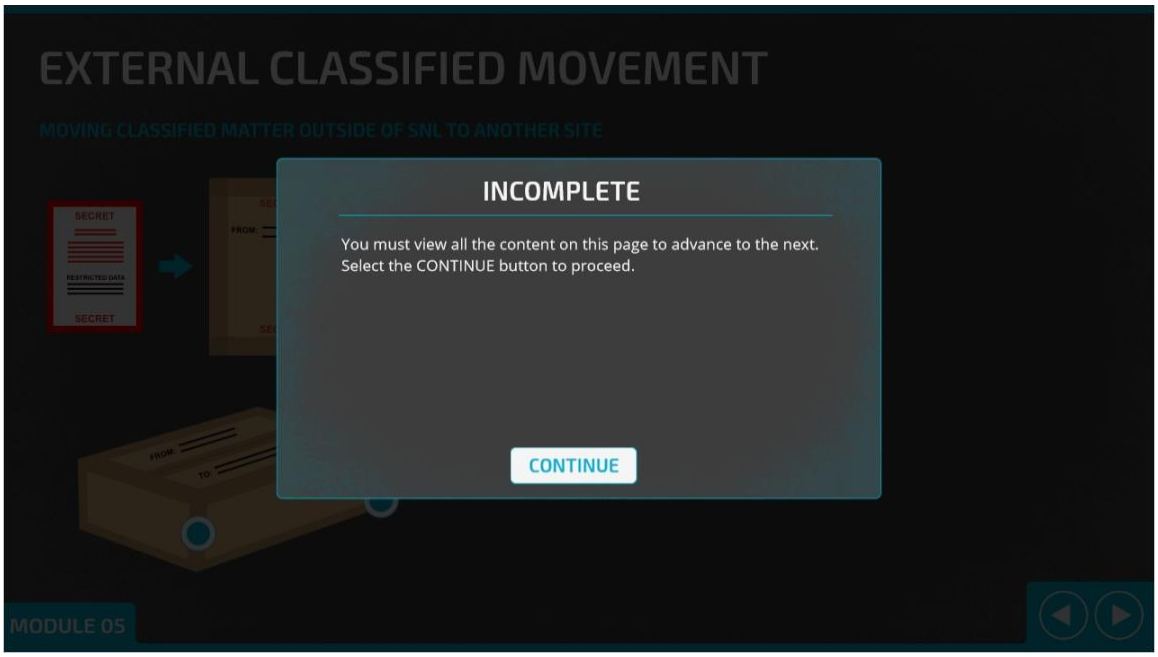
EXTERNAL CLASSIFIED MOVEMENT

Select each button to learn more about how to double-wrap classified matter for external movement. You must view all content to proceed.
Inner package: Before packaging classified matter, ensure all classified item(s) are marked and have the appropriate cover and backing sheets, if applicable. Place the item(s) inside an opaque envelope/package that is marked with the classification of the item inside the package. The envelope/package must contain the site's inner classified mailing address (taken from the CMCD).

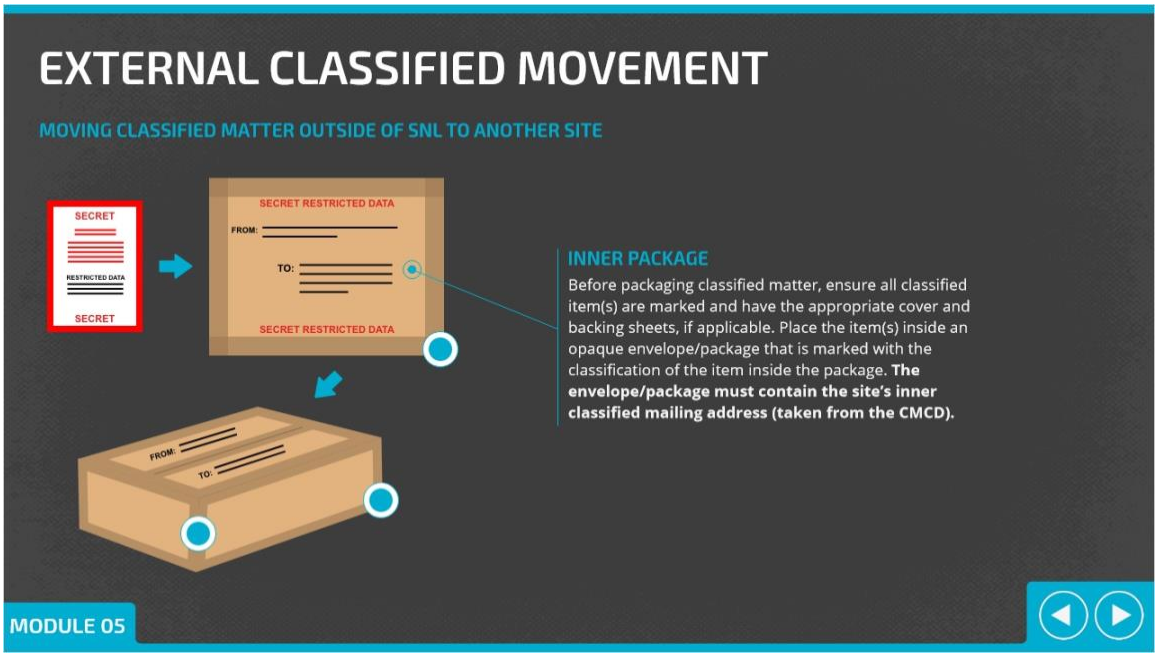
Outer package: Place the inner package inside a larger unmarked envelope/box that is sealed on all seams/edges.
The outer package must include the site's outer classified mailing address (taken from the CMCD).

Note: Inner and outer packages must be sealed on all sides/edges to provide tamper indication.

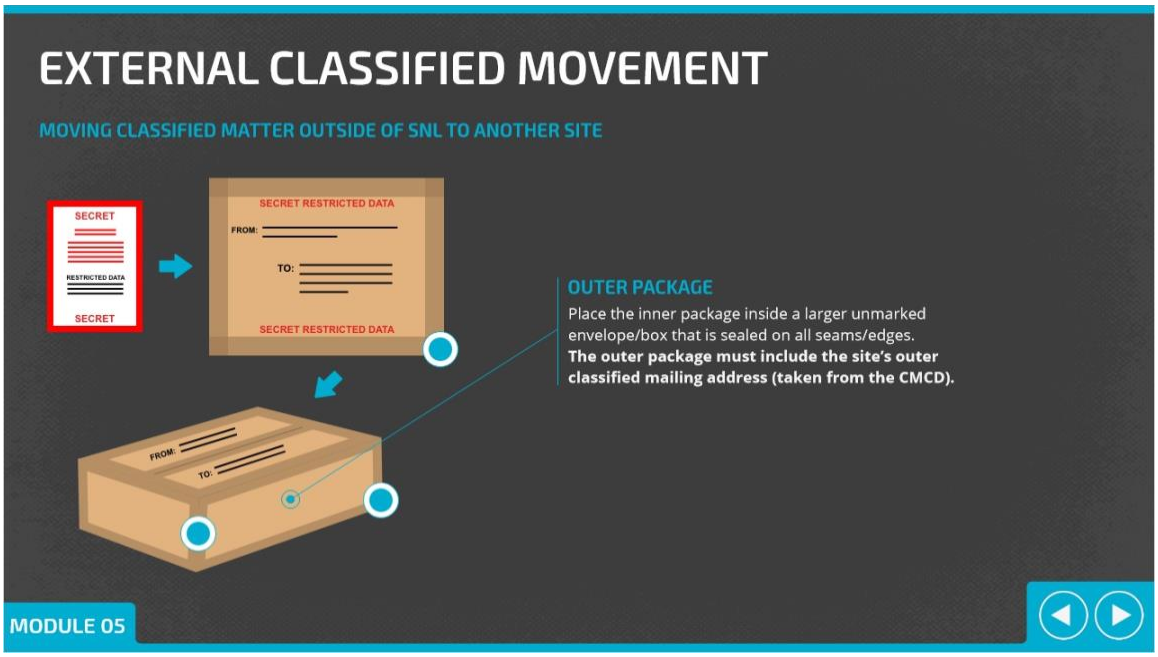
completion (Slide Layer)



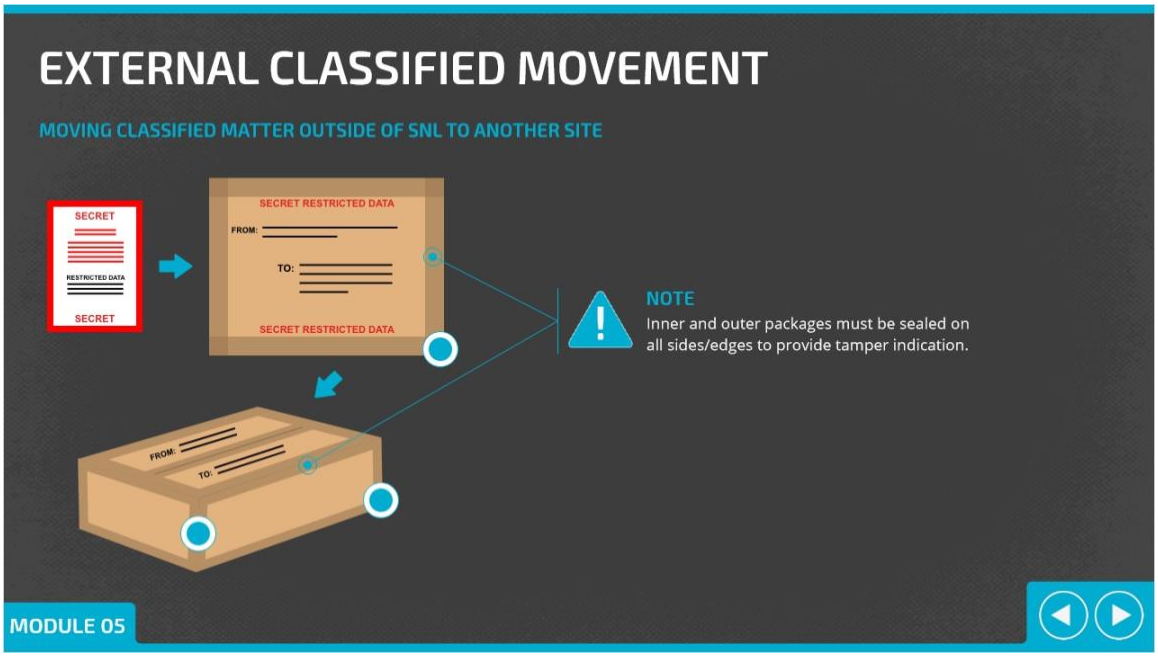
inner (Slide Layer)



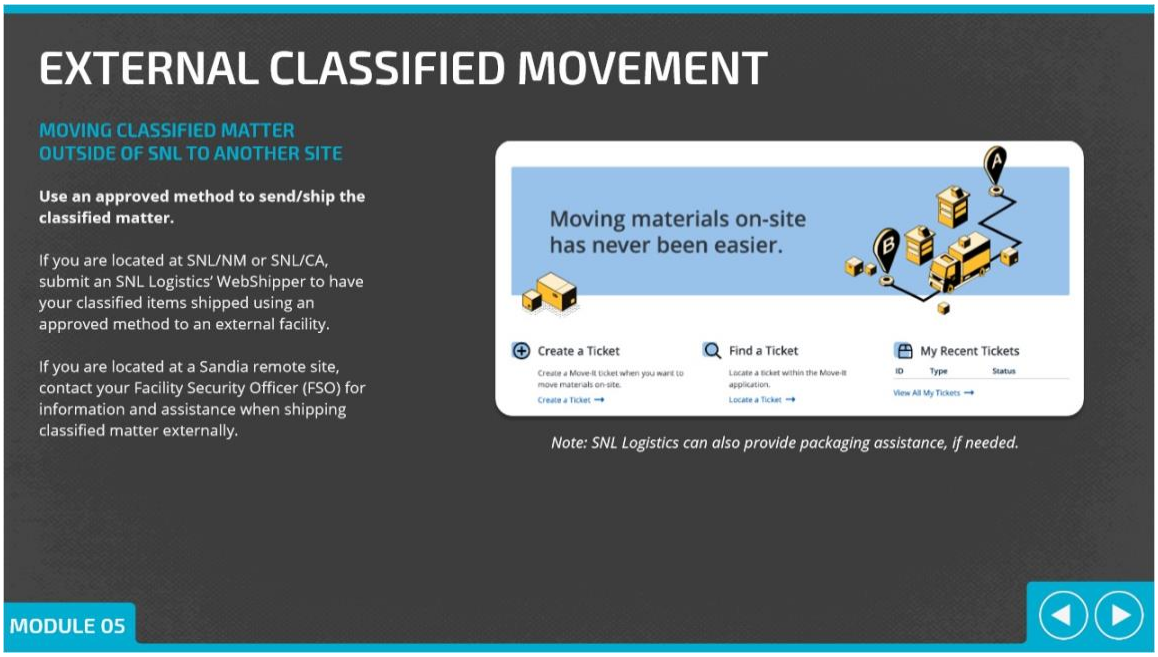
outer (Slide Layer)



note (Slide Layer)



1.13 External Classified Movement



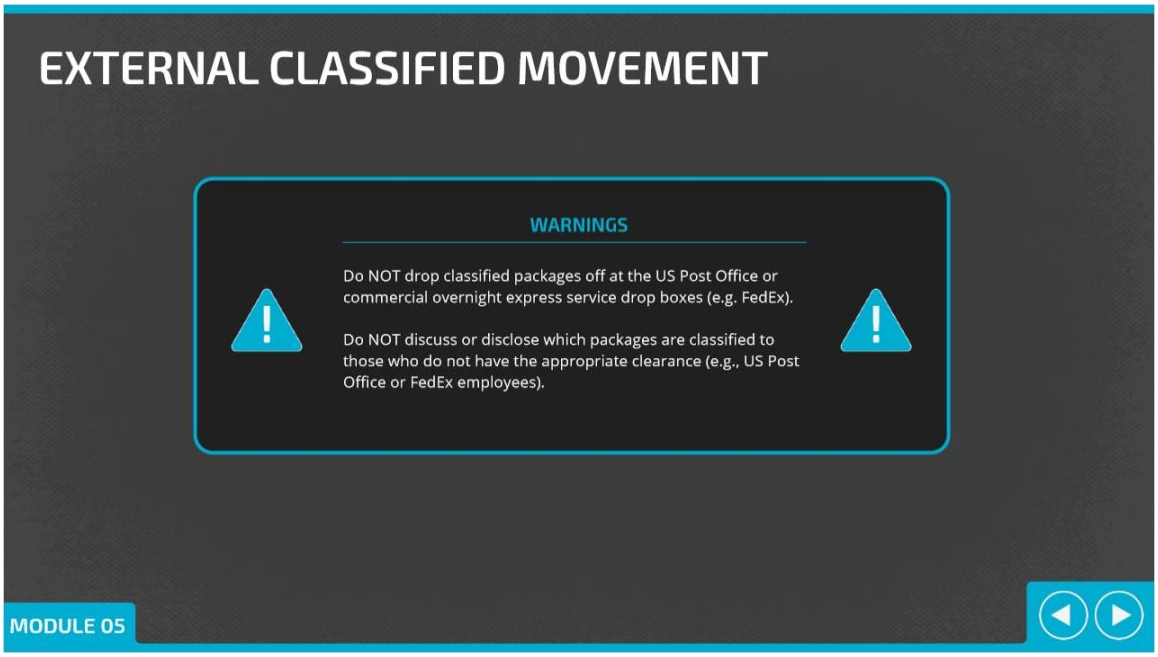
Notes:

External classified movement

MOVING CLASSIFIED MATTER OUTSIDE OF SNL TO ANOTHER SITE

Use an approved method to send/ship the classified matter.
If you are located at SNL/NM or SNL/CA, submit an SNL Logistics' WebShipper to have your classified items shipped using an approved method to an external facility.
If you are located at a Sandia remote site, contact your Facility Security Officer (FSO) for information and assistance when shipping classified matter externally.

1.14 External Classified Movement



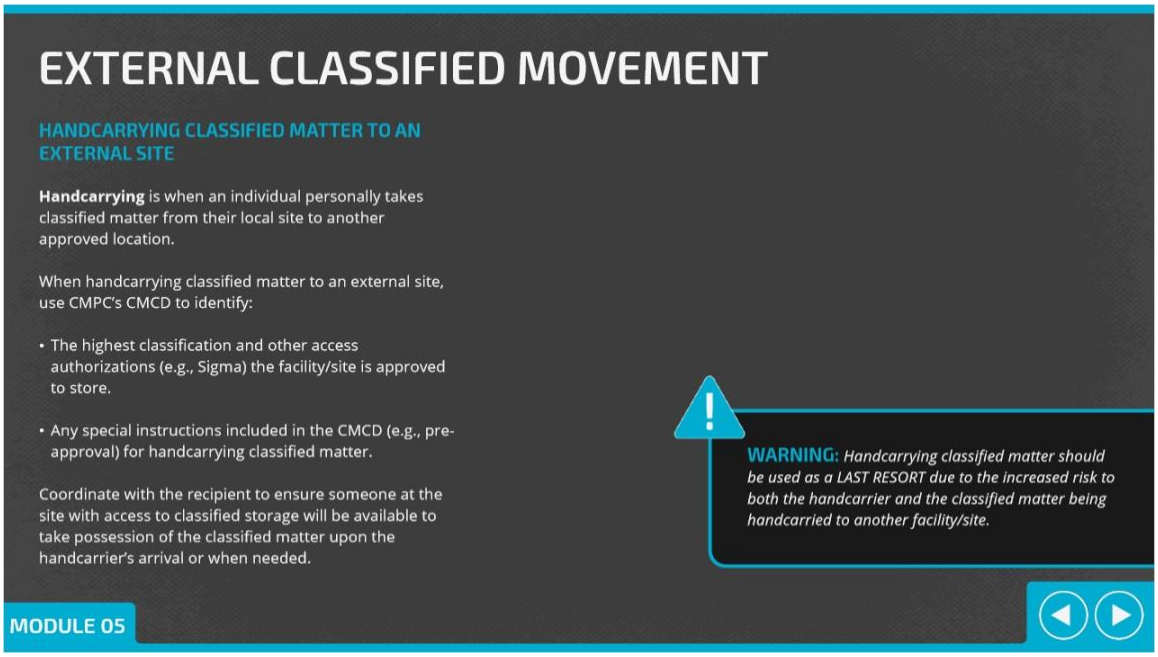
Notes:

EXTERNAL CLASSIFIED MOVEMENT

Warnings

Do NOT drop classified packages off at the US Post Office or commercial overnight express service drop boxes (e.g. FedEx).
Do NOT discuss or disclose which packages are classified to those who do not have the appropriate clearance (e.g., US Post Office or FedEx employees).

1.15 External Classified Movement- Handcarrying



Notes:

EXTERNAL CLASSIFIED MOVEMENT

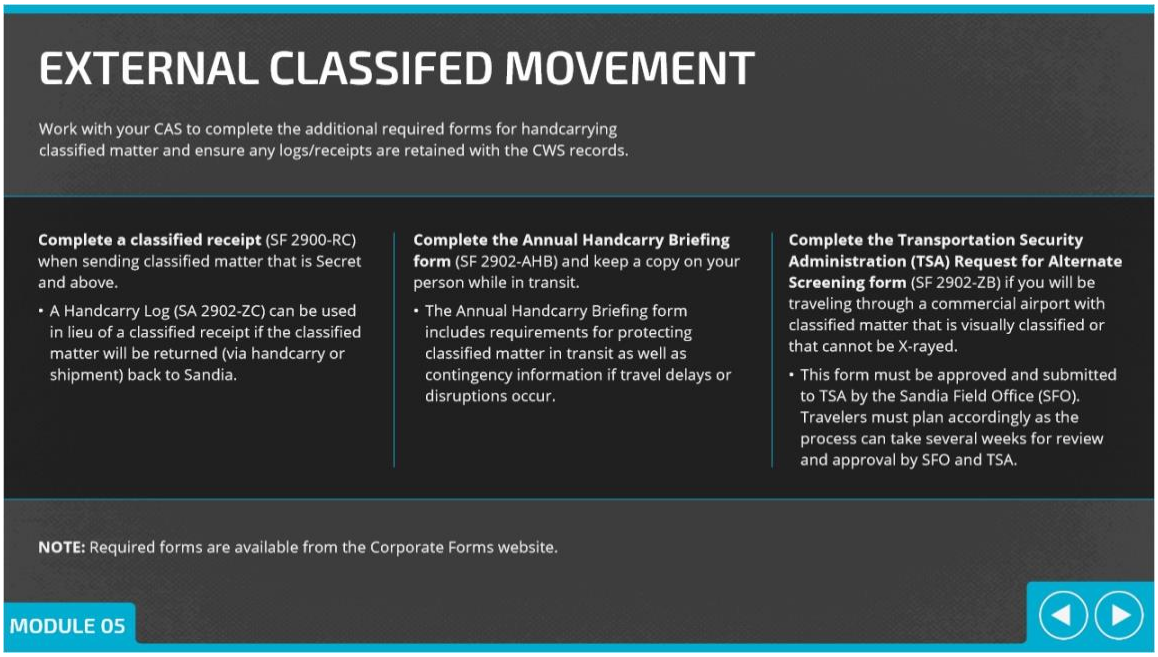
HANDCARRYING CLASSIFIED MATTER TO AN EXTERNAL SITE

Handcarrying is when an individual personally takes classified matter from their local site to another approved location.
When handcarrying classified matter to an external site, use CMPC's CMCD to identify:

Use CMPC's CMCD to identify:
The highest classification and other access authorizations (e.g., Sigma) the facility/site is approved to store.
Any special instructions included in the CMCD (e.g., pre-approval) for handcarrying classified matter.
Coordinate with the recipient to ensure someone at the site with access to classified storage will be available to take possession of the classified matter upon the handcarrier's arrival or when needed.

WARNING: Handcarrying classified matter should be used as a LAST RESORT due to the increased risk to both the handcarrier and the classified matter being handcarried to another facility/site.

1.16 External Classified Movement - Handcarrying



Notes:

EXTERNAL CLASSIFED MOVEMENT

Work with your CAS to complete the additional required forms for handcarrying
classified matter and ensure any logs/receipts are retained with the CWS records.

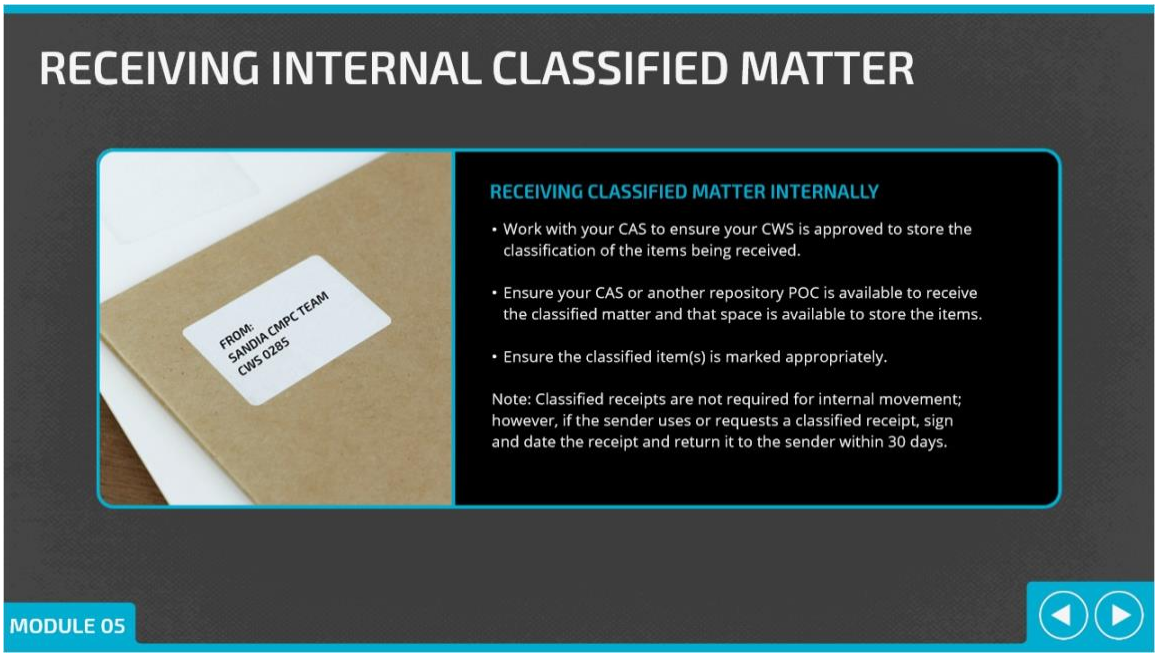
Complete a classified receipt (SF 2900-RC) when sending classified matter that is Secret and above.
- A Handcarry Log (SA 2902-ZC) can be used
  in lieu of a classified receipt if the classified matter will be returned (via handcarry or shipment) back to Sandia.

Complete the Annual Handcarry Briefing form (SF 2902-AHB) and keep a copy on your person while in transit.
- The Annual Handcarry Briefing form includes requirements for protecting classified matter in transit as well as contingency information if travel delays or disruptions occur.

Complete the Transportation Security Administration (TSA) Request for Alternate Screening form (SF 2902-ZB) if you will be traveling through a commercial airport with classified matter that is visually classified or that cannot be X-rayed.
- This form must be approved and submitted to TSA by the Sandia Field Office (SFO). Travelers must plan accordingly as the process can take several weeks for review and approval by SFO and TSA.

Note: Required forms are available from the Corporate Forms website.

1.17 Receiving Internal Classified Matter



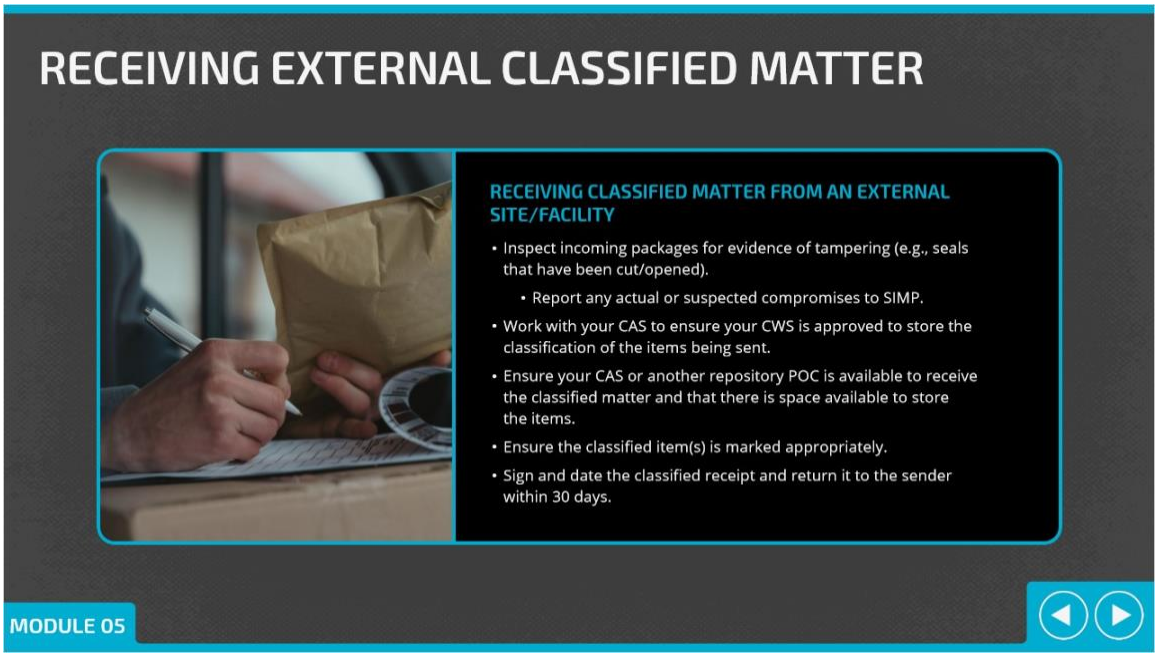
Notes:

RECEIVING INTERNAL CLASSIFIED MATTER

Receiving classified matter internally.

Work with your CAS to ensure your CWS is approved to store the classification of the items being received.
Ensure your CAS or another repository POC is available to receive the classified matter and that space is available to store the items.
Ensure the classified item(s) is marked appropriately.
Note: Classified receipts are not required for internal movement; however, if the sender uses or requests a classified receipt, sign and date the receipt and return it to the sender within 30 days.

1.18 Receiving External Classified Matter



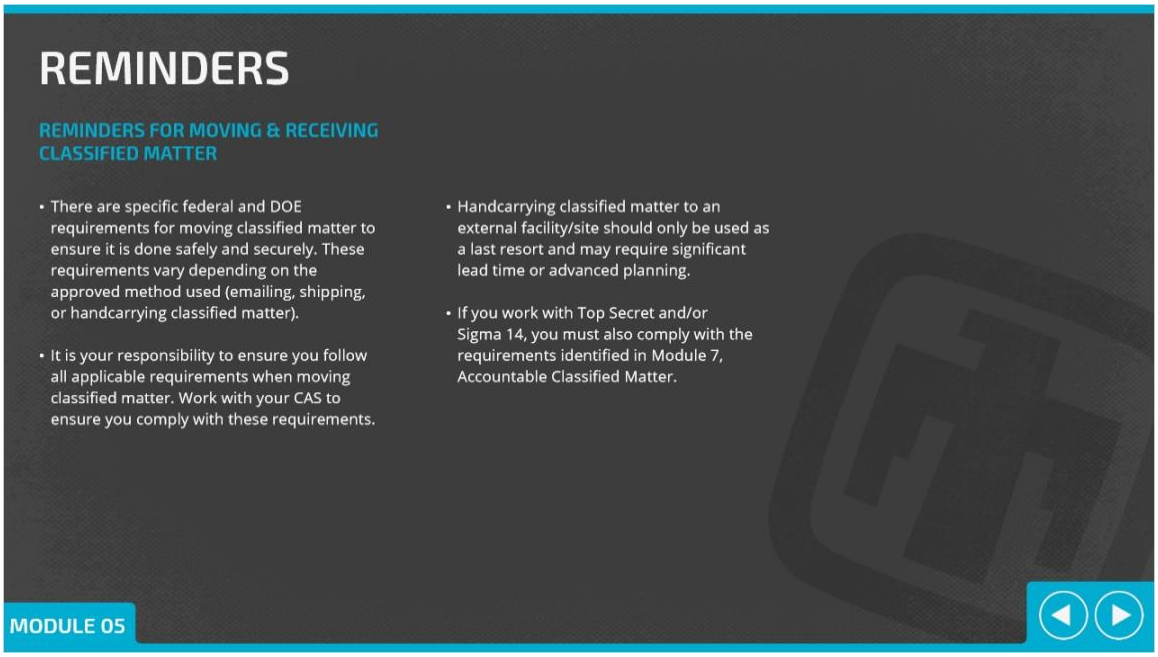
Notes:

RECEIVING EXTERNAL CLASSIFIED MATTER

RECEIVING CLASSIFIED MATTER FROM AN EXTERNAL SITE/FACILITY

- Inspect incoming packages for evidence of tampering (e.g., seals that have been cut/opened).
- Report any actual or suspected compromises to SIMP.
- Work with your CAS to ensure your CWS is approved to store the classification of the items being sent.
- Ensure your CAS or another repository POC is available to receive the classified matter and that there is space available to store
  the items.
- Ensure the classified item(s) is marked appropriately.
- Sign and date the classified receipt and return it to the sender within 30 days.

1.19 Reminders for Moving & Receiving Classified Matter



Notes:

REMINDERS

REMINDERS FOR MOVING & RECEIVING
CLASSIFIED MATTER

There are specific federal and DOE requirements for moving classified matter to ensure it is done safely and securely. These requirements vary depending on the approved method used (emailing, shipping, or handcarrying classified matter).
It is your responsibility to ensure you follow all applicable requirements when moving classified matter. Work with your CAS to ensure you comply with these requirements.

Handcarrying classified matter to an external facility/site should only be used as a last resort and may require significant lead time or advanced planning.
If you work with Top Secret and/or Sigma 14, you must also comply with the requirements identified in Module 7, Accountable Classified Matter.

1.20 Reporting Requirements



Notes:

REPORTING REQUIREMENTS

Report the following situations to SIMP immediately:

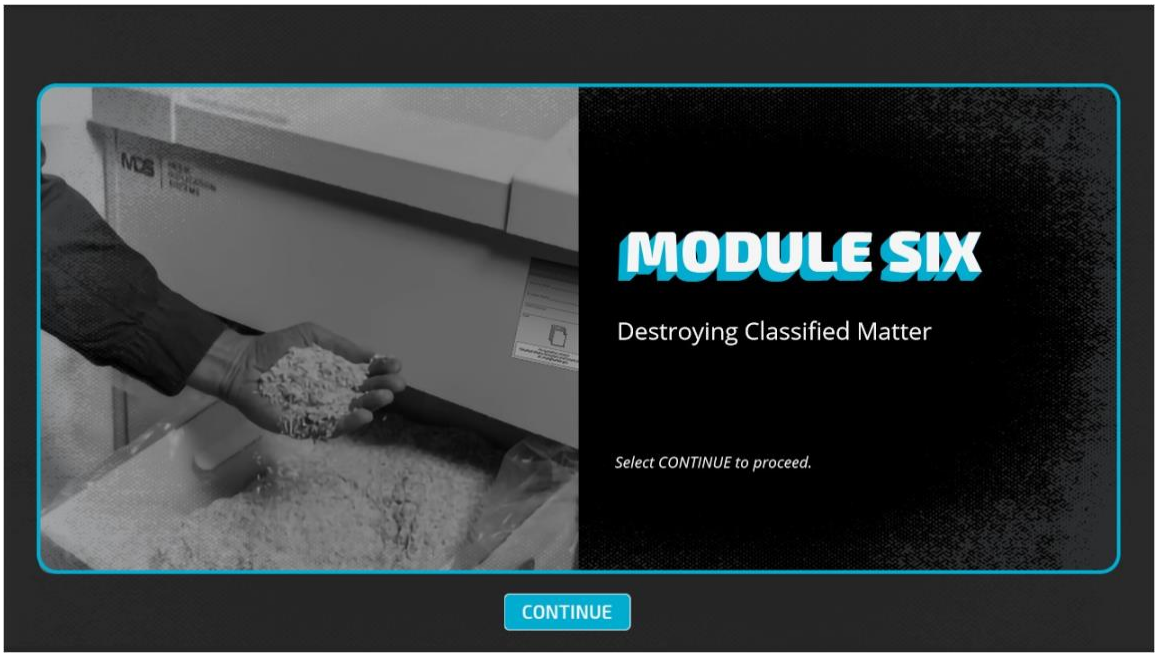
Anytime a classified package is not appropriately protected or is found unattended.
Anytime a classified package shows potential evidence of tampering (e.g., broken seals or intentional damage to the outer or inner layer of wrapping).
Anytime a classified shipment is lost or the location of a classified shipment is unknown after 30 days of being sent.
NOTE: When reporting, do not discuss details via telephone, alphanumeric pager, email, or voicemail.

Be on alert for potential evidence of tampering.

SEC301: Module Six

1. Module Six

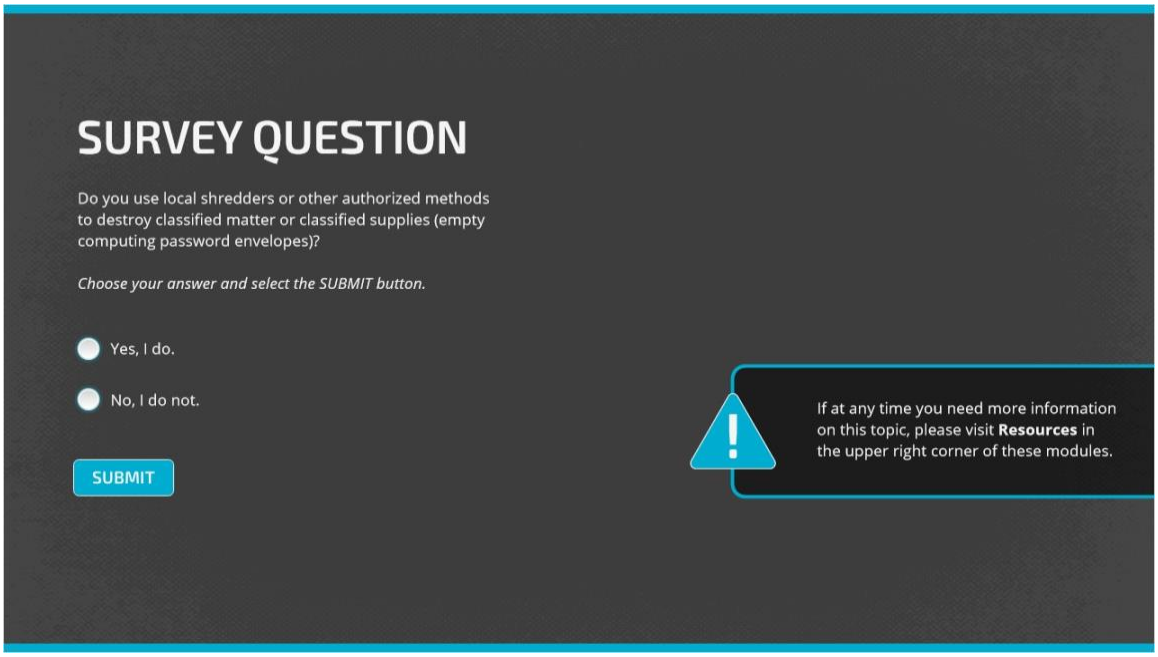
1.1 Module Introduction



Notes:

Module six: Destroying Classified Matter

1.2 Survey



Notes:

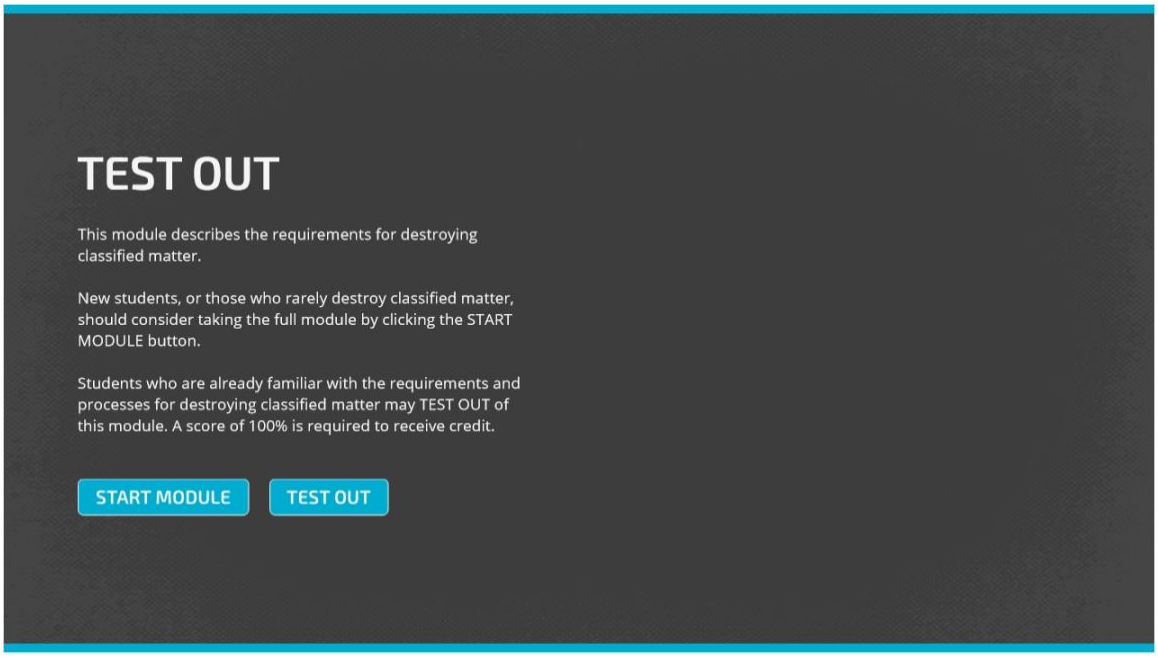
Survey Question:

Do you use local shredders or other authorized methods to destroy classified matter or classified supplies (empty computing password envelopes)?

Choose your answer and select the SUBMIT button.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option



Notes:

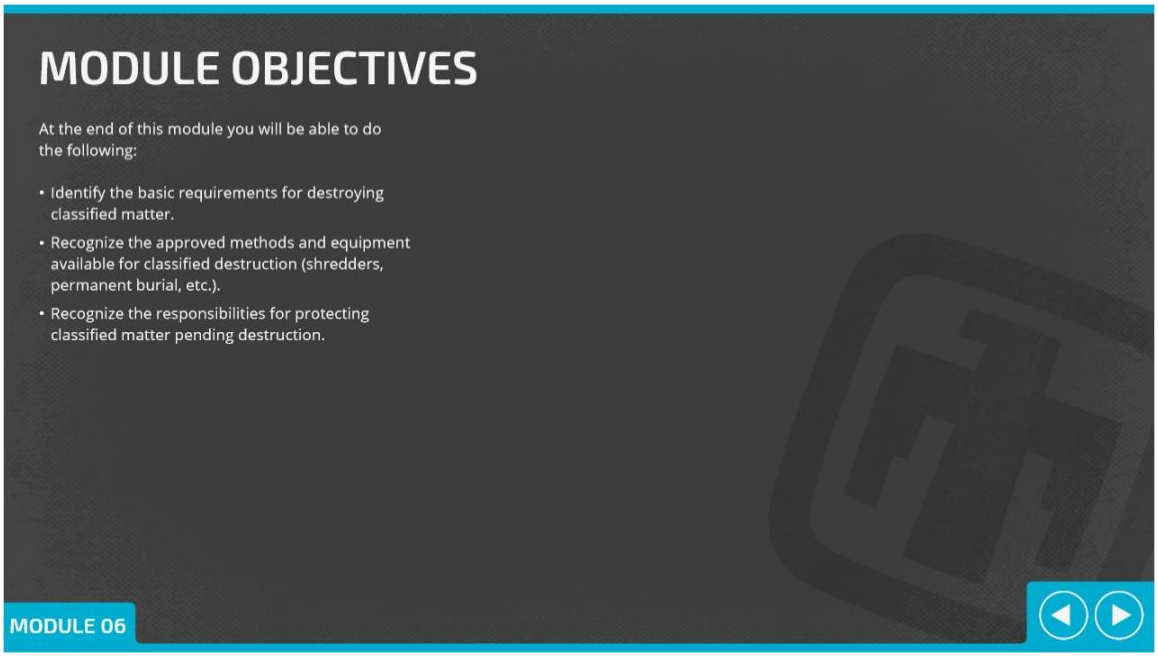
Test Out

This module describes the requirements for destroying classified matter.

New students, or those who rarely destroy classified matter, should consider taking the full module by clicking the START MODULE button.

Students who are already familiar with the requirements and processes for destroying classified matter may TEST OUT of this module. A score of 100% is required to receive credit.

1.4 Objectives



Notes:

Module Objectives

At the end of this module you will be able to do the following:

- Identify the basic requirements for destroying classified matter.
- Recognize the approved methods and equipment available for classified destruction (shredders, permanent burial, etc.).
- Recognize the responsibilities for protecting classified matter pending destruction.

1.5 Classified Destruction Requirements



Notes:

CLASSIFIED DESTRUCTION REQUIREMENTS

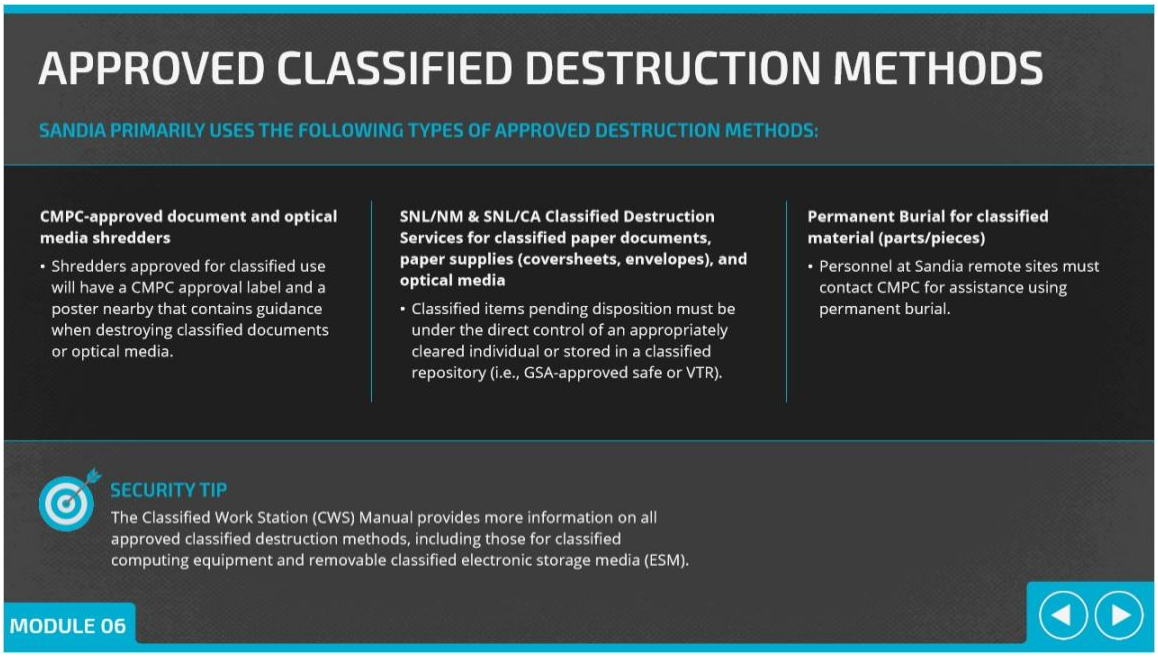
Per federal requirements, classified matter must be destroyed beyond recognition such that subsequent recovery or reconstruction of the matter is not permitted.

The destruction requirements vary depending on the type of classified matter being destroyed (e.g., documents, media, parts/pieces). Therefore, you must use an approved destruction method for your specific type of classified matter.

Classified items pending disposition must be under the direct control of an appropriately cleared individual or stored in a classified repository (i.e., GSA-approved safe or vault-type room [VTR]). They must never be left unattended.

SECURITY TIP:
Accountable classified matter (e.g., Top Secret, Designated UK matter) has additional destruction requirements, which are detailed in Module Seven.

1.6 Approved Classified Destruction Methods



Notes:

APPROVED CLASSIFIED DESTRUCTION METHODS

SANDIA PRIMARILY USES THE FOLLOWING TYPES OF APPROVED DESTRUCTION METHODS:

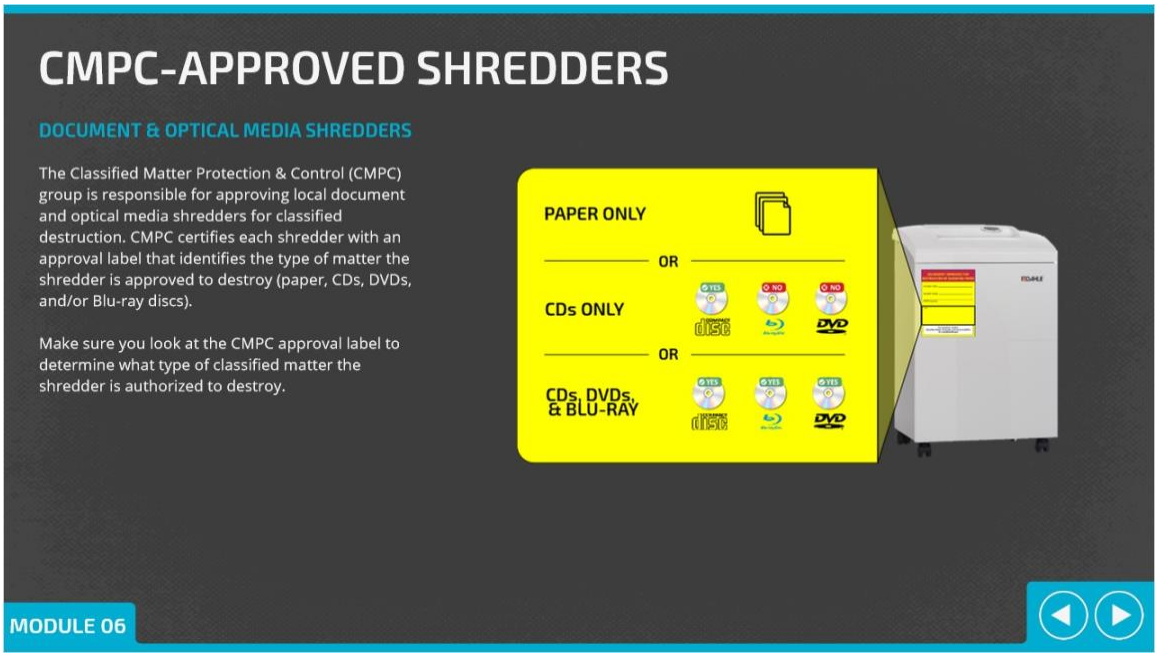
CMPC-approved document and optical media shredders.
Shredders approved for classified use will have a CMPC approval label and a poster nearby that contains guidance when destroying classified documents or optical media.

SNL/NM & SNL/CA Classified Destruction Services for classified paper documents, paper supplies (coversheets, envelopes), and optical media.
Classified items pending disposition must be under the direct control of an appropriately cleared individual or stored in a classified repository (i.e., GSA-approved safe or VTR).

Permanent Burial for classified material (parts/pieces).
Personnel at Sandia remote sites must contact CMPC for assistance using permanent burial.

SECURITY TIP:
The Classified Work Station (CWS) Manual provides more information on all approved classified destruction methods, including those for classified computing equipment and removable classified electronic storage media (ESM).

1.7 CMPC-Approved Document and Optical Media Shredders



Notes:

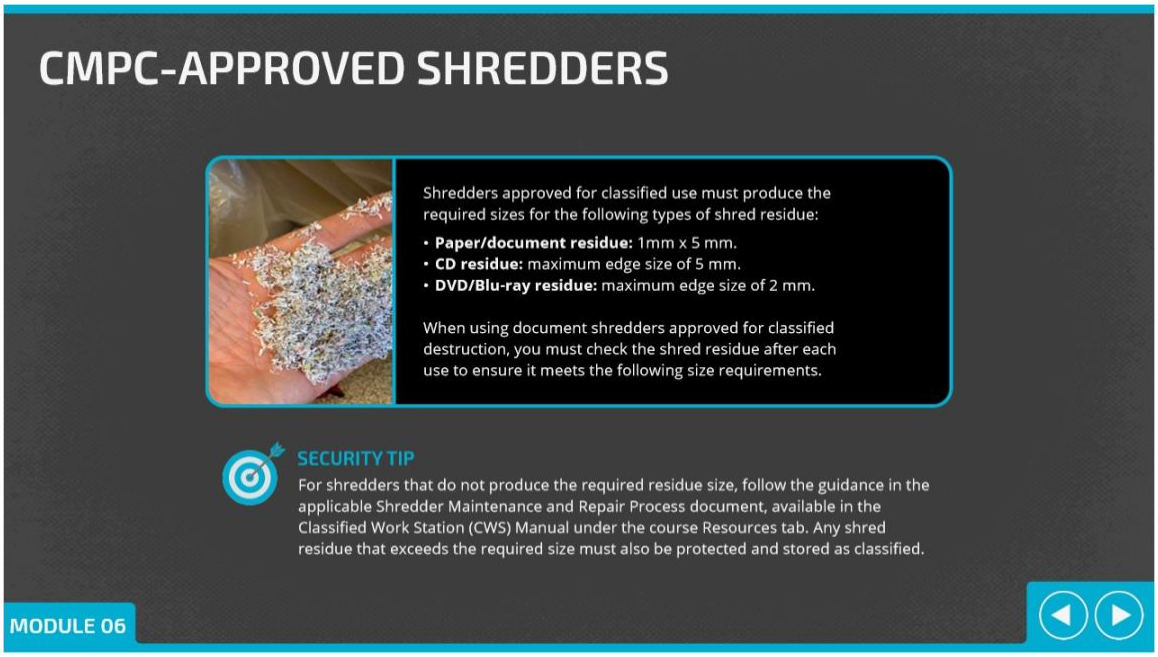
CMPC-APPROVED SHREDDERS

DOCUMENT & OPTICAL MEDIA SHREDDERS

The Classified Matter Protection & Control (CMPC) group is responsible for approving local document and optical media shredders for classified destruction. CMPC certifies each shredder with an approval label that identifies the type of matter the shredder is approved to destroy (paper, CDs, DVDs, and/or Blu-ray discs).

Make sure you look at the CMPC approval label to determine what type of classified matter the shredder is authorized to destroy.

1.8 CMPC-Approved Document and Optical Media Shredders



Notes:

CMPC-APPROVED SHREDDERS

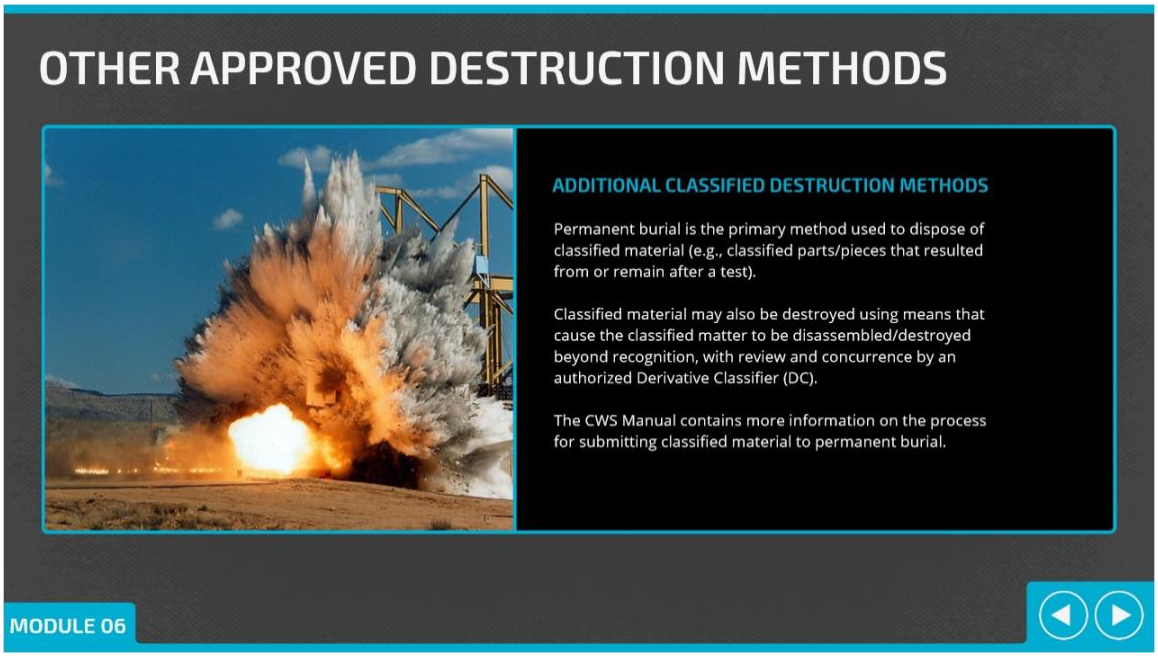
Shredders approved for classified use must produce the required sizes for the following types of shred residue:

- Paper/document residue: 1mm x 5 mm.
- CD residue: maximum edge size of 5 mm.
- DVD/Blu-ray residue: maximum edge size of 2 mm.

When using document shredders approved for classified destruction, you must check the shred residue after each use to ensure it meets the following size requirements.

Security tip: For shredders that do not produce the required residue size, follow the guidance in the applicable Shredder Maintenance and Repair Process document, available in the Classified Work Station (CWS) Manual under the course Resources tab. Any shred residue that exceeds the required size must also be protected and stored as classified.

1.9 OtherApproved Classified Destruction Methods



Notes:

OTHER APPROVED CLASSIFIED

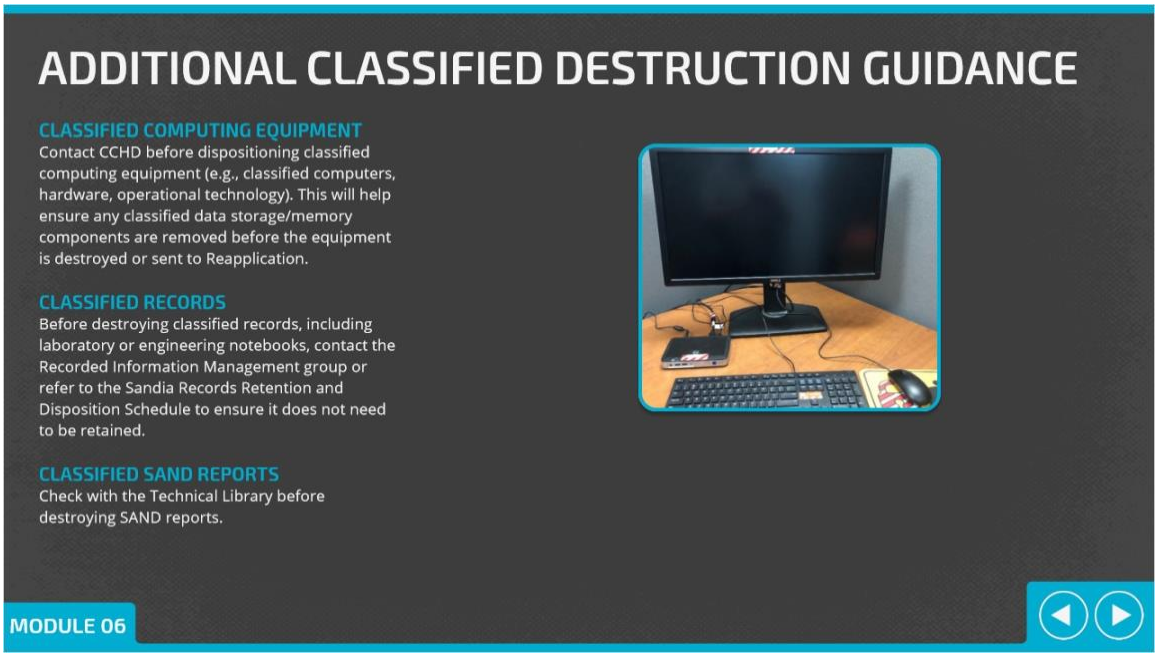
DESTRUCTION METHODS

Permanent burial is the primary method used to dispose of classified material (e.g., classified parts/pieces that resulted from or remain after a test).

Classified material may also be destroyed using means that cause the classified matter to be disassembled/destroyed beyond recognition, with review and concurrence by an authorized Derivative Classifier (DC).

The CWS Manual contains more information on the process for submitting classified material to permanent burial.

1.10 Additional Classified Destruction Guidance



Notes:

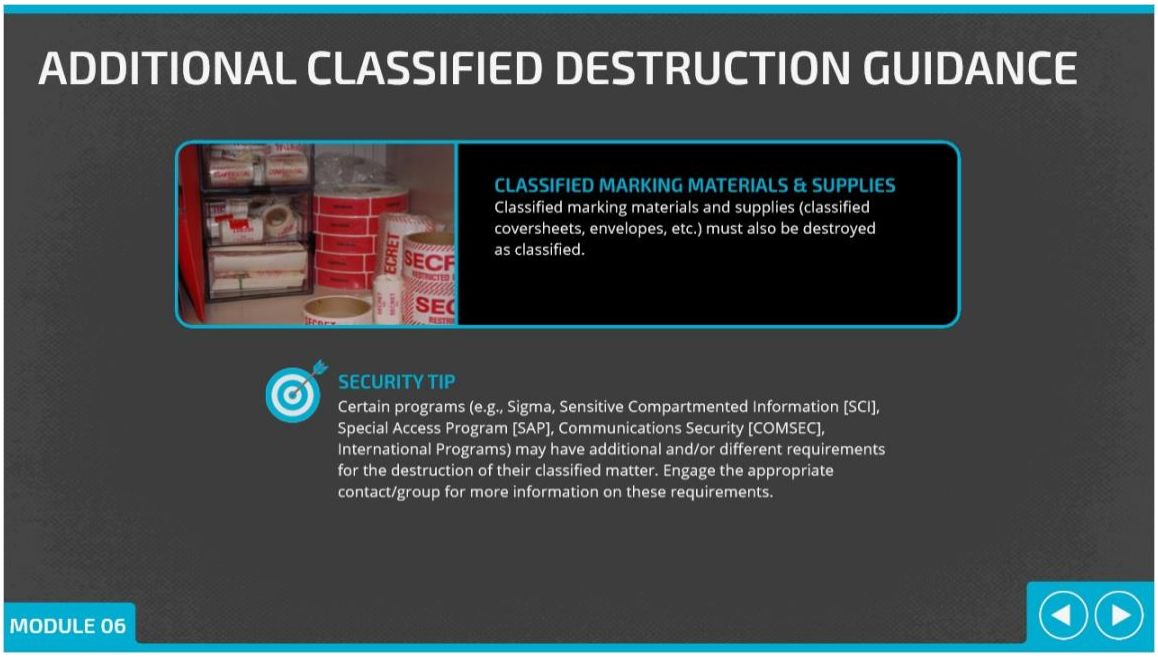
ADDITIONAL CLASSIFIED DESTRUCTION GUIDANCE

CLASSIFIED COMPUTING EQUIPMENT
Contact CCHD before dispositioning classified computing equipment (e.g., classified computers, hardware, operational technology). This will help ensure any classified data storage/memory components are removed before the equipment is destroyed or sent to Reapplication.

CLASSIFIED RECORDS
Before destroying classified records, including laboratory or engineering notebooks, contact the Recorded Information Management group or refer to the Sandia Records Retention and Disposition Schedule to ensure it does not need to be retained.

CLASSIFIED SAND REPORTS
Check with the Technical Library before destroying SAND reports.

1.11 Additional Classified Destruction Guidance



Notes:

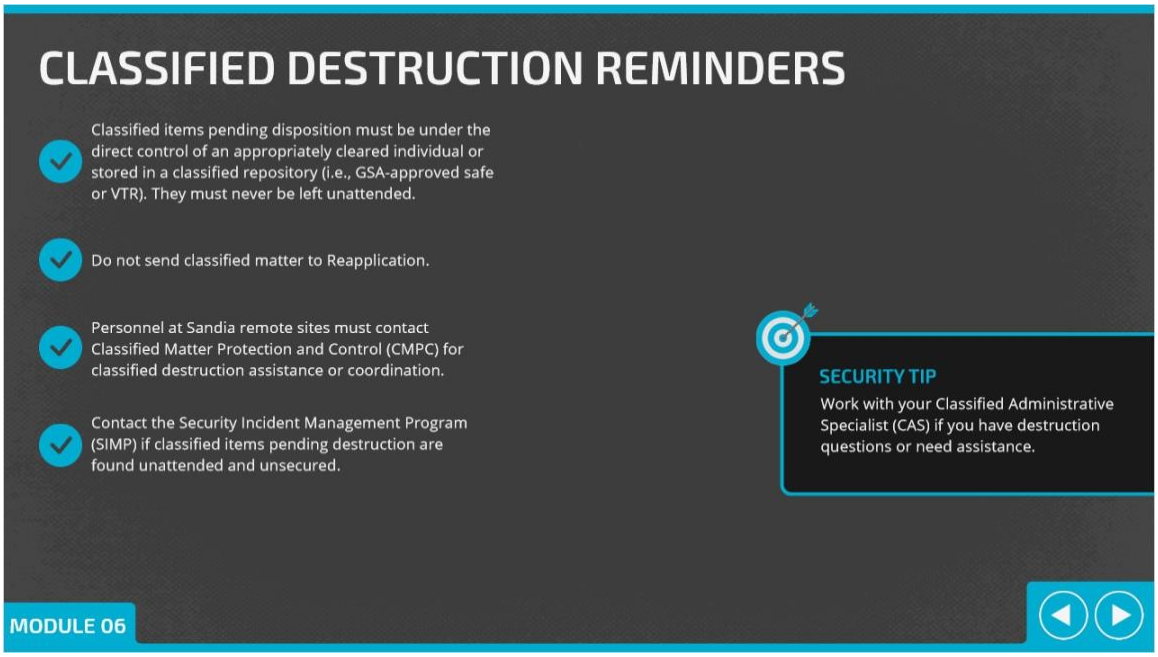
ADDITIONAL CLASSIFIED DESTRUCTION GUIDANCE

CLASSIFIED MARKING MATERIALS & SUPPLIES

Classified marking materials and supplies (classified coversheets, envelopes, etc.) must also be destroyed as classified.

SECURITY TIP: Certain programs (e.g., Sigma, Sensitive Compartmented Information [SCI], Special Access Program [SAP], Communications Security [COMSEC], International Programs) may have additional and/or different requirements for the destruction of their classified matter. Engage the appropriate contact/group for more information on these requirements.

1.12 Final Takeaways



Notes:

Header: Safeguards and Security.

Classified items pending disposition must be under the direct control of an appropriately cleared individual or stored in a classified repository (i.e., GSA-approved safe or VTR). They must never be left unattended.

Do not send classified matter to Reapplication.

Personnel at Sandia remote sites must contact Classified Matter Protection and Control (CMPC) for classified destruction assistance or coordination.

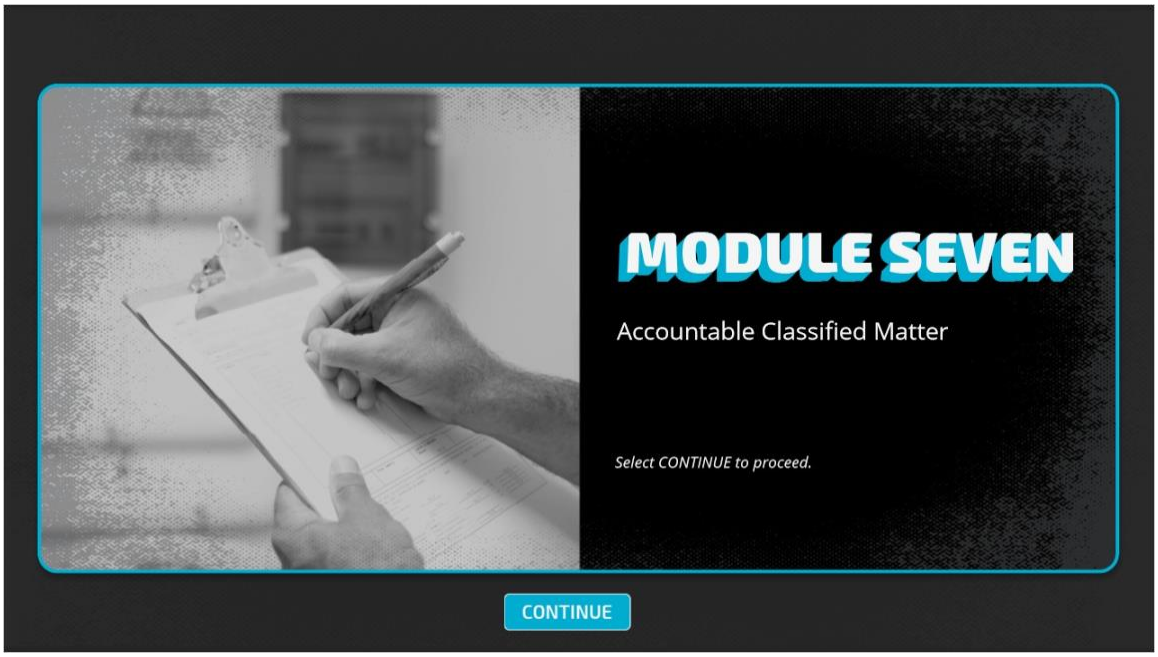
Contact the Security Incident Management Program (SIMP) if classified items pending destruction are found unattended and unsecured.

SECURITY TIP: Work with your Classified Administrative Specialist (CAS) if you have destruction questions or need assistance.

SEC301: Module Seven

1. Module Seven

1.1 Module Introduction

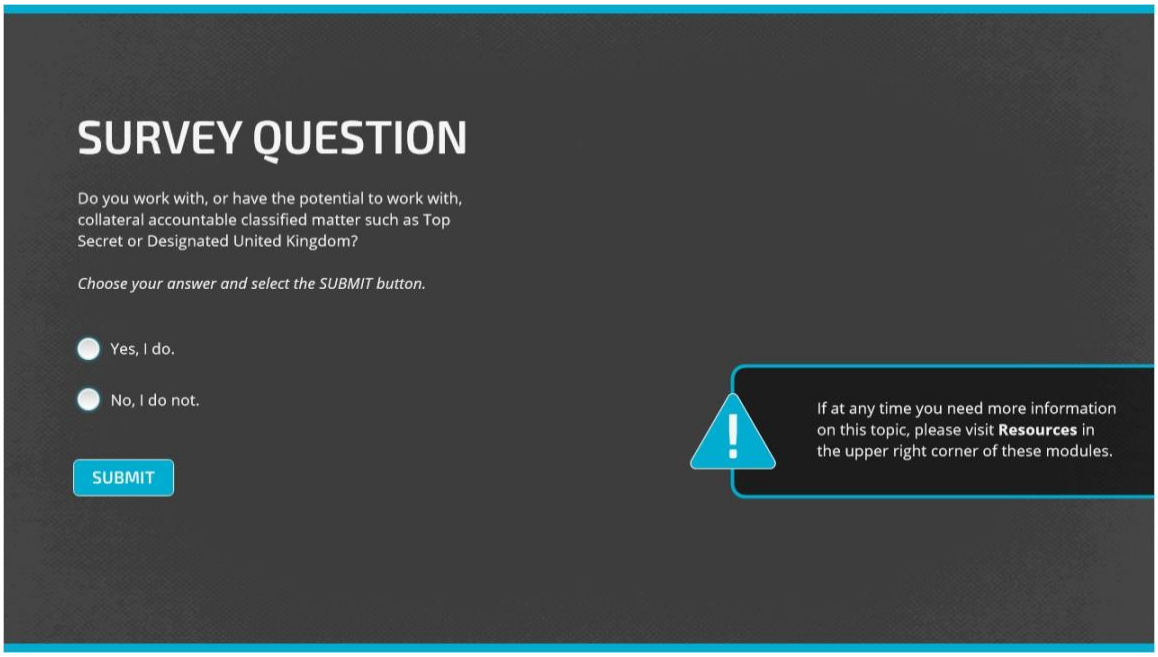


Notes:

Module seven

Accountable Classified Matter

1.2 Survey



Notes:

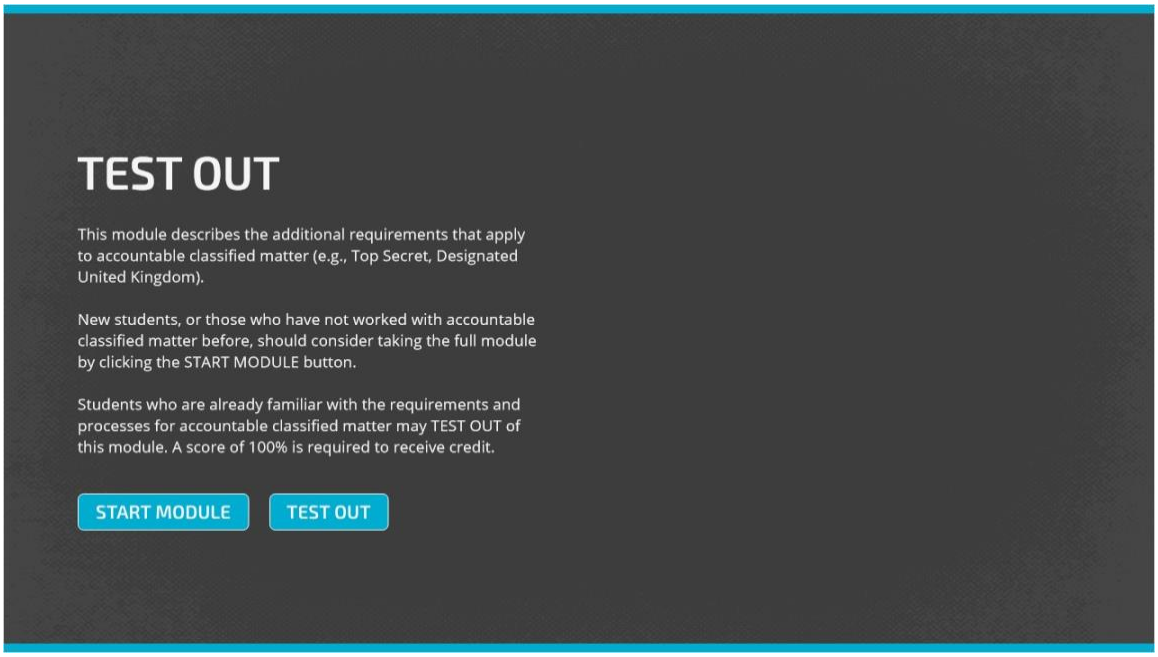
SURVEY QUESTION

Do you work with, or have the potential to work with, collateral accountable classified matter such as Top Secret or Designated United Kingdom?

Choose your answer and select the SUBMIT button.

If at any time you need more information on this topic, please visit Resources in the upper right corner of these modules.

1.3 Test Out Option



Notes:

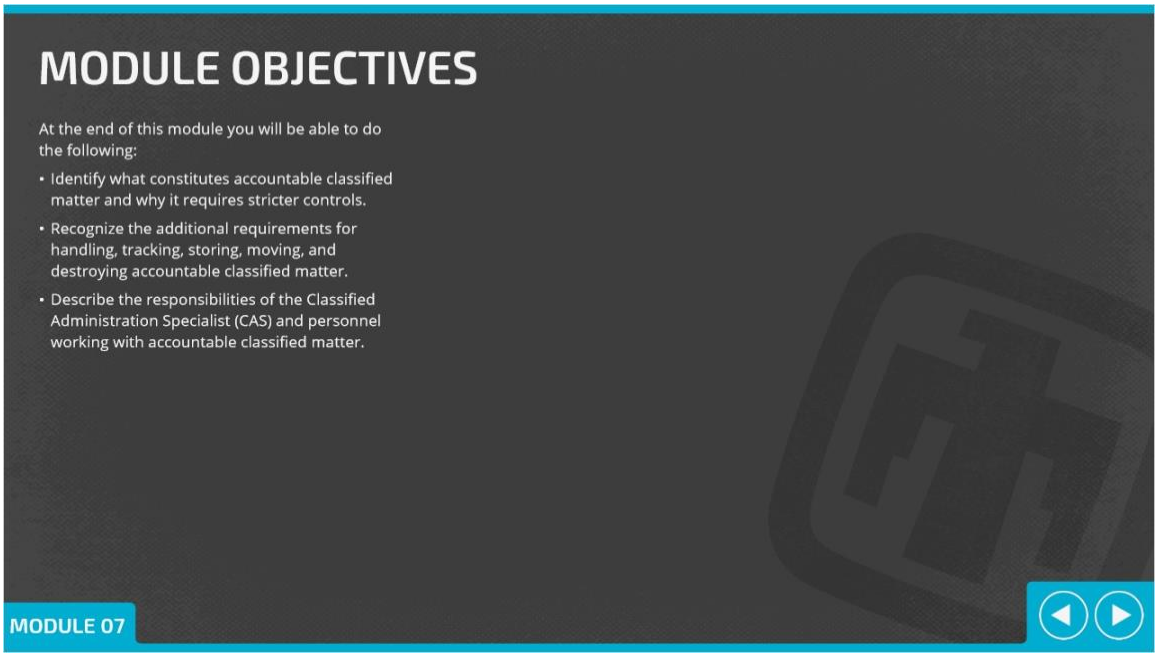
TEST OUT

This module describes the additional requirements that apply to accountable classified matter (e.g., Top Secret, Designated United Kingdom).

New students, or those who have not worked with accountable classified matter before, should consider taking the full module by clicking the START MODULE button.

Students who are already familiar with the requirements and processes for accountable classified matter may TEST OUT of this module. A score of 100% is required to receive credit.

1.4 Objectives

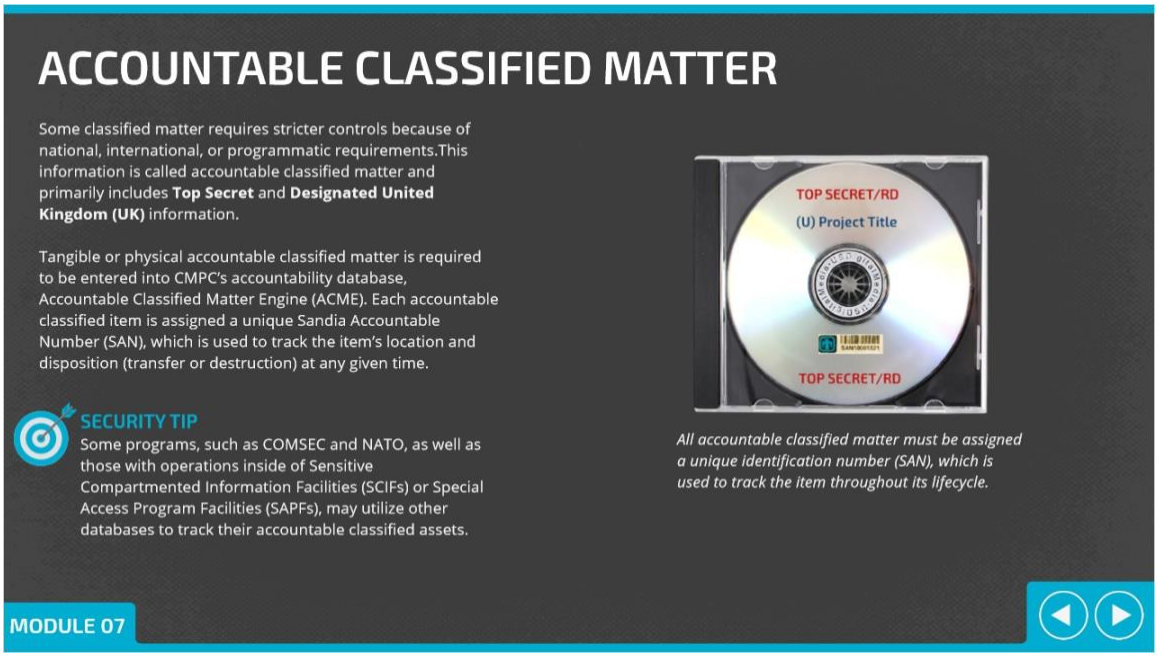


Notes:

MODULE OBJECTIVES

At the end of this module you will be able to do the following:
- Identify what constitutes accountable classified matter and why it requires stricter controls.
- Recognize the additional requirements for handling, tracking, storing, moving, and destroying accountable classified matter.
- Describe the responsibilities of the Classified Administration Specialist (CAS) and personnel working with accountable classified matter.

1.5 Accountable Classified Matter



Notes:

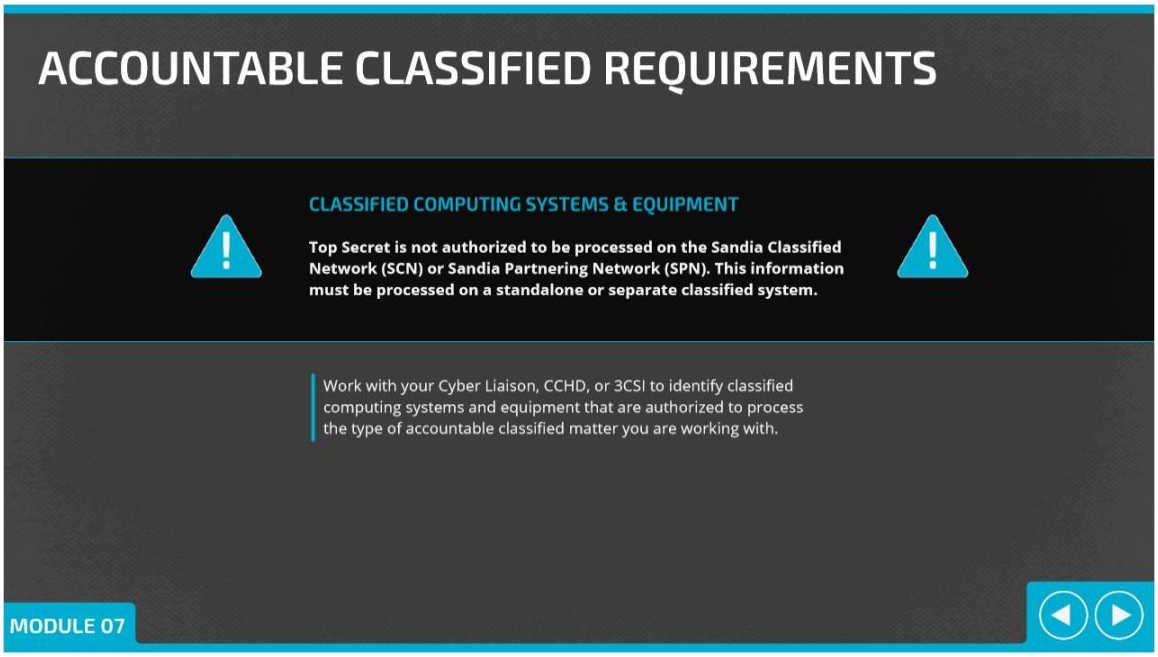
ACCOUNTABLE CLASSIFIED MATTER

Some classified matter requires stricter controls because of national, international, or programmatic requirements.This information is called accountable classified matter and primarily includes Top Secret and Designated United Kingdom (UK) information.
Tangible or physical accountable classified matter is required to be entered into CMPC's accountability database, Accountable Classified Matter Engine (ACME). Each accountable classified item is assigned a unique Sandia Accountable Number (SAN), which is used to track the item's location and disposition (transfer or destruction) at any given time.

SECURITY TIP:
Some programs, such as COMSEC and NATO, as well as those with operations inside of Sensitive Compartmented Information Facilities (SCIFs) or Special Access Program Facilities (SAPFs), may utilize other databases to track their accountable classified assets.

All accountable classified matter must be assigned a unique identification number (SAN), which is used to track the item throughout its lifecycle.

1.6 Accountable Classified Matter Requirements



Notes:

ACCOUNTABLE CLASSIFIED REQUIREMENTS
Classified computing systems & equipment

Top Secret is not authorized to be processed on the Sandia Classified Network (SCN) or Sandia Partnering Network (SPN). This information must be processed on a standalone or separate classified system.
Work with your Cyber Liaison, CCHD, or 3CSI to identify classified computing systems and equipment that are authorized to process the type of accountable classified matter you are working with.

1.7 Accountable Classified Matter Requirements



Notes:

REQUIREMENTS

External movement of accountable classified matter.
Top Secret classified matter may only be moved via the Defense Courier System (DCS), handcarry, or electronic transmission (e.g., email) on an approved network. It MAY NOT be transmitted via USPS mail service or FedEx.

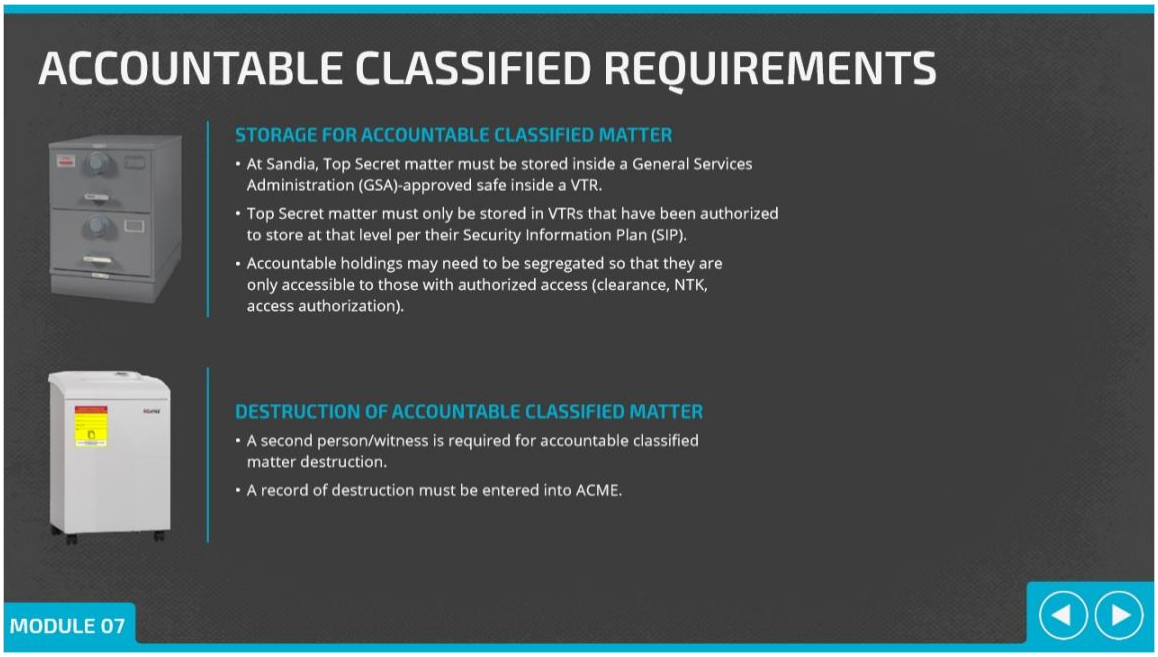
NOTE: S&S-MAN-060, Accountable Classified Work Station (CWS) Manual, provides more information on the different transmission processes, timeframes, and forms required to move accountable classified matter.

For Designated UK matter, contact the Nuclear Deterrence Partnerships and International Programs department for more information.

For other programs requiring accountability, contact the responsible POC (e.g., COMSEC Account Manager, Program Security Officer).

Top Secret classified matter is only authorized to be moved via the DCS, handcarry, or email on an approved network.

1.8 Accountable Classified Matter Requirements (Con'd)



Notes:

ACCOUNTABLE CLASSIFIED REQUIREMENTS

STORAGE FOR ACCOUNTABLE CLASSIFIED MATTER:
At Sandia, Top Secret matter must be stored inside a General Services Administration (GSA)-approved safe inside a VTR.
Top Secret matter must only be stored in VTRs that have been authorized to store at that level per their Security Information Plan (SIP).
Accountable holdings may need to be segregated so that they are only accessible to those with authorized access (clearance, NTK, access authorization).

DESTRUCTION OF ACCOUNTABLE CLASSIFIED MATTER:
A second person/witness is required for accountable classified matter destruction.
A record of destruction must be entered into ACME.

1.9 CAS Responsibilities with Accountable Classified Matter



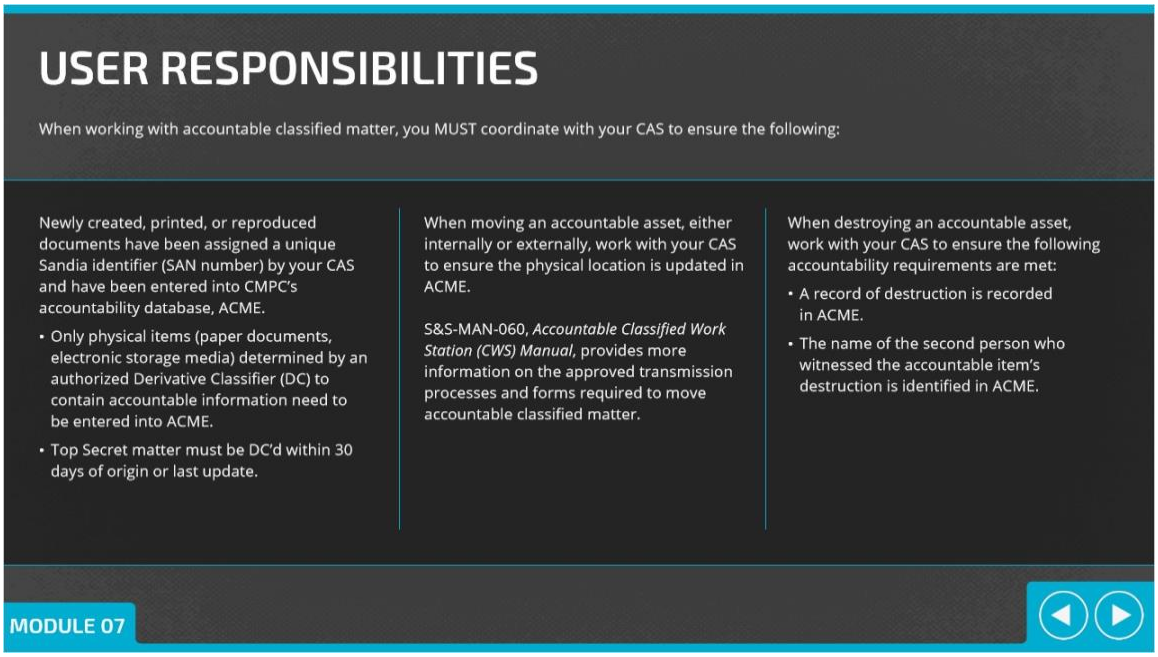
Notes:

CLASSIFIED ADMINISTRATIVE SPECIALIST

Accountable CAS Responsibilities

- CASs of accountable CWSs must complete additional CMPC training to ensure they are aware of the requirements associated with handling, protecting, and tracking accountable classified matter.
- CASs must assign a unique identification number (SAN number) to each tangible/physical accountable classified item and enter this number into ACME.
- When accountable classified matter is in use (i.e., removed from storage), a locally developed process or system must be established to identify the asset's location.
- CASs must perform a physical inventory of all their accountable holdings annually, as directed by CMPC.
- CASs must retain accountable classified matter receipts with their CWS records in accordance with the appropriate retention period (3 years for Designated UK matter, and 5 years for Top Secret matter).

1.10 Your Responsibilities



Notes:

USER RESPONSIBILITIES

When working with accountable classified matter, you MUST coordinate with your CAS to ensure the following:

Newly created, printed, or reproduced documents have been assigned a unique Sandia identifier (SAN number) by your CAS and have been entered into CMPC's accountability database, ACME.

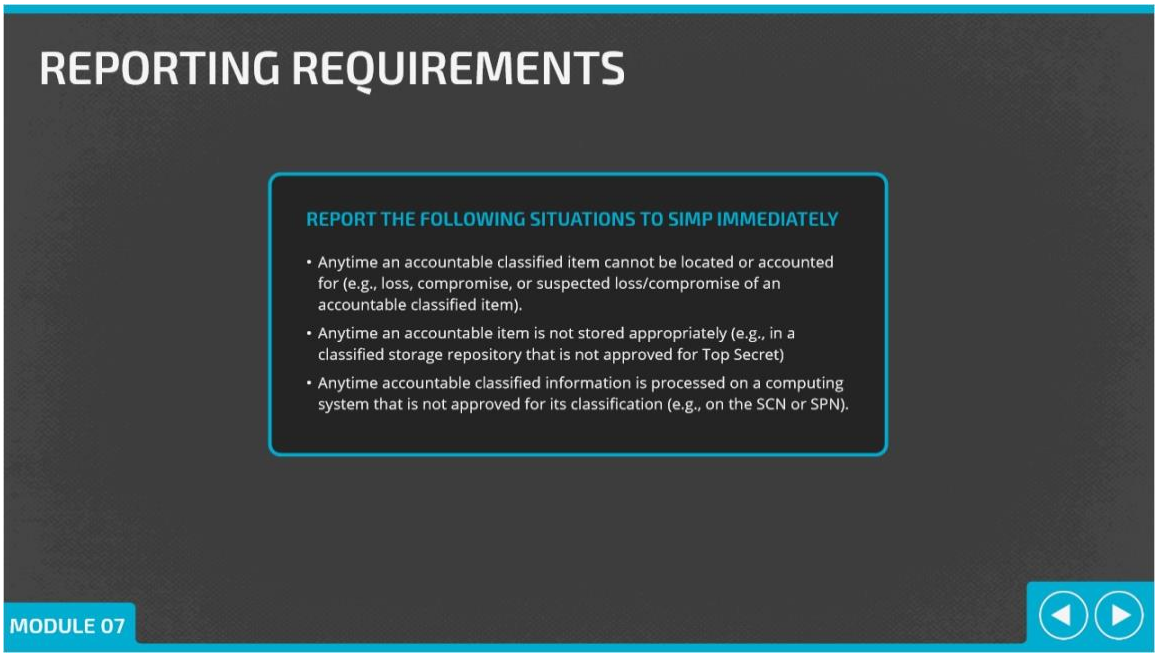
- Only physical items (paper documents, electronic storage media) determined by an authorized Derivative Classifier (DC) to contain accountable information need to be entered into ACME.
- Top Secret matter must be DC'd within 30 days of origin or last update.

When moving an accountable asset, either internally or externally, work with your CAS to ensure the physical location is updated in ACME. S&S-MAN-060, Accountable Classified Work Station (CWS) Manual, provides more information on the approved transmission processes and forms required to move accountable classified matter.

When destroying an accountable asset, work with your CAS to ensure the following accountability requirements are met:

- A record of destruction is recorded in ACME.
- The name of the second person who witnessed the accountable item's destruction is identified in ACME.

1.11 Reporting Requirements



Notes:

REPORTING REQUIREMENTS

- REPORT THE FOLLOWING SITUATIONS TO SIMP IMMEDIATELY
  Anytime an accountable classified item cannot be located or accounted for (e.g., loss, compromise, or suspected loss/compromise of an accountable classified item).
  Anytime an accountable item is not stored appropriately (e.g., in a classified storage repository that is not approved for Top Secret)
  Anytime accountable classified information is processed on a computing system that is not approved for its classification (e.g., on the SCN or SPN).