

# SEC301 Classified Matter Training

SAND 2015-7085 TR



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

## Welcome Page

Are you wondering why you have to take this training course? By virtue of holding a DOE clearance, you either work with classified or have the potential to do so. This course is designed to increase your understanding of policies, procedures, and practices for handling classified matter. Handling classified is an important and challenging task. There are many resources available to assist you with this responsibility. These resources will be identified throughout this course.



As an individual holding a security clearance, your responsibilities when dealing with classified must be taken seriously to ensure that classified matter is afforded the appropriate level of protection and control to prevent loss or compromise. Such loss or compromise carries a substantial risk to our nation's security and Sandia's reputation.

Various procedures within the Corporate Policy System are referenced in this course. These documents are continually revised to capture changes based on Department of Energy (DOE) requirements, federal and state laws, and Sandia National Laboratories (SNL) best-management practices. **If there is a discrepancy between the Corporate Policy System and this training, follow the requirements in the Corporate Policy System.**

# Module 1: Define Classified Matter

After completion of this module, you will be able to:

- Recognize classified and unclassified matter.
- Identify DOE classification levels and categories.
- Describe accountable versus non-accountable classified matter.
- Recognize marked classified matter.

## Recognize Classified and Unclassified Matter

There is a broad spectrum of information at Sandia. It's important to know and understand the differences between unclassified non-sensitive matter, unclassified controlled information (UCI), and classified matter so that adequate control and protection measures are taken to ensure only authorized individuals access the information.

### Unclassified Non-Sensitive:

This is information or material that has been determined **NOT** to be sensitive or classified, or that has been declassified by proper authority. Unclassified non-sensitive information requires no special protection, unless it contains OPSEC Critical Information.



Examples include *Sandia Lab News*, *Porcelain Press* and websites on the Sandia Open Network (SON). **Use caution** when accessing and using open-source information from the internet. This information must undergo a classification review to ensure the information you pulled is, indeed, unclassified.



### Recognize OPSEC Critical Information:

UUR information, which may still contain information that is advantageous for our adversaries when compiled, can harm SNL programs, activities, resources, or personnel. Review ISS100.3.4, *Conduct Operations Security*, to familiarize yourself with how to protect critical information.

## Recognize Classified and Unclassified Matter

### Unclassified Controlled Information (UCI):

This is information that, when disclosed, lost, misused, altered, or destroyed could adversely affect the national security, Sandia National Laboratories, or our business partners.

The identification and protection of this type of information is required by the code of federal regulations, public law, governmental directives, DOE orders or contracts with business partners. Such information may also be subject to Sandia's processes to protect commercially valuable information. This information requires some controls to ensure only authorized individuals access this information.

Think about how you handle your social security or credit card numbers. Access to this information must be limited, controlled, and protected.

<p style="text-align: center;"><b>OFFICIAL USE ONLY</b></p> <p><u>May</u> be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category Exemption #7, Law Enforcement.</p> <p>Department of Energy review required before public release</p> <p>Name/Org: John Doe Date:5/26/2015</p> <p>Guidance (if applicable) n/a</p>
--



**Examples** of UCI are: Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), Personally Identifiable Information (PII), and Export Controlled Information (ECI).

Check TEDS for additional training in OUO (OUO101, *Understanding Official Use Training*) and Export Control (ECI100, *Export Control Awareness Training*).

## **Recognize Classified and Unclassified Matter**

### **Classified Information:**

Classified information is information that is rigidly controlled and protected in the interest of national security. Classified matter must be protected in a manner that ensures that access is strictly controlled.



Examples include nuclear weapon information and information regarding national security.

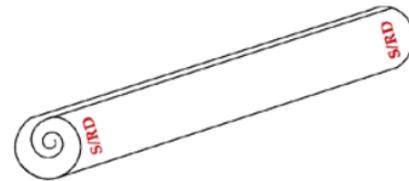
For the remainder of this course we will focus on how to identify, protect, control, and handle this type of information.

## Classified and Unclassified Matter

### What types of classified matter exist at Sandia?

Classified matter is a document (includes cyber media) or material deemed to contain classified information.

- Classified **documents** are any type of recorded information. Some examples are printed documents (e.g., reports, memos), photographs, blueprints, CDs/DVDs, removable hard drives, and handwritten notes.
- Classified **materials** can be chemical compounds, metals (unclassified sample pictured), fabricated or processed items, machinery, equipment, or any combination thereof that contains or reveals classified information.



## Identify DOE Classification Levels and Categories

When dealing with classified, the level and category must be identified. For each classified asset (e.g., document, CD, part/piece) one level and one category must be designated. The classification level is written first, followed by the category (e.g., SECRET + RESTRICTED DATA = SRD). Abbreviations are acceptable when space is limited. Identification of the classification level and category is important because our classified must marked to reflect this information. The markings are then used to determine how we protect these important assets.

### Classification Levels:

Classification levels identify the degree of damage to national security if an unauthorized disclosure of this information is made.



**Top Secret (TS):** Unauthorized disclosure of this information could reasonably be expected to cause **exceptionally grave damage to national security.**

**Secret (S):** Unauthorized disclosure of this information could reasonably be expected to **seriously damage national security.**

**Confidential (C):** Unauthorized disclosure of this information could reasonably be expected to cause **damage to national security.**

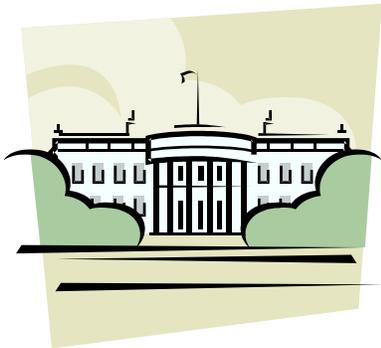
### **Identify DOE Classification Levels and Categories**

The classification of a classified document also includes the category of information. The category tells you what type of information you are dealing with.

**Restricted Data (RD):** RD is the most restrictive of the classified categories. RD includes all data concerning design, manufacture or utilization of atomic weapons; production of special nuclear material (SNM); or use of SNM in production of energy.

**Formerly Restricted Data (FRD):** Information determined jointly by DOE and DoD to relate primarily to military use of atomic weapons.

**National Security Information (NSI):** Information important to the national security for reasons other than those in the RD and FRD categories, and classified in accordance with Presidential Executive Orders.



Restricted Data and Formerly Restricted Data were both established in the Atomic Energy Act and are applicable to work performed by the Department of Energy and its contractors.

National Security Information is derived from Presidential Executive Order and is commonly used by other United States federal agencies (in addition to the DOE).

**For guidance on Foreign Government Information (FGI) or Transclassified Foreign Nuclear Information (TFNI) see SNL Corporate Policy ISS100.1.12, *Foreign Government Information*. Contact the Classification Office or your Program Security Officer if you have questions.**

## DOE Classification Levels and Categories

### Caveats

Some classified information not only includes a classification level and category, but also a caveat. Caveats are additional designations used to designate special information and/or access restrictions (e.g., Sigma 15, Critical Nuclear Weapon Design Information [CNWDI]). An example of a caveat with an access restriction is NOFORN (No Foreign Dissemination).

### Identify Classified Matter in Your Subject Area

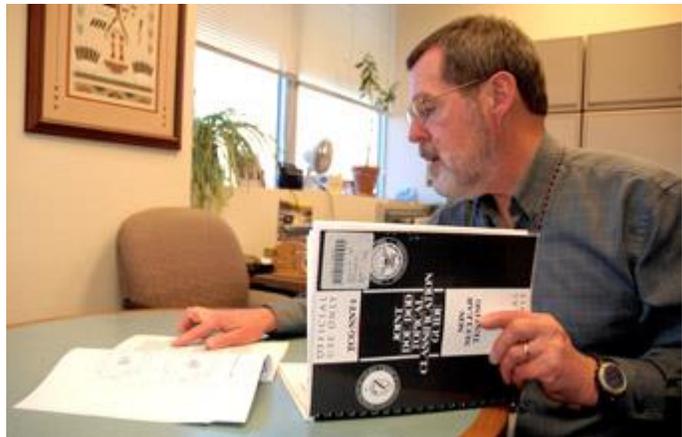
Some of your work may deal with classified matter, and some may not. Your manager is your best resource for determining what is potentially classified in a particular subject area. When you start a new project always ask what the project's classification will be.

Classification briefings on specific subjects are available to help you understand your classified work. Talk to your manager for more information. The SNL Classification Office is also available to answer your questions.

### Who determines whether information is classified?

Final classification determination for information (e.g., newly-written report, data collected from an experiment) must be made by a Derivative Classifier (DC). A DC uses a classification guide to determine the appropriate level, category and caveat (if applicable) of the classified information.

A DC is only authorized to review specific matter in his or her area of expertise. Further, DCs are only authorized to review specific levels and categories of information.



A recent change in requirements has prompted the creation of an Email-Only DC. These are individuals who have limited authority to perform reviews of their sent emails on classified systems only (as long as the content of the email is within their authority). See this [website](#) for more information on an EDC.

Do you know who your DC is? Ask your manager!

### **Accountable and Non-Accountable Classified Information**

The United States Government has determined that some classified matter requires stricter controls. This means this type of classified information must be carefully tracked at all times. This information is called **accountable classified information**. Examples of accountable classified information are:

1. All Top Secret information
2. Any matter designated as accountable because of national, international or programmatic requirements (e.g., Sigma 14, designated United Kingdom, North Atlantic Treaty Organization (NATO) Atomic).

### **What are the additional controls for accountable classified matter?**

1. All accountable matter has an additional marking (SNL issued barcode sticker) that has a unique identification number. Contact your Classified Administrative Specialist (CAS) for these stickers.
2. When the bar-code sticker (unique identification number) is affixed to the accountable classified asset, the asset must be entered into an SNL accountability system. This database is used to track the exact location of the asset when it is located at SNL.
3. The CAS is required to perform an annual physical inventory of all accountable assets at a designated time during the year. He/she uses the information from the database and physically checks each asset to ensure all items are accounted for.



### **How does this impact you?**

If you deal with accountable classified you must work closely with your CAS to ensure this classified is controlled correctly. We will talk about these controls further in later modules in this course.

Non-accountable classified matter must still be carefully protected, but is not required to be tracked in a database and inventoried annually.

### Recognize Marked Classified Matter

Classified matter must be marked appropriately for two main reasons:

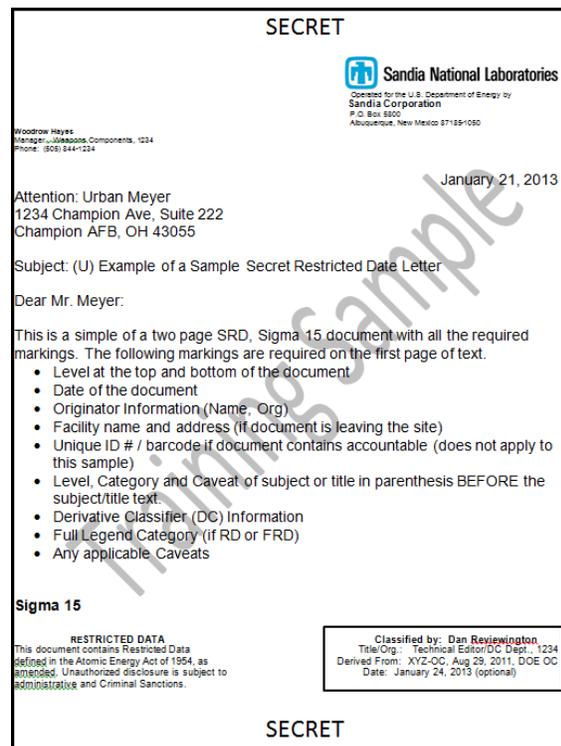
1. Alert individuals that classified information is present.
2. Warn holders of special access of safeguarding requirements. Some classified assets have additional markings that warn you who cannot access the information.

Examples include:

- NOFORN- No foreign national can access this type of information
- Sigmas with an Access List (Sigma 14, Sigma 15, Sigma 20) - an individual must satisfy the requirements to be on one of these access lists before he/she can access this type of information.



Classified matter must be marked with the classification level, category (if RD or FRD) and caveat. In circumstances when classified material cannot be marked, the container/bag in which it is stored will be marked. Items can also be tagged to indicate their classification. Some unclassified examples are shown below.



## Module 2: Access, Control, and Protection of Classified Matter

After completion of this module, you will be able to:

- Determine who can access classified matter.
- Be aware of the penalties identified in 10 CFR824, *Procedural Rule for the Assessment of Civil Penalties for Classified Information Security Violations*.
- Define need to know.
- Identify DOE's No Comment Policy for Classified Areas.
- Identify control methods for classified.
- Identify protection methods for classified.



Access, control and protection of classified information are essential to protecting our nation's security. There are many countries, criminals, and activists that have a desire to gain possession of our country's classified information. We must work together to ensure all classified matter is appropriately identified and marked, so we can control access.

### Determine Who Can Access Classified Matter



Only authorized individuals can access classified matter. Your manager plays a major role in what you access by identifying what type of classified information you handle when he/she submits the request for your clearance.

The Department of Energy has the authority to penalize contractors or subcontractors who violate any rule, regulation, or order relating to the safeguarding or security of classified information. Civil penalties may be assessed if a person “by an act or omission causes, or creates a risk of, the loss, compromise or unauthorized disclosure of classified information.” [10 CFR 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*].

**Determine Who Can Access Classified Matter**

The matrix below indicates the level and categories of classified matter an L-cleared and Q-cleared individual can access.

*LEFT TO RIGHT  
HIGHEST CATEGORY TO LOWEST CATEGORY*

<i>Access Authorization</i>	<i>Restricted Data (RD)</i>	<i>Formerly Restricted Data (FRD)</i>	<i>National Security Information (NSI)</i>
<i>Top Secret (TS)</i>	Q	Q	Q
<i>Secret (S)</i>	Q	Q L	Q L
<i>Confidential (C)</i>	Q L	Q L	Q L

*TOP TO BOTTOM  
HIGHEST LEVEL TO LOWEST LEVEL*

**Did you know DOE has added three new clearance levels (in addition to L and Q)?**

New clearances are; DOE Top Secret, DOE Secret, and DOE Confidential. These do not equate to the DoD clearances (i.e., DOE TS does not equal DoD TS). Sandia has chosen to only issue L and Q clearances, but it's important to know an individual from another site may have one of these new clearances. For more information on these new clearances and what levels of classification to which they allow access, talk to your manager.

## Determine Who Can Access Classified Matter

### Do you work with contractors on classified projects?

Before providing classified information to a contractor employee, you must know if the contractor's contract security classification specification (CSCS) permits the contractor access to the level, category, and caveats (if applicable) of the information. Check with your manager to determine the contractor's CSCS.

### Define Need-to-Know

Having an authorized, active clearance is not all you need to access classified information. You must also have a need-to-know (NTK) to be granted access. This means you require access to (including incidental access), to perform tasks or services essential to the fulfillment of a classified contract or program for an authorized government function.



Individuals from all over the United States and the world visit Sandia to collaborate on classified projects. Establishing need to know and verifying clearances is important in the following situations:

- United States Cleared Visitor—Verify the visitor's access authorization (clearance and any additional access requirements) and need-to-know before allowing them access to classified information.
- Cleared Foreign National—Verify the cleared foreign national's credentials (clearances established and approved by the appropriate US Government Agency and any additional access requirements) and programmatic need-to-know.

**Note:** Do not forget to follow export control policies when sharing information with foreign nationals. Visit the Export/Import Control website for more information.

### Who determines need-to-know?

Need-to-know is determined by the owner/holder of the classified matter or by the manager of the department that owns the classified.

### Something to Think About

Much of the classified work performed at Sandia resides on approved classified networks. Access to many files is controlled by metagroups. These metagroups must be constantly monitored to ensure NTK is always enforced. Ask your manager about the metagroups used by your organization.

## Determine Who Can Access Classified Matter

### “No Comment” Policy on Classified Information in the Public Domain

Sometimes classified information appears in the news, on the internet, or in other public sources without authorization. It is important that we continue to control our classified information in situations like these.



Many make the mistake of assuming the information is no longer classified if it has been revealed to the public. Release of this information does not mean it has been declassified. The fact that the classified information has appeared publically is itself classified to the same level and category of the information in question.



It is a violation of the Department of Energy’s “No Comment” Policy for a Sandia employee or contractor to confirm, deny, or expand on the classification status of information or the accuracy of unauthorized public disclosures. Making a comment may result in greater damage to national security than if no comment were made at all. Using the phrase “No Comment” may result in confirming classified information.

If you must respond, your response should be a very general “We do not comment on this type of information” when approached with a question about a classified subject. Contact the Classification Department for more information on the “No Comment” policy.

## Determine Who Can Access Classified Matter

### Accessing Vaults and Closed Areas

Before we discuss who can access a vault or closed area, it's important to know what we are talking about. Many of Sandia's classified assets are located inside of vaults and closed areas.

- A vault is a windowless enclosure that is resistant to forced entry and has a DOE approved system that detects unauthorized entry.
- A closed area (formerly called a VTR) is an area used for safeguarding matter and/or security interests that, due to the size, nature, or operational necessity cannot be adequately protected by normal safeguards or stored in approved containers (e.g. GSA-safes). These closed areas meet DOE requirements for protection (e.g., alarm system, locks).

### Granting Access to a Closed Area

Access to a closed area is carefully controlled. This is to ensure only authorized individuals with the appropriate clearance and need-to-know have access.

A closed area resident is someone who has the appropriate clearance and need-to-know, and has been added to the associated closed area's access list. Closed area residents should work with their manager to ensure they have completed all required closed area training.

If you are not granted access to the closed area, you are considered a "non-resident." A non-resident must be escorted at all times by a resident when accessing the closed area. Before being escorted into the closed area, the resident will ensure all classified matter inside the closed area is secured so the non-resident does not have access to it.



## Identify Methods of Controlling Classified Matter

### Who helps me control my classified?

Earlier in the course, we discussed working with your Classified Administrative Specialist (CAS) when dealing with accountable classified matter. The CAS also assists with all other classified matter within your area.

The CAS is the individual who assists with the classified operations within a designated area. This designated area is called a Classified Work Station (CWS). These areas can include a few rooms, to multiple rooms and closed areas within multiple buildings. Each CWS has a CWS Manager who is responsible for the classified work within the CWS.

### How can your CAS help you?

The CAS is a local resource to help you with your classified processing. These individuals (Primary & Alternate CASs) can assist with your classified questions. Some examples of actions they can assist with include:

- Identifying a GSA-approved safe or closed area that is authorized at the appropriate level, category and caveat (if possible) to store your classified.
- Transferring classified assets to another CWS (within Sandia) or to an external customer. The CASs will ensure the required verifications and documentation are made before the transfer.
- Making copies of classified documents.
- Verifying that you have appropriately marked your documents before storing them.



**Do you know who your CAS is?** If you do not know who your CAS is, ask your manager. The CASs take additional training and are knowledgeable of available resources to assist with day-to-day classified operations.

## Identify Methods of Controlling Classified Matter

### What you should know before you use classified:

Aside from having the appropriate clearance and need-to-know, there are a few more things you should know before working with classified:

1. **Are you current in your training?**

- Individuals who will create classified matter that will be marked as final (meaning the information will be reviewed by a derivative classifier) are required to take SEC303, Classified Marking Training. Work with your training coordinator to enroll in this class.
- Individuals with a classified computing email account who are not authorized derivative classifiers (DCs) must also take Email-Only DC or EDC training. See this [website](#) for more information on an EDC.



2. **Is your area approved for classified processing?** You can only perform classified work in areas that provide control measures equal to or greater than those present in Limited Areas.

**Note:** If you MUST conduct classified work outside of a Limited Area, you must have an approved security plan (designating this area as a Temporary Limited Area) prior to performing that work. Contact Physical Security for more information.

3. **Have you identified an approved storage location?** Your CAS will help you identify your options to store your classified when you are finished processing it. Plan ahead so classified can be stored appropriately. If your CAS is not available, work with the alternate CAS, a CAS of another CWS or your manager to identify an approved storage location. If you are at SNL/NM or SNL/CA, as a last resort (e.g., working during non-operational hours) contact the Protective Force who can assist with temporary storage.

4. **Will you be using classified computing equipment?** Work with the Cyber Security Representative (CSR) to ensure you know what type of classified can be processed on your computing system. This individual can also assist you with day-to-day questions about these systems (e.g., how to properly log in and log off the systems).

The Transmission Security Checklist (TSC) is a DOE and SNL requirement. The TSC is required anytime the owner or location of the classified system changes or the owner receives a DiGS alert. Contact your CSR or CCHD for assistance.

These are all important items to consider before dealing with classified. Being able to successfully answer these questions will help ensure the classified information is protected.

### Do you work from home?



If so, you should NEVER process any classified or work on information related to a classified subject area. Remember, work on classified subject areas at the unclassified level can easily cross into the classified realm and cause a high level security incident.

## Identify Methods of Controlling Classified Matter

### Control Measures for Classified Matter While in Use

Once you have the need-to-know and appropriate clearance, it's important that you know how to control classified in your possession. When you are processing classified you **must** control it by:

- Keeping it in your possession at all times.
- Relinquish your classified only to individuals with proper access authorization and need-to-know.

When removing classified from an approved repository (GSA-safe or closed area) you must always use a cover and backing sheet. Your CAS can help you find these materials for your documents.

Classified may be removed from storage to perform official work only. **DO NOT** take classified with you to perform non-official business (e.g., offsite for lunch or personal appointments).



### Protection Measures When Processing Classified



When you have classified in your possession it is important that you take adequate measures to ensure there is no inadvertent disclosure of the classified information. To do this, you can display appropriate signage when classified is being processed. You must also position your equipment and/or documents so your processing is not readily visible to an unauthorized individual.

## Identify Methods of Controlling Classified Matter

### Hosting a Meeting that will Include Classified Information?

When you are the host of a meeting that may include classified information, there are verifications that must take place first to ensure the information is protected and controlled appropriately. Following these steps will help you and your meeting attendees prevent a possible security incident. The meeting host has the following responsibilities:

#### 1. Plan the meeting.

- **Identify your meeting participants and verify they have the appropriate access (security clearance) and need-to-know.** If your meeting includes visitors to SNL, work closely with the Badge Office to ensure their classified visit was processed and approved. The Badge Office will help you ensure these visitors have the appropriate access to participate in the meeting.
- **Verify location of the meeting is approved for classified processing.** If you are using video conferencing or computer equipment, make sure they are approved for the level and category of the classified information being discussed. If you have a question about the classified computer, contact your Cyber Security Representative.
- **Ensure the room has appropriate signage posted before the meeting.**
- **Open removable partitions (if applicable).**



#### 2. Start of the meeting.

- **Make a controlled article announcement to ensure all controlled articles are removed from the area prior to the commencement of the meeting.**
- **Open the meeting by announcing the level of classified (level, category, caveat [if applicable]) information to be discussed at the meeting.** This way everybody is aware of the information being discussed. Those taking classified notes **must** mark their draft document that contains classified at this classification until the document can be reviewed by a derivative classifier.
- **Verify attendees are badged and have the appropriate clearance.** Attendees must have the appropriate access authorization to attend the meeting. This includes verifying clearance and checking access list (if the meeting will include Sigma 14, Sigma 15 or Sigma 20 information).



# Module 3: Create and Generate Classified Matter

After completion of this module, you will be able to:

- Understand the requirements when creating classified
- Identify the required markings for a draft document.
- Recognize responsibilities for obtaining classification determination.
- Recognize when a draft classified document must be finalized.



## Create Classified Matter

Classified matter at Sandia is generated in many ways. Some of the common ways we process classified at Sandia include:

- **Processing classified on an approved classified computer system:** It's important to know what level and category of information your classified computer system is approved for. The Sandia Restricted Network (SRN) is not approved for processing classified information. Contact your Cyber Security Representative to discuss what classification you are authorized to process on the classified systems in your area.



**Your classified password must be protected and secured in an approved repository.**

- **Creating classified notes:** Classified notes can be handwritten notes taken from a meeting or during data collection from a classified experiment.
- **Creating classified blueprints and design documents.**
- **Recording video or taking photographs of classified assets.**
- **Creating/Handling Classified Hardware (parts, pieces, components):** These are pieces of tangible material that are visually classified.

## Create and Generate Classified Information

### Create Classified Document

Classified documents can be created electronically and non-electronically. When first creating a draft classified document, it's important that the document is properly marked. Marking the document is important because it alerts us that the information is sensitive and must be protected as classified. Let's discuss how this is done for both the electronic and non-electronic methods.

**Non-electronic classified document:** When you write down classified information you have created non-electronic classified. This type of information should be marked at the highest level and category you believe it to contain until it can be reviewed by an authorized DC. If you are unsure, error on the side of caution and consult your DC.



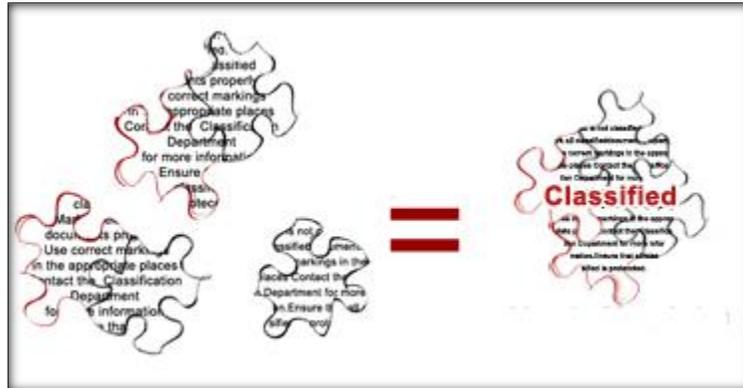
**Electronic classified document:** This is when classified is generated on an approved classified computing system. When creating classified in this environment, until reviewed by a DC, mark documents created on a computer at the classification level and category for which the computer system is accredited.

If data is to be exported from a classified system to an unclassified system via electronic media, an Authorized Transfer Point (ATP) must be used and approved processes followed.

## Create and Generate Classified Information

### Association and Compilation

When working with both classified and unclassified information, always keep in mind classification association. When information is combined or compiled, it could reveal information of greater sensitivity than any of the individual bits of information separately. This applies to both documents and materials.



When this information is compiled and deemed to now be classified, it must be identified and handled as such. These situations can occur whenever information is compiled and are of special concern when creating and responding to e-mail messages.

Compilation does not happen *only* when combining unclassified information. Combining multiple bits of classified information could potentially elevate the Level and/or Category of the information. For example, you wish to merge two reports classified as SNSI. There is the potential these two reports put together could possibly result in a new document with a higher level and/or category.

Consult your derivative classifier if you ever have any questions or concerns about compilation.

## Create and Generate Classified Information

### How do you mark a classified draft document?

Classified draft documents must be marked so they are properly controlled and protected. When marking a classified draft you must have the following:

### Required Markings on Classified Draft Document

#### First page of printed text:

1. Date of Origination.
2. Classification LEVEL centered at the top and bottom
3. Classification CATEGORY (if RD or FRD) following the Classification LEVEL on top and bottom of page.
4. Classification of the Subject or Title: For example, “(U) The BCS Bowl Formula.”
5. The words “Draft” or “Working Paper” annotated anywhere on the page.
6. Add caveats, if applicable, anywhere on the page.

#### Interior pages of printed text (if applicable):

1. Classification LEVEL at the top and bottom of each interior page
2. Classification LEVEL at the top and bottom of the back of the last printed page.

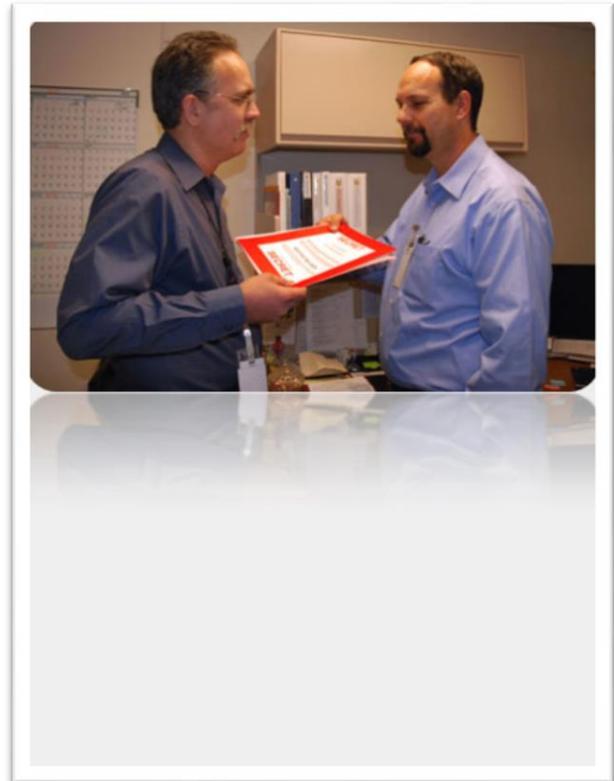
### Will you remember the required markings on a classified draft?

Some individuals mark classified frequently, and others may not. If you think you may forget these requirements, don't worry. Resources are available. Add the [CMPC Marking Guide](#) to your web browser favorites to use as a reference.

### Create Classified Matter

We discussed in module one that an authorized derivative classifier (DC) is the individual who provides the final classification level, category and caveat. When working with a DC, you must always work with the DC in person, or via a secured means. Do **not** discuss classified on an unsecured phone or on an unclassified computer (Sandia Restricted Network).

Discussing potentially classified information using an unsecure method could result in a potential compromise in classified information and a security incident.

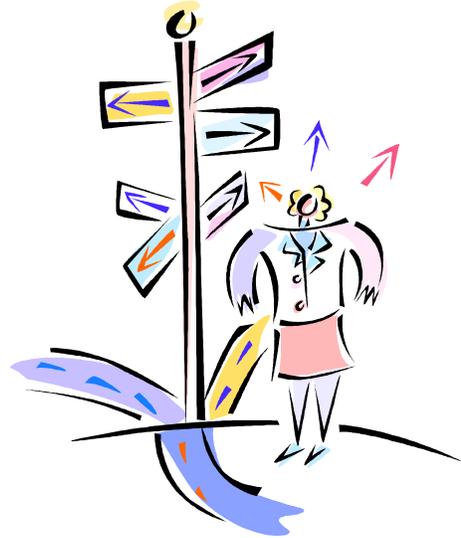


## Create and Generate Classified Information

### When must a draft document be reviewed by a derivative classifier and marked as final?

There are multiple situations when a classified draft document must be reviewed by a derivative classifier.

1. **Permanently filed:** You are done making changes to the draft and will keep the document with your other final classified documents.
2. **Retained for more than 180 calendar days or 30 days for Top Secret:** If you have a draft document that has not been edited for more than 180 days, it must be; sent to a derivative classifier and marked as final OR; destroyed in an approved shredder.



If you are continually adding information to your draft document, it's considered a "living document." You must annotate the date when you make your changes. These new dates will reset the 180 calendar days or 30 days for Top Secret. A good example of this is engineering or lab notebooks.

3. **When the classified draft is released outside the working group (printed and electronic document):** If you are going to share your information with somebody outside the working group your document must be reviewed by a derivative classifier and marked as final.

It's important that the official classification be identified, so the appropriate protection measures are taken to protect that information. The federal government requires that information identified as NSI have a declassify date. If potentially NSI is not reviewed by a DC, there is a risk that the declassify date never be assigned to that asset, thus putting us at risk of being out of compliance with federal policy.

### Where do I go to learn about how to mark a final document?

Work with your training coordinator to enroll in SEC303, *Classified Marking Training*. Add the [CMPC Marking Guide](#) to your web browser favorites to use as a reference.

## Module 4: Store Classified Matter

After completion of this module, you will be able to:

- Identify requirements for storing classified matter.
- Identify procedures for storing classified matter.
- Identify processes for protecting classified combinations.

### Where can you store classified?

Classified matter, when not in use, must be stored in approved repositories. The repositories approved for storage are closed areas (pictured), Vaults, and GSA-approved safes. Your locked desk drawer or locked office **is not** an acceptable location to store classified.



Approved repositories must be protected at the highest level and category of information being stored in them. This means individuals with access to the repositories (i.e., know the combination), must have the appropriate clearance, NTK, and other programmatic requirements if applicable (e.g., Sigma Access List). These repositories **must not** have any external markings indicating the level of information being stored within.

Approved repositories will only be located in areas approved for classified processing (e.g., Limited Area). Consult your CAS if you have a question about where your approved repositories are located, and what level and category can be stored in them. Speak with your Closed Area Custodian if you have questions about a closed area.

**These approved repositories must be kept locked when not under direct supervision of an authorized individual.**

### Can I store unclassified in a repository with my classified matter?

Unclassified assets can be comingled with classified in a repository, but must **always** be marked to ensure they are identified and protected accordingly.

## Store Classified Matter

Items susceptible to theft (e.g., funds, firearms, precious metals, medical items) cannot be stored with classified. If classified matter is hazardous or radioactive and cannot be stored in an approved repository, contact Physical Security for assistance.

Storage requirements differ for accountable and non-accountable classified matter. Specific storage practices also vary between the various departments and their Classified Work Station (CWS). Each CWS is approved to store different level, category, and caveats of classified matter. This approval is important because it dictates access authorization, Protective Force patrol frequency, and response times. Speak with your CAS if you have questions about what you are allowed to store in your CWS.





## **Store Classified Matter**

### **Locking and Checking Approved Repositories**

When not in use and when unattended, classified repositories **must** be secured and locked. Each time the repository is locked, it must be annotated on the SF 702. The individual who opened the repository can be the same person who locks it. However, at the end of operations, a second person must perform a check to verify the repository was locked. The second person performing the check **must** be different than the person who last locked the repository.

The following processes are generic procedures used for GSA-approved safes and closed areas. Consult your CAS or CWS Manager for specifics on how to lock repositories in your area.

### **Locking GSA-Approved Safes:**

1. Close all safe drawers.
2. Turn the spin dial counter clockwise a minimum of four complete revolutions to extend the safe's bolt.
3. Turn the spin dial clockwise a minimum of four complete revolutions to ensure the safe is locked.
4. Turn and pull ALL handles to ensure the safe is secured.
5. Complete the "Locked By" portion of the SF 702, *Security Container Check Sheet*.

### **Checking a GSA Approved Safe:**

Once the repository has been locked for the final time that day, it must be checked by a second person (two-person rule). The process below is a generic procedure on how to perform the check.

1. Try to turn and tug the handle of each drawer to verify they are locked.
2. Rotate the spin-dial(s) one to four times to the left (this will ensure that the capacitors within locks that are rarely used maintain their charge).
3. Initial the "Checked By" column on the SF 702, *Security Container Check Sheet*.

## Store Classified Matter

### Locking and Checking Closed Areas:

Methods for locking and checking of closed areas vary and are dependent on the configuration of your closed area. Information on how to lock and perform the check on a closed area can be found in *Closed Area Training* (SEC180). The check must be completed by a second-person, different than the individual who locked the closed area. The SF 702, *Security Container Check Sheet*, **must** be annotated to document the closed area has been locked and checked.



### What if there is nobody around to check my safe or Closed Area?



If you are unable to find somebody to perform the check that the repository is locked, contact the Protective Force. You **must** remain in the area until the Protective Force Officer arrives, performs the check, and completes the SF 702, *Security Container Check Sheet*.

### What if I never open my repository? Does somebody still need to perform the check?

Repositories must be checked daily **if** personnel with combinations are working in the area, even if the repository was not opened. Talk to your manager for more information on how he/she defines “working in the area.”

## Store Classified Matter

### Classified Combinations:

Combinations of repositories must be protected at the highest classification level and category of the matter being protected and comply with access restrictions to combinations. Each spin-dial of a repository must have a unique combination. Individuals who knowledge of the combination must have the appropriate clearance, and need-to-know of the contents in the repository.



Combinations must be changed within 10 working days if any of the following occur:

1. Individual with the combination no longer needs access.
2. Individual's access authorization is downgraded to a lower level than the matter being stored in the repository. This means an individual could downgrade their security clearance OR have their Sigma Access revoked (if the combination protects Sigma information).
3. Compromise or suspected compromise of the repository's combination.
4. Approved safe is removed from service, or has been serviced. When serviced at SNL/CA, change the combination if the repository was serviced by an uncleared locksmith or technician.

Make sure to partner with your CAS and other members of your organization to ensure only authorized individuals have the combinations and access to your repositories.



Classified combinations cannot be changed to the factory default until the **ENTIRE** safe is empty and no longer storing classified.

**Store Classified Matter**

**Classified Combinations:**

The classified combinations are captured on a required SF 700 form (pictured). An addendum to the SF 700 called the SF 2900-ADD is also used to capture the names of all individuals who have the repository's combination. Work closely with your CAS and Closed Area Custodian (for closed areas) when changing the repository's combination.

CLASSIFICATION LEVEL		
<b>SECURITY CONTAINER INFORMATION INSTRUCTIONS</b> 1. Complete Part 1 and Part 2A (in end of flap). 2. Detach Part 1 and attach to the inside of the control drawer of the security container. 3. Mark Parts 2 and 2A with the highest classification level stored in the security container. 4. Detach Part 2A, insert in envelope (Part 2) and seal. 5. See Privacy Act Statement on reverse.  8. DATE COMBINATION CHANGED  10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE  11. Immediately notify one of the following persons, if this container is found open and unattended.	1. AREA OR POST <i>(if required)</i>	2. BUILDING <i>(if required)</i>
	3. ROOM NO.	4. ACTIVITY (Division, Branch, Section or Office)
	5. CONTAINER NO.	6. MFG. & CLASS OF CONTAINER
	7. MFG. & LOCK MODEL	8. SERIAL NO. OF LOCK
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

2. NSN 7540-01-214-5372

STANDARD FORM 700 (REV. 4-01)  
Prescribed by NARA/ISOO  
32 CFR 2003

**WARNING**  
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CLASSIFICATION LEVEL \_\_\_\_\_

SECURITY CONTAINER NUMBER \_\_\_\_\_

COMBINATION

\_\_\_\_\_ turns to the (Right) (Left) stop at \_\_\_\_\_

\_\_\_\_\_ turns to the (Right) (Left) stop at \_\_\_\_\_

\_\_\_\_\_ turns to the (Right) (Left) stop at \_\_\_\_\_

\_\_\_\_\_ turns to the (Right) (Left) stop at \_\_\_\_\_

**WARNING**  
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.  
UNCLASSIFIED UPON CHANGE OF COMBINATION.

**2A.** INSERT IN ENVELOPE

SF 700 (REV. 4-01)  
Prescribed by NARA/ISOO  
32 CFR 2003

## Module 5: Reproduce Classified Matter

After completion of this module, you will be able to identify requirements for reproducing classified documents.

Reproduction of classified in this module is defined as creating a copy or duplicate of existing classified matter. When reproducing classified it's important that you remember the following key requirements:

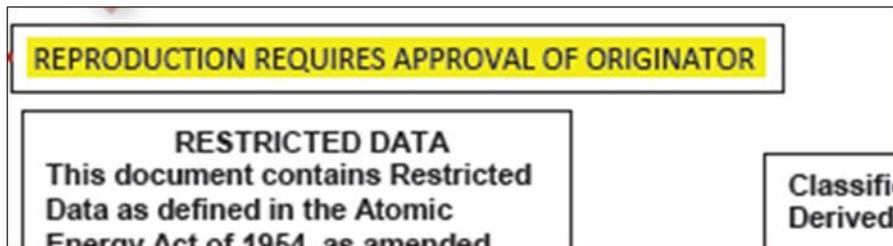
1. **Can you reproduce/copy the item?**
2. **Only use approved copy machine and follow the classified copier process.**



## Reproduction of Classified Matter

### Can you reproduce/copy the classified item?

1. Many classified assets are marked with a reproduction limitation (see below). In cases like this you must receive approval from the originating agency before making a copy.
2. If the classified asset is accountable you **must** work with your CAS to make the copy. This will ensure the newly created copies receive a unique ID number and are entered into the SNL accountability system.
3. Never create a copy of an externally (non-SNL) created classified document for anybody outside of Sandia.



## Reproduction of Classified Matter

### Process to copy classified matter

When making copies of classified, you **MUST** use a copy machine approved for classified copying. Such machines have a sticker that says the machine is approved for use with classified. This approval means the machine has the appropriate set-up (e.g., is not connected to an unclassified network, does not have memory to store previous jobs). **Never** use a machine that does not have an approval sticker.



Contact your CAS if you have questions about what copy machines are approved for classified processing in your area.

### Requirements when making copies of classified:

1. Find the sticker that says the copy machine is approved for use on classified.
2. If in the presence of others, ensure those individuals have the appropriate access authorization (e.g., clearance, need-to-know).
3. **Never** leave the copy machine when copies are being made.
4. Generate only the number of copies necessary.
5. When copying is complete, count and verify all copies were made (e.g., no copies still on the machine, in the bin, or jammed in the machine).
6. Destroy unacceptable or excess copies by following classified destruction process.
7. Turn the machine off, count to five, and turn machine on again.
8. Run three blank copies to verify there are no latent images remaining (shred blank copies as classified waste).

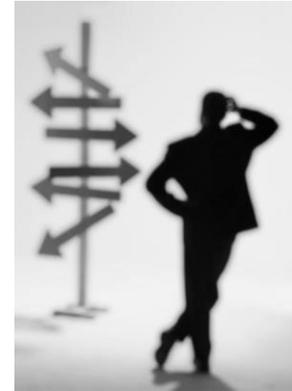
**Afraid you'll forget the steps above?** These are also listed in the CMPC poster posted above or next to the authorized copy machine.

## Module 6: Move Classified Matter

After completion of this module, you will be able to:

- Identify procedures for internal and external movement of classified matter.
- Identify requirements for transmitting classified matter by phone, facsimile (fax), and computer.
- Identify requirements for handcarrying classified matter.

Movement of classified matter always involves risk. As a DOE clearance holder, you are responsible for controlling and minimizing these risks. Since there is a risk of compromise when moving classified, work closely with your CAS. They will help ensure all requirements are met prior to the classified being moved.



### Methods of Movement

Classified matter must only be moved during the performance of official and contractual duties. For the purpose of this course, movement of classified matter is defined as sending or carrying a classified item by any of the following means:

- Mailing (e.g., classified documents and classified cyber media)
- Shipping (e.g., classified parts/components)
- Electronic Transmission (e.g., approved classified email, phone and fax machine)
- Handcarrying

## **Movement of Classified Matter**

Classified matter is moved on a daily basis at Sandia. This movement may be internal (transferred within same SNL site) or externally (transferred to an external customer or different SNL site). There are a number of checks conducted and subsequent documentation that must be created when moving classified internally or externally.

**Internal Transfer:** Your CAS will assist you in identifying and coordinating the transfer with the CAS in the department where you are sending your classified matter. They will check to ensure the final destination is approved to store what you are sending.



**External Transfer:** The destination facility must be approved to store classified matter by the federal government. There must be an approved, active contract with your organization in order to receive classified matter. Finally, the facility and contract must be authorized to receive the level/category/caveat of information you wish to send. This information is captured in the Classified Matter Channel Directory. Your CAS can assist with performing the verification of this information.

In most cases, receipts are required for transfer of classified matter. Work with your CAS to ensure the receipt documentation is prepared and stored correctly.

If you work in the Field Intelligence Element (FIE), contact your Program Security Officer for programmatic requirements for moving classified.

## Movement of Classified Matter

### Shipping and Mailing Classified Matter

There are dedicated departments at Sandia that process the shipping and mailing of classified matter. You and your CAS must use your site's internal resources (e.g., SNL mails services, shipping department, Document Control Office [SNL/CA]; Defense Courier Service for mailing Top Secret and Sigma 14). You must **never** go directly to the U.S. Post Office or Federal Express to send classified matter.



Your CAS can assist with you with meeting packaging requirements for your classified items before mailing or shipping.

### Transmitting classified by Phone or Facsimile (Fax)



Classified matter can only be processed on approved equipment (e.g., Secure Terminal Equipment [STE]). These classified phone lines are approved for a certain classification level and category. Check with your manager to verify what level of classified you are authorized to process on these lines. When faxing classified using an approved fax machine, confirm and document receipt (verbal or written) with your intended recipient.

**Work with your CAS when faxing accountable classified matter.**

## Movement of Classified Matter

### Classified Email

Classified emails can ONLY be sent on an approved classified network (e.g., Sandia Classified Network [SCN]). It's important to know that each classified network at Sandia is approved for a certain classification category and level. For example, the SCN is **not** approved for processing Top Secret or Sigma 14 information.



Some types of classified information have additional programmatic requirements. For example, classified emails (both internally and externally) that contain Sigma 15 information must be encrypted by Entrust (or equivalent encryption method). If you are unsure of what you can process on your system, contact your Cyber Security Representative or Manager.

As of 1 October, 2016 all classified email messages must be marked with the appropriate classification determined by an authorized Email Derivative Classifier (EDC) or Derivative Classifier (DC).

## Movement of Classified Matter

### Handcarrying Classified Matter

The term “Handcarry” in this section, means an individual personally delivers a classified asset to a recipient using an external transfer (e.g., recipient is located outside of SNL, or is located at another SNL location). Due to the risk, handcarry of classified must only be used as a **last resort** when moving classified matter.

Think about all the unexpected situations that could occur when you travel. Canceled flights, stolen bags, and weather delays are a few examples of situations people at Sandia could encounter when traveling.

As was discussed earlier in the module, multiple verifications and documentation must be completed before a classified item can be transferred. When coordinating a handcarry, you should work closely with your CAS.



## Movement of Classified Matter

### Handcarry Documentation

In addition to the standard checks and receipts that must be created when transferring an asset externally, there is additional documentation that must be complete when handcarrying:



- 1. Annual Handcarry Briefing (SF 2902-AHB):** This Sandia-owned form must be completed annually. It documents the rules and requirements you must follow when handcarrying classified and is signed by both the individual authorized to handcarry and their manager. The original should be filed by your CAS and a copy must accompany you when you handcarry a classified item. Contingency phone numbers can be found on this form. Individuals who encounter unplanned issues (e.g., weather delay, lost bag) must contact these numbers for assistance.
- 2. Handcarry Log (SA 2902-ZC):** This log documents all classified items that are in transit during a handcarry in case any unexpected issues are encountered while in transit (e.g., vehicle accident, medical emergency). You must work closely with your CAS to ensure the disposition of your classified asset is captured on this log.

## Movement of Classified Matter

### Handcarry Requirements

Your CAS is not only going to help you ensure your destination is approved to store what you are handcarrying; he/she will also help you prepare receipts and properly package your item (e.g., boxes, envelopes, handcarry bags, etc.). When traveling with classified, you **must** protect your classified item.

1. Never open your classified asset to reveal its contents. Better to miss your flight than to compromise classified information.
2. When you arrive at your location, immediately report to the final destination so the item can be properly secured. Coordinate this with your POC from this facility. If you are delayed or unable to get to the facility, contact the contingency number on your Handcarry Briefing. **Do not store** your classified in a hotel room safe.
3. When flying, place your classified underneath the seat in front of you. This way you can ensure it remains in your control at all times.
4. Classified items that **are not** visually classified (e.g., documents, CDs) can go through the airport X-ray machines. **IF** you handcarry classified material that is visually classified or will be damaged by the airport X-ray machine, work with your CAS to submit the paperwork for alternative screening. This information must be provided to the airport TSA well in advance of your travel day.
5. **DO NOT** handcarry accountable classified information without consulting your CAS. Additional verifications and documentation must be completed before these items may be handcarried.



# Module 7: Destroy Classified Matter

After completion of this module, you will be able to:

- Identify procedures for destroying classified matter.

The volume of classified assets at Sandia should always be kept to a minimum. The more we have, the more time and money we must spend to protect it. A higher quantity also increases the chances of a possible security incident.

This means excess copies and obsolete/unneeded assets should be destroyed as soon as practical. Familiarize yourself with the *Sandia Records Retention and Disposition Schedule*, as some items are required to be retained for a certain period of time. Your CAS and Manager can help.

There are multiple ways to destroy classified and these are dependent on:

- Classification of classified matter (accountable vs. non-accountable)
- Type of classified matter (Document, CD/DVD, hard media, part/component)
- Volume of classified matter

Anybody authorized to deal with classified (e.g., clearance and need-to-know of the matter) can destroy non-accountable classified matter, as long as they are knowledgeable of the approved processes.

Accountable classified has additional requirements for destruction. Work closely with your CAS when destroying accountable to ensure all the appropriate processes are followed.



## **Destroying Classified**

There are multiple, approved options available to destroy classified. These options are dependent on the type of classified you wish to destroy and what type of classified asset are you trying to destroy.

**Classified Document Shredder:** This method is commonly used to destroy smaller amounts of classified documents. Before shredding your classified, it's important that you follow the simple process:

- 1) **Make sure the document is not accountable (does it have a bar code sticker?).** If it does, stop and work with your CAS to destroy this document.
- 2) **Check for “Approved CMPC to Shred Classified” sticker.** DOE has requirements on how large the residue from the shredder must be. This sticker confirms the shredder's residue meets the requirement (1 mm x 5 mm).
- 3) **Shred document and inspect residue.** To inspect the residue, you must sift through the basket of residue to ensure the document shredded correctly. If it did not shred correctly, the bag of residue must be protected and stored as classified.

Following this process is important to ensure each time the approved shredder is used, the residue meets the federal size requirement. Shredders can malfunction, and failure to follow these steps could result in a possible security incident. Residue that is too large is still considered classified and cannot be left unattended.

## Destroying Classified

**Large Quantities of Classified Documents and/or CDs/DVDs:** When you need to destroy a large amount of classified documents, or CDs/DVDs (no other cyber media), work with your CAS to submit a request to have your items picked up. These classified items are stored in red destruction bags, which must be stored in an approved repository before they are picked up.

**Classified Material (e.g. parts, pieces, components, 3-D models) and Cyber Media (e.g., hard drives, laptops, VHS tapes, microfiche):** Classified material may only be destroyed using equipment and processes approved by the CMPC program. Classified material destroyed in an experiment is not considered destruction of classified material. Work with your CAS to identify options to dispose of classified material used in an experiment.



The approved method used by Sandia is permanent burial. When you need to destroy classified material, you must work closely with your CAS so that these items can be sent to the appropriate Classified Work Station (CWS), who will ship these items to the federally approved permanent burial site.

# Module 8: Security Concerns and Emergency Procedures

After completion of this module, you will be able to:

- Identify requirements for reporting incidents or potential incidents of security concern.
- Identify control measures for protecting classified matter during an emergency

## Report Incidents of Security Concern

As a clearance holder, reporting incidents of security concern is one of your most important responsibilities. Some examples of incidents or potential incidents of security concern include:

- Conducting work with classified matter in an area that does not have an approved security plan in place.
- Having a classified conversation on an unsecured telephone line.
- Sending classified e-mail via unsecured means.
- Leaving a classified document or material unattended.
- Failing to properly secure a repository (safe or closed area).
- Having lost or misplaced classified matter.
- Mistakenly share classified information to an unauthorized audience.



## Report Incidents of Security Concern

If you ever have a doubt or suspect an incident:

1. Contact the Security Incident Management Program (SIMP) and use the OOPS process. Do not provide details of the incident on the telephone, pager, email or voicemail as you do not want to inadvertently reveal classified information on an unapproved means.
  - OOPs- Call 311 from your office phone. They will ensure all the appropriate management and applicable staff are notified of the incident.
  - SIMP at SNL/NM and Remote Sites; call 505-283-SIMP (7467); SNL/CA 925-294-9600.
2. Take action to preclude further compromise (e.g., remain with classified matter if you found it unattended or with unlocked repository).
3. Cooperate with SIMP Inquiry Officials or appropriate security program management. **Do not** personally investigate incidents.



### **Control measures for protecting classified matter during an emergency**

During an **emergency**, your life and safety take precedence over the need to shut down equipment or secure classified matter. If it is feasible and safe for you to do so, return the classified to an approved storage repository OR keep in your possession when evacuating.



Once you have evacuated, immediately locate a Security Officer or Incident Commander to inform them you either:

- Have classified in your possession.
- Left classified matter out and unattended.

If you left classified matter unattended, you will be allowed to re-enter the area before the other building occupants. Be sure to inspect the classified matter as soon as building re-entry is allowed to ensure everything is still accounted for.

# Module 9: CWS Manager Responsibilities

After completing this module, you will be able to:

- Identify the tasks included in the oversight of a CWS.
- Identify the tasks included in oversight of a Classified Administrative Specialist (CAS).
- Identify your responsibilities for management of, access to, and use of classified matter.
- Identify your responsibilities for management of classified matter storage.

CWS managers play an important role in the management of classified at Sandia. As a CWS Manager, you are responsible for the classified operations within a CWS. You play a vital role in ensuring classified matter receives the appropriate level of protection for its level, category and applicable caveats.

## Oversight of a CWS

Being the individual who oversees the CWS is a big responsibility. There are individuals – the primary and alternate Classified Administrative Specialist (CAS) – you appoint who will help you and the other members performing classified work within your CWS. They will help with the day-to-day activities within your CWS to ensure you are complying with the policies to properly control, and protect your classified matter. As a CWS Manager, you must also ensure any incidents or potential incidents of security concern are reported to SIMP and to OOPS.



## Oversight of CWS

As the CWS Manager, you will work with your CASs to provide detailed information about your CWS. This information is captured in the Classified Work Station Authorization (CWSA) application (online tool on the SRN). Some examples of information about your CWS captured in the CWSA are:

- Highest level, category and caveat of the classified information processed and stored.
- Type of classified matter stored within your CWS (e.g., documents or material).
- Location of all your approved repositories (e.g., closed areas, GSA-approved safes) that store classified within your CWS.
- List of organizations that your CWS receives classified mail/shipments for.
- Primary delivery location of your CWS (where you receive your shipments/mail).



The CWSA application is the tool you or your CASs will use to submit a change to your current CWS, submit a request to open a new CWS, or submit a request to close an open CWS.

### Oversight of CAS

Changes to your CWS can be submitted by you or your CASs. These changes are made using the CWSA tool. When a CAS submits a change, an automated workflow process begins. For significant changes, you will be sent an email with a link to CWSA that will provide information about the change, as well as the ability to approve or reject.

Approver Site	Request Status	
NewMexico	Draft	Actions ▾
California	Pending CWS Manager Approval	Actions ▾

Data in the CWSA is used for assessments and audits. It's important that this information always be kept current. The Classified Matter Protection and Control (CMPC) Department can assist if you or your CASs has any questions accessing or making changes within the CWSA application.

When you appoint a new Primary or Alternate CAS, you must verify he/she has the appropriate authorization (e.g., security clearance, Sigma access [if applicable]) and ensure he/she completes the required CAS training.

When a new CAS is appointed, you must assist in their transition and help them get familiar to the classified operations within your CWS.

Providing CASs with the authority, support, and time to perform their duties is vital to the success within a CWS. Protection of classified matter is critical and the CAS's efforts to run an effective CWS must be supported by the CWS Manager.



### **Management of, Access to, and Use of Classified Matter**

As a CWS Manager, you will work closely with your CAS to ensure all individuals working with classified within your CWS are appropriately trained and knowledgeable of the requirements. This includes careful control of classified matter, and ensuring that only authorized individuals have access.



One example of controlling classified is authorizing who in your CWS is authorized to send and receive classified mail (documents).

At SNL/NM the CWS Manager identifies these individuals on the [SF 2900-CMD, Classified Mail Delivery Posting](#). Individuals on this form must have the appropriate access authorization and have access (e.g., combination) to an approved repository so the item can be stored when it is received. Classified Couriers use this poster to verify you are authorized to receive mail before relinquishing control of the item.

As the CWS Manager, you are the key decision maker in deciding who can and cannot access classified matter. These decisions include:

1. **Need-to-Know:** You may be asked by your CAS to confirm need-to-know to an individual before they can access classified matter.
2. **Security Clearance:** You will ensure only individuals with the appropriate security clearance access the classified information within your CWS.
3. **Programmatic Access:** Your CWS may include work for special programmatic requirements that may include additional access policies (e.g., Sigma 14, 15, 20 Access List, Special Access Programs [SAPs]). Notify your CAS about who has access to the classified within your CWS.
4. **Security Repository Access (GSA-approved safes, Closed Areas):** You will help your CAS ensure that repository access (e.g., combination) is restricted to authorized personnel only. This access should be kept to a minimum.

### **Review of Classified Holdings**

Classified holdings should always be kept to a minimum. A review of holdings is required to be performed by each CWS once every 12 months. You will work with your CAS to facilitate this review. Results must be documented and stored with your CWS records.

### **Management of classified matter storage**

The previous page mentioned determining who can access your repositories that store classified matter. Whenever an individual no longer needs access to a repository the combination must be changed. Common examples of situations that warrant a change to the combination include:

- Individual with the combination leaves Sandia (retires, quits, fired).
- Individual with the combination receives clearance downgrade or clearance suspension (no longer authorized access to repository's contents).
- Individual with combination no longer has NTK for items stored in the repository.
- Individual with the combination no longer fulfills programmatic requirements (e.g., no longer of Sigma 14, 15, 20 Access List).
- Potential compromise of the combination or classified matter within the repository.



As CWS Manager, you must work with your CAS to ensure all the required documentation for storage of classified (e.g., SF 700, SF 702) are complete.

### **Management of classified matter**

CWS Managers of CWSs that are approved to store accountable classified matter (e.g., TS, Sigma 14, Designated United Kingdom assets) must ensure their CAS completes the required annual inventory. The CWS Manager should assist the CAS by communicating the temporary halt in activity to members of the CWS so the physical inventory can be conducted.



Each CWS will be assessed to verify all corporate and federal requirements are being met. As CWS Manager, it's important that you work closely with your staff and with your CAS to ensure your CWS is in compliance.

### **Annual Handcarry Briefings**

Some CWS Managers have individuals within their CWS who handcarry classified assets externally (to a site with a different facility code). These CWS Managers must ensure individuals performing these handcarries are aware of their responsibilities. Both the individual and the CWS Manager sign the [SF 2902, AHB, Annual Handcarry Briefing](#). This document is kept in the CWS records by the CAS and must be re-signed annually.

**SEC301**  
***Classified Matter Training, Final Test***

**Printed Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_ **Org. #:** \_\_\_\_\_

**To receive credit, complete this test and scan and email it to [security@sandia.gov](mailto:security@sandia.gov) or FAX it to (505) 845-0607. Please print clearly and include your middle initial so credit can be given the correct person.**

**Directions: Circle the correct answer for each question.**

Module 1:

1. Which of the following are the three DOE classification levels?
  - a. Top Secret, Secret, Formerly Restricted Data
  - b. Top Secret, Secret, Confidential
  - c. Secret, Restricted Data, Confidential
  - d. Restricted Data, Formerly Restricted Data, National Security Information
  
2. A report was written and marked as SFRD Sigma 15. Which of the following is the report's category?
  - a. Secret
  - b. Formerly Restricted Data
  - c. Sigma 15
  - d. None of the above
  
3. Which of the following is classified?
  - a. A resume marked UCI
  - b. A CD marked as Secret Formerly Restricted Data
  - c. An email identified as OUO
  - d. A database printout marked UCNI
  
4. Classified matter must be marked with classification level, category (if RD or FRD) and caveat. In circumstances when the item cannot be marked, a container/bag in which the item is stored can be marked.
  - a. True
  - b. False
  
5. Information that has been determined to be accountable (e.g., marked with bar-code sticker with a unique identification number), must be tracked and inventoried.
  - a. True
  - b. False

Module 2:

6. You have a Q-clearance. In addition to the need-to-know, you must meet additional requirements (i.e., be on an access list) to access which of the following?
  - a. Secret Formerly Restricted Data
  - b. Confidential Formerly Restricted Data
  - c. Secret Restricted Data Sigma 15
  - d. Confidential Restricted Data
  
7. Which of the following can an L-cleared individual with a need to know access?
  - a. Secret Restricted Data (SRD)
  - b. Top Secret National Security Information (NSI)
  - c. Secret Formerly Restricted Data (SFRD)
  
8. Who determines need-to-know?
  - a. Security Incident Management Program (SIMP)
  - b. Classified Matter Protection & Control (CMPC)
  - c. Owner/Holder or the manager of the department that owns the classified
  - d. Sandia's Need-To-Know special operations team.
  
9. It is a violation of the Department of Energy's "No Comment" policy for a Sandia employee or contractor to confirm, deny, or expand on the classification status of information or the accuracy of unauthorized public disclosure.
  - a. True
  - b. False
  
10. Which of the following is **not** a protective measure that must be followed when working with classified?
  - a. Relinquish it only to individuals with proper access authorization and need-to-know
  - b. When in a Limited Area, lock your classified in your desk when it is not being used.
  - c. Return classified to an approved repository (GSA-safe, closed area) when you complete your work.
  - d. Maintain appropriate control of classified matter in your possession
  
11. When hosting a classified meeting you must perform all of the following except:
  - a. Verify participants have the appropriate access authorization and need-to-know
  - b. Ensure approved portable electronic devices are removed from the area (per corporate policy)
  - c. Contact CMPC program for permission
  - d. Start meeting by announcing the classification being discussed
  
12. A Classified Administrative Specialist (CAS) is a local resource who can help me:
  - a. Assist with classified marking questions
  - b. Assist with the transfer of classified matter to another Classified Work Station or to an external customer.
  - c. Identify a safe or closed area approved to store your classified matter.
  - d. All of the above

Module 3:

13. Who is the recommended resource for determining what is classified in a particular subject or program?
  - a. Your Classified Administrative Specialist (CAS)
  - b. Your co-worker
  - c. Your OAA, SMA, or OMA
  - d. Your manager and/or Derivative Classifier (DC)
14. Who makes the classification determination of a finalized classified document?
  - a. The creator of the document
  - b. The closed area custodian
  - c. An authorized Derivative Classifier (DC)
  - d. Your Classified Administrative Specialist (CAS)
15. You may create classified files on a computer using the:
  - a. Sandia Restricted Network (SRN)
  - b. Sandia Open Network (SON)
  - c. Sandia Classified Network (SCN)
  - d. Sandia Common Operating Environment (COE)
16. When are you required to have a draft document (non-TS) reviewed by a derivative classifier and marked as final?
  - a. When it is permanently filed
  - b. When moved outside the office, team (working group, or department that created it)
  - c. More than 180 days from the last date it was updated
  - d. All of the above
17. Mark classified drafts created via the computer at the classification level and category which the computer system is accredited to process until reviewed by a Derivative Classifier (DC)
  - a. True
  - b. False

Module 4:

18. When locking an approved repository (GSA-safe, closed area) for the day, the individual who locked the repository can be the same person who checks the repository.
  - a. True
  - b. False
19. Which of the following **is not** an approved storage container for classified matter?
  - a. GSA-approved security container (safe)
  - b. An approved closed area
  - c. In any locked desk drawer in a Limited Area
  - d. An approved vault

20. Repositories must be checked daily IF personnel with combinations are working in the area.
- True
  - False
21. The combination for a classified storage container must be changed when any of the following occur, EXCEPT:
- Individual with combination gets a clearance downgrade or clearance suspension
  - Compromise or suspected compromise of the repository's combination
  - An individual with the combination leaves Sandia for another job
  - A new member joins the department

Module 5:

22. When is a stand-alone copy machine approved for classified copying/reproducing?
- The machine is marked "Classified Copying Prohibited"
  - The machine is located in a Limited Area and has a sticker approving its use for classified copying
  - The machine is located in a locked room in a Property Protected Area (PPA)
  - The machine is marked "Unlimited Release Approved"
23. Which of the following is a step found on the CMPC poster posted above copy machines approved for classified copying?
- Never leave copy machine when copies are being made
  - After completion of making a classified copy, turn machine off, count to five, and turn machine on again.
  - Run three blank copies to verify there are no latent images remaining (shred blank copies as classified waste)
  - All of the above are steps listed on the CMPC poster.

Module 6:

24. Movement of classified matter is only allowed in the performance of official and contractual duties.
- True
  - False
25. When moving classified externally work with your CAS to verify the destination is approved for use in the Classified Matter Channel Directory.
- True
  - False
26. It is important to work with your CAS when coordinating an internal transfer, to ensure the final destination is approved to receive and store what you are transferring.
- True
  - False

27. All of the following are requirements for handcarry, EXCEPT:
- If an individual encounters any unplanned issues (e.g., weather delay, lost bag), they must contact the contingency number found on the Annual Handcarry Briefing form.
  - Individual using handcarry must carry a copy of the Annual Handcarry Briefing form (SF 2902-AHB) with them during their travel.
  - when you arrive at your location, immediately deliver the item to your destination location for proper storage
  - if you are delayed and unable to deliver your item to its destination, drop your classified off in a FedEx box.
28. Classified faxes can only be sent on \_\_\_\_\_ :
- Any fax machine purchased with an SNL p-card
  - Secure Transmission Equipment (STE) (classified phone lines)
  - Any fax machine located inside the Limited Area
29. To transmit classified matter electronically via computer (i.e. email), you must:
- Phone the recipient to advise that a classified email will be sent using the Sandia Restricted Network (SRN).
  - Only send classified email messages on an approved classified system
  - Mark all emails sent on classified computing systems
  - All of the above
  - B and C only

Module 7:

30. When shredding a classified document, you must:
- Make sure document is not accountable (accountable documents can only be destroyed by your CAS)
  - Check shredder to ensure it has been approved by CMPC and meets federal requirements to shred classified.
  - After shredding non-accountable document, open basket below and inspect residue to ensure it shredded correctly.
  - All of the above
31. To dispose of classified material (parts, pieces), you must:
- Use equipment or processes approved by Shipping and Receiving
  - Use equipment or processes approved by Classified Matter Protection and Control (CMPC)
  - Use equipment or processes that ensure classified markings have been removed.

Module 8:

32. All of the following are examples of incidents of security concern that need to be immediately reported, EXCEPT:
- a. Conducting work with classified matter in an unapproved area
  - b. Leaving a classified document or material unattended
  - c. Performing SFRD classified work on the Sandia Classified Network (SCN)
  - d. Mistakenly sharing classified to an unauthorized audience
  - e. Having a classified conversation on an unsecured telephone line
33. Report incidents of security concern to:
- a. your Classified Administrative Specialist (CAS)
  - b. the Classified Matter Protection and Control Department
  - c. your local Badge Office
  - d. SIMP and OOPs
34. In an emergency, the need to shut down equipment or secure classified matter takes precedence over the health and safety of personnel.
- a. True
  - b. False

IF you are a Classified Work Station Manager, proceed to the next page.



## Additional Quiz Questions for CWS Manager

The questions below are for individuals who are Classified Work Station (CWS) Managers.  
Circle the correct answer.

### Module 9:

1. Detailed information about your CWS is captured in the Classified Work Station Authorization (CWSA) application.
  - a. True
  - b. False
  
2. Which of the following is an example of the information found in the CWSA application about your CWS?
  - a. Highest level, category and caveat (if applicable) of classified information processed and stored.
  - b. Location of all your approved repositories (e.g., GSA-safes and closed areas)
  - c. List of organizations that your CWS receives classified mail for
  - d. Primary delivery location for your CWS
  - e. All of the above
  
3. As CWS Manager, you must appoint a Primary and Alternate CAS\_\_\_\_\_ :
  - a. that has completed required CAS training.
  - b. that possesses the appropriate access authorization (e.g., security clearance, Sigma access [if applicable]).
  - c. and assist in their transition to their new position (e.g., familiarize them with classified operations within CWS).
  - d. All of the above
  
4. Some of your responsibilities for management of, access to, and use of classified matter include all of the following EXCEPT:
  - a. respond to need-to-know inquiries from your CAS
  - b. help your CAS with repository access (e.g., approve who is granted access to combination)
  - c. submit clearance documentation for all individuals within your building
  - d. if your station has programmatic requirements (e.g., stores Sigma 14, 15, 20), ensure additional requirements are met before giving an individual access.
  
5. You must work with your CAS to ensure the combination of a repository (e.g., GSA-approved safe, closed area) is changed if which of the following occur.
  - a. Individual leaves Sandia (retires, quits, terminated)
  - b. Individual with combination receives clearance downgrade or clearance suspension
  - c. Individual with combination no longer has need-to-know for items stored in repository
  - d. Potential compromise of combination or classified matter
  - e. All of the above