SEC301 – Full Course Transcript

Introduction Module

Thank you for taking time out of your busy schedule to take this class. You may be wondering why this course was assigned to you? This class is required for members of the workforce who hold a Q-clearance. Because you have a Q-clearance, you have the potential to encounter and handle classified. Managers may also assign this training to L-cleared individuals who work with classified. Your current responsibilities right now may or may not include handling classified but because you have a security clearance, that could potentially change in the future.

Our nation's security depends on the protection of sensitive information. Because you have a DOE security clearance, it's crucial that you are aware of how to properly handle classified matter and make sure it is always safeguarded. Knowledge of these policies is crucial to ensure this important information is always protected.

If your current work does not involve classified and you don't believe there is any potential of encountering classified in the future, please contact the Personnel Security Office to discuss the process to downgrade your clearance.

This course has a 24-month refresher requirement. If you just received your Q-clearance, you will learn the basic policies associated with protection of classified. If you have had your Q-clearance for a while, this training will ensure that you are still knowledgeable of these important policies, including any updated policies or procedures.

This class may take up to 90 minutes to complete. But don't worry, if you are already knowledgeable of these policies, you can complete the test-out quiz available at the beginning of each module. This will significantly cut down the time required to complete the course. Don't worry if you are not able to complete the training in one sitting. If you need to take a break, or attend a meeting, you can either leave your browser open or simply close it and come back to the training later. When you come back to the class you'll be able to pick up where you left off.

This course includes narration throughout so please be sure you have your speakers or headphones set to hear the audio. You can also view the transcript by clicking on this icon. Feel free to use the back arrows on each page to go back or use the media player to pause or rewind when necessary.

There are many important policies associated with protection of classified. If you don't work with classified frequently, you may forget. Resources will be provided in this course at the end of each module. Please consider bookmarking the links to the resources as they may come in handy in the future. These resources are available on the internal Sandia Restricted Network. If you are a PO Contractor or sub-contractor, feel free to work with your Sandia Designated Representative if you have questions or would like to access the resources.

If there are any discrepancies between this training and Sandia's lab policy, always follow the applicable lab policy.

Always remember that having a security clearance comes with very serious responsibilities for protecting our nation's classified information. Thank you for taking the time to learn what you need to know to make sure that classified is always safeguarded appropriately.

Module 1 – What does "classified" mean?

Learning Outcomes
In this module, we'll take a look at what classified means. You'll find out what makes documents and materials classified, how you will know if something is classified and who can help you identify classified in your daily work. Let's get started.

Congratulations
Congratulations, Justin! Now that you have your clearance, you are likely to be working with classified information. Depending on your assignments, your job may now include creating and working with documents and other materials that must be reviewed for classification. That's why everyone with a clearance needs to understand the requirements of dealing with classified here at Sandia. Being the holder of a security clearance comes with great responsibilities. It will be up to you to make sure that classified information is always protected to maintain our nation's security and make sure that we never lose the trust that the Department of Energy places in Sandia to safeguard some of our country's most sensitive information. The policies for protection and control of classified come from the federal government and are outlined in detail in Sandia's Laboratory Policy System. If there is ever a discrepancy between the Laboratory Policy System and this training, always follow the requirements in the Laboratory Policy System. Now, let's get started by taking a look at what we mean when we say that something is classified.

What does classified mean?
Sandia deals with sensitive information daily and much of it is classified. Classified is information that the federal government has determined must be protected. In the interest of national security, access is restricted to people with the necessary security clearance and need-to-know (NTK).

Sandia deals with all types of classified including documents that range from formal reports and design blueprints, to informal handwritten notes. We also deal with classified computers, electronic storage media, and other types of equipment that has storage capability. We deal with material that may be classified due to its dimensions, composition, or association with a particular project and discussions that contain classified information take place regularly.

How do you know something is classified? (Levels & Categories)
When working with classified information, a classification level and category must be identified. The classification level and category let us know how we must control and protect classified assets, and also tell us what type of information we are dealing with.

Classification levels tell us how sensitive the classified information is. The level identifies the degree to which national security could be damaged if the classified matter were to be disclosed without proper authorization. There are three levels of classification:

Top Secret or TS means that unauthorized disclosure of this information could reasonably be expected to cause exceptionally grave damage to national security. Due to the criticality of this information, much more rigorous federal requirements exist for protection and control of Top Secret.

Information identified with the classification level Secret means unauthorized disclosure could reasonably be expected to cause serious damage to national security.

If matter is classified as Confidential, unauthorized disclosure of this information could reasonably be expected to cause damage to national security. You may have seen the term “confidential” used in private industry such as banks and insurance companies who use it to indicate that information is sensitive. However, it is important to note that private industry does not use the term in the same context as government classified. At Sandia, anytime you work with Confidential, you must treat it as classified.

In addition to identifying the classification level, the classification category of information must be identified. The category tells you what type of information you are dealing with. Here at Sandia, we primarily use three categories of classification. They are Restricted Data, Formerly Restricted Data and National Security Information.

Restricted Data or RD, is the most access restricted classification category. 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 or 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 or NSI is information that is important to national security for reasons other than those in the RD and FRD categories and it is classified in accordance with Presidential Executive Order. Examples of NSI include information related to military operations, foreign government information, intelligence-related activities, and economic or scientific information associated with national security.

Because Restricted Data and Formerly Restricted Data are associated with information related to the design and use of nuclear weapons as well as information associated with special nuclear material, RD and FRD information is primarily produced by individuals who perform work for the Department of Energy and the National Nuclear Security Administration. Because National Security Information includes broader areas of information, the majority of United States federal agencies and contractors work with NSI. At Sandia, work is performed in all of these classification categories

A fourth category of information exists called Transclassified Foreign Nuclear Information or TFNI. TFNI involves information on atomic energy programs of other nations and can be adequately safeguarded in a manner similar to NSI. This information is very rare at Sandia and in most cases is unique to special program areas. Speak with your Program Security Officer if you have any questions about working with TFNI.

What are caveats?

So now that you know about classification levels and categories, let’s talk about some instances where additional classification guidance is given. Some classified, but not all, may also include a caveat. Caveats

are designations from classification guidance used to indicate additional access or dissemination restrictions. Common examples you may see at Sandia include "NOFORN," meaning the information cannot be shared with a foreign national individual or foreign government. Another common caveat is Sigma 15, which has additional access restrictions and requirements that are controlled by SNL's Use Control Office

How do we use classification levels and categories?
At this point, you may be asking yourself, what do I do with classification levels, categories and caveats and who determines what they are?

First, classified must have both a classification level and category, which are paired together and then marked accordingly. For example, a document containing the classification level Secret, and category Restricted Data would be Secret Restricted Data or SRD. Marking the classified is very important so individuals are alerted to its presence and have the information they need to appropriately safeguard and protect it. We'll discuss this more in later modules as there are different requirements associated with the various activities involving classified like storing, moving, and destroying.

Who determines if information is classified?
Now that you know what classification levels, categories and caveats are, let's discuss who actually makes the decision about whether or not something is classified. At Sandia, we have individuals called Derivative Classifiers or DCs. These DCs receive training and have access to classification guidance that they use to help them determine the appropriate classification level, category and caveat if applicable. These DCs are only authorized to review specific matter in their area of expertise. Sandia's Classification Office provides the DC training, access to the appropriate classification guides, and grants them authority to make classification decisions.

There is also a population of individuals who are called Email-Only DCs or EDCs. Email-Only DCs are individuals with classified computing email capabilities. EDCs take training and use classification guidance to determine the sensitivity of emails they send on classified computing systems. Email-Only DCs are only authorized to review the emails that they themselves compose and send. This authority to determine the classification of their own emails is limited to their area of expertise.

Need to find a DC? Want to become a DC or EDC?
To find a DC or to submit a request to be a DC or EDC, visit the Classification Office's Jupiter website.

What if it's not classified anymore?
Sandia has many classified documents from years past. If you are uncertain that the information is still classified, you must engage a Derivative Declassifier or DD. These individuals are different from a DC and are found in the Classification Office. Derivative Declassifiers help with both declassification reviews and downgrades of classification.

Identify Classified Matter in Your Subject Area
Working with classified subject areas is challenging, as you must have a solid understanding of what is potentially classified and what is not. Security incidents have occurred involving individuals who inadvertently disseminated classified information by unapproved means. Your manager and your local DC are your best resources to discuss what is potentially classified in your work activities. There are also

classification briefings on specific subject areas available to help you understand your classified work. Talk to your manager for more information. The SNL Classification Office Helpline (505-844-5574) is also available to answer your questions.

On-the-Job Training (Knowledge Check)
Now that you have a better understanding of classified matter, help Justin decide what he needs to do in order to protect classified appropriately.

Accountable Classified Matter
Some very specific classified matter requires stricter controls. These controls include specific classified information that must be carefully tracked at all times and inventoried annually. This information is called accountable classified information. All Top Secret classified physical assets such as printed documents, storage media, etc. are considered accountable classified.

Some other types of information are considered accountable because of national, international or programmatic requirements. Some examples include: Sigma 14, designated United Kingdom, and North Atlantic Treaty Organization (NATO) ATOMAL.

So exactly what are the additional controls for accountable classified matter? All accountable matter has an additional marking which is an SNL issued barcode sticker that has a unique identification number. This unique ID is affixed to the accountable asset and is used for entry into the required SNL accountability database. This database is used to track the exact storage location of the asset. The database is used to perform required physical inventories that are facilitated by an individual called a Classified Administrative Specialist or CAS. If accountable classified is removed from the storage location, you must work with a CAS so they can track its location. If accountable classified is ever received or DC'd, you must immediately work with a CAS to ensure the item is entered into the accountability database.

You'll learn more about the CAS in the next module as they are going to be a tremendous resource for you to ensure that you are following all the requirements to protect classified.

So, how does accountable classified impact you? Only a small percentage of the classified holdings at SNL are considered accountable. If you deal with accountable classified, you must work closely with your CAS to ensure this classified is controlled correctly and inventory records are always accurate.

Classified that is not considered accountable must still be carefully protected and stored, but it is not required to be tracked in a database and inventoried annually.

Resources
These resources can provide helpful information if you ever need assistance in dealing with classified.

Module 2 - Classified at Sandia

Learning Outcomes
Now that you understand what classified is and the different types of classified matter that exist at Sandia, let's talk about some of the terms that are specific to working with classified here at Sandia and identify the resources that are available to help you follow requirements for protecting and controlling classified.

What is a CWS?
Sandia has multiple locations throughout the United States, and each is unique in the type of classified projects that take place. At Sandia we utilize a term called a "Classified Workstation" or "CWS". Some people hear the word "workstation", and think it means computer or office, but that's not the case here. At Sandia, a CWS is an area where classified is processed and stored. In most cases, this includes multiple locations within a building or in multiple buildings located in areas approved for classified work.

CWSs are used at Sandia for multiple reasons. CWSs provide an efficient way to conduct audits that ensure Sandia protects classified in compliance with federal policy. Treating classified work areas as one cohesive CWS also aids in the retention of required documents and federal forms. CWSs are also utilized to help Logistics facilitate movement of physical classified from one location to another.

In most cases, each organization at Sandia does not need its own CWS. One CWS will often cover multiple organizations and different projects. Within each CWS, access to classified matter is protected so that only those with appropriate clearance and need-to-know have access to approved storage locations.

In addition to CWSs, at some SNL sites, there are unique areas that also process classified but follow specific federal requirements for their operations. These are Special Access Programs or SAPs and Sensitive Compartmented Information Facilities or SCIFs. These areas have Program Security Officers who are your primary resource for any questions you may have about the different requirements in those programs.

Classified Administrative Specialist
Each CWS has a primary Classified Administrative Specialist or CAS and at least one alternate CAS. These are individuals who take additional training, are knowledgeable of available resources and can help you with day-to-day classified operations.

Your CAS can help you work with classified in a number of ways. He or she can assist with marking classified matter, help you identify an approved location to store classified, assist with moving classified, and lastly help with destroying classified. And remember that CASs MUST be engaged if you work with accountable classified matter to make sure that the inventory database is current.

With the exception of a few special programs, if your work involves classified, it falls within an established CWS and has CASs assigned to help. If you are unsure who your CAS is, talk to your manager.

CWS Manager
Each CWS at Sandia has a manager who must be from any level of management. The CWS Manager is the designated POC for the CWS. CWS Managers work with the other organization managers who utilize

the CWS and help ensure day-to-day operations are in compliance with security policy. This includes identifying the CASs for the CWS, as well as approving modifications to the CWS in the Classified Workstation Authorization application.

The CWS Manager also assists with CWS audits and assessments and works with affected organization managers and/or staff to address any issues identified.

Deployed Security Professional and Embedded Security Professional
Another resource to help you with classified activities are individuals called Deployed Security Professionals or DSPs and Embedded Security Professionals. These individuals are assigned to Centers and Divisions and partner with you to help accomplish your work while complying with security policies. These individuals are knowledgeable in both security policies and the work being conducted by your organization. They help identify risk in day-to-day work and create solutions to avoid security incidents. They can also help you with any security-related questions.

Security Connection
We've discussed a number of people who can help you if you ever have questions about policies associated with protecting classified. Sandia also offers a very valuable security resource known as Security Connection. Security Connection includes both a telephone help line and a website within the Sandia Restricted Network or SRN.

Reaching the helpline is as simple as dialing 3-2-1 from any Sandia desk phone or 505-845-1321 from any other phone. The Security Connection operator who takes your call will either provide an immediate answer to your question or will reach out to the appropriate security department on your behalf and get an answer for you quickly. Calling Security Connection can save you time in finding answers to your security-related questions.

Security Connection also hosts a website on the SRN. You can use this site to find helpful information on a variety of security-related topics.

Classified Matter Protection and Control
The Classified Matter Protection & Control or "CMPC" team ensures classified matter is properly controlled and protected at Sandia by providing guidance and training, interpreting DOE orders and Federal regulations and routinely assessing the workforce. This team can provide assistance with any policy-related issue associated with protection and control. CMPC's resource website contains useful links to a variety of manuals, websites, documents and more. Most helpful when working with classified are the Classified Workstation Manual and the Classified Marking Guide. These two documents contain detailed information on various topics to help you protect your classified matter. CMPC can be reached directly at cmpc@sandia.gov. Send them an email if you need help.

Protecting Classified Depends on YOU
All these individuals and resources can help you with your day-to-day work associated with classified. While they are helpful, these resources are not solely responsible for ensuring that CWS operations are in compliance with CMPC policies. By virtue of having a security clearance, YOU are ultimately responsible for abiding by all security polices and protecting classified information.

If you ever find yourself in a situation involving a classified activity and you are unsure on what to do, call a time-out and contact one of the many resources available to you here at Sandia!

Resources
Always remember that it is very important that you know which information sensitivities are involved in your work. If you are unsure, contact your manager, your authorized DC or the Classification Office. Visit Jupiter website to find your DC. If you work with classified, talk with your manager to find out who can help you and keep the resources listed below handy.

Module 3 - Creating Classified

Learning Outcomes
In this module, we'll take a look at how different types of classified are created. We'll discuss the basic concepts related to marking classified and what other requirements you need to follow when creating the various types of classified matter that may be part of your daily work at Sandia.

Creating Classified
Let's now focus on the requirements associated with creating classified. All Information that is potentially classified must be marked and protected as such. Think of it this way, if you have two documents, one is classified and one is not, without markings how would you know which to protect? We must mark these items to both alert others to the presence of classified and to provide information on how it must be protected. We also need to indicate which DC made the classification determination, and what classification guidance they used.

Classified Documents:
Let's start with classified documents. Documents are considered any type of recorded information regardless of what form they are in. They may be a compilation of information from various sources, data from experiments, or original ideas from experience and/or knowledge. Documents can be both physical items as well as electronic files stored on computing systems. Classified documents include any of these examples.

When creating a document, federal policy requires that we mark the document with the highest potential classification we believe it contains. If you are unsure of the classification, talk to your DC.

If you must work on a document that has already been DC'd and marked as final, per SNL Classification Office policy, it must be reviewed again by a DC when you add technical or programmatic content OR if you believe the sensitivity identified is not correct.

If you are just beginning to create a classified document and it has not yet been reviewed by a DC, it is considered a draft. The author is responsible for identifying the highest potential classification of the draft and making sure that it is marked as such. Federal policy requires that the official classification eventually be identified. This means classified drafts must be reviewed by an authorized DC and marked with final classification when one of the following occurs:

1. It's been 180 calendar days from last entry.
2. The document is shared outside the ad hoc working group. OR
3. The document is filed permanently.

For more details about when and how classified drafts must be reviewed by a DC, check out the Classified Marking Guide and the CWS Manual on the CMPC resource page. You'll find more information on what an ad hoc working group means, as well as old marking requirements and when older documents have to be re-marked to current marking requirements. And remember that you can learn how to mark classified in more detail by taking SEC303, Classified Marking Training.

Classified Computing:
Creation of classified documents most often takes place on a computer. Classified and potentially classified information must only be processed on approved computers and networks that meet rigorous requirements to make sure that the information is controlled and protected. Many different classified networks and stand-alone computers exist at Sandia that process various classification levels and categories. The highest level and category of information each classified system is authorized to process is referred to as "system-high." For example, system-high for the most commonly used classified computing network, the Sandia Classified Network or SCN is Secret Restricted Data. This means that while working on the SCN, you cannot process any information with a classification that is higher than SRD. If you needed to work on information classified as Top Secret, you would need to find another system authorized for processing Top Secret.

If you are going to perform work on a classified computer, you must know the highest classification the computer can process before you start. Some computers have storage capability and some do not. Those with storage capabilities must be marked and protected as classified. For more information about the classified computer you work with, contact your Cyber Security Representative or CSR. CSRs have knowledge of the security plans associated with the different classified stand-alone computers and networks and can tell you what the classification limitations are. They can also help you if you have questions about computing-related equipment such as printers and scanners.

Passwords to classified stand-alone computers and networks must be marked and protected at system-high. These passwords allow you access to classified information and must also be protected as classified. You are the only individual who should have knowledge of your classified password. Therefore, the password must be stored in a sealed, opaque envelope that is also marked and protected at system-high. You must also sign or print your name across the envelope seal in order to detect if the envelope has been tampered with.

Classified Email:
All emails sent on classified networks must be reviewed and marked with the appropriate classification. This includes both classified and unclassified. It also means that if you are responding to an email chain, you must review the entire email string when identifying the classification sensitivity.

All individuals with Outlook capabilities on a classified computing system must complete training to be an email-only Derivative Classifier or EDC. This limited authority allows EDCs to review and mark the emails they send only if the message contains content within their area of approved authority. This EDC training is accessed through Jupiter, which is an application owned by the Classification Office.

Classified Storage Media:
When working with classified computers, you may have a need to create electronic storage media. Examples of this media may include a CD, DVD or removable hard drive. Policies and capabilities for creating media vary for each classified computing network or stand-alone computer. Your Cyber Security

Representative can help you understand the rules for the computer and networks you use to create media.

When media is connected to a classified computing system, it must then be marked with the system-high classification markings and protected as such. If the media needs to be marked at a lower classification because the information it contains is lower than system high, an authorized DC must be consulted and an authorized transfer point or ATP must be used to make sure that no data has been unintentionally added to the media. Your Cyber Security Representative can assist you if you need to locate an ATP. To ensure that media is not left unprotected, cases holding media must also be marked with appropriate classification markings. The cases are considered unclassified when the media is not inside the case.

There may be times when you have to transfer or move information off of a classified computer. Depending upon the situation, there are various options available to facilitate the process. A common example is called the Downshift process which helps with movement of unclassified information from the Sandia Classified Network (SCN) to the unclassified Sandia Restricted Network (SRN). This process includes an ATP and must also include an authorized DC to make sure that the information flowing down from a classified network to an unclassified network is truly unclassified information.

Classified Equipment:
Technology is quickly evolving and some equipment used for classified projects may have the potential to create and store data. Examples include oscilloscopes, calibration devices, and cameras.

Equipment with storage capabilities must be marked with the highest potential classified information they contain and protected as such. This type of equipment is referred to as Operational Technology or OT. If such equipment is used for classified projects and is later needed for unclassified projects, the memory must be cleared prior to use to be sure it is cleared of any classified data. Cyber Security's website provides guidance on how to request approval for the clearing procedure, how to mark the equipment, and other important OT information.

One piece of equipment that you may have a need to use is a stand-alone classified copy machine. These copy machines are not connected to a network and are present in the limited area. Before using the equipment, be sure that it has signage stating it's approved for classified use. A poster will be located by these machines and provide instructions on how to clear the memory after making copies so that no classified is still in the memory of the equipment.

Some equipment may have capabilities that are prohibited. These could include Wi-Fi or Bluetooth technology. These controlled articles are prohibited unless approval is received by using the Controlled Article Registration Process or CARP. See the CARP website for more information.

Classified Material:
Your work at Sandia may also involve classified material. Classified material may be a part or piece that is considered classified because of its dimensions, association with a classified project, or the material that it is made of. Classified materials include, but are not limited to, chemical compounds, metals, fabricated or processed items, or any combination that contains or reveals classified information.

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. If

the material is NSI, the NSI category marking is not required. Markings on classified material must be visible, regardless of the angle or positioning of the material. If items cannot be marked, the container holding the item may be marked. This is helpful for very small items**.**

When marking is not practical, written notification of the markings must be furnished to recipients. Material is not required to have the DC information as that information is captured on the associated blueprint or design documentation.

There may be instances where your work involves assembly of multiple pieces to form a larger piece of classified material. In those instances, we must make sure that the larger assembled material is marked with the single highest classification level and single highest classification category of the assembled piece and protected it accordingly.

Accountable Classified:
As you may recall from module 1, accountable classified is matter that is required to be tracked from cradle to grave and physically inventoried annually. Examples are Top Secret physical matter or other classified that is required to be tracked as accountable due to special program requirements such as Sigma 14 and Designated United Kingdom classified. If you create this type of classified, remember to work closely with your CAS to ensure that matter is tracked in the accountability database.

Classified Association/Compilation Risk:
One area to be very cautious of is classified association or compilation. This risk exists when working with both classified and unclassified information. When information is compiled, it could reveal information of greater sensitivity than any of the individual bits of information separately. When compiled information is determined to be classified, it must be handled and protected at the appropriate classification.

For example, you should be sure to use caution when writing emails or responding to email chains on unclassified computing systems. An unclassified email could become classified simply due to the associations made in the thread of related messages. Consult your DC if you have any questions or concerns about compilation or association risks with your work. If there are risks, utilize an approved classified computing system.

Remember…
Your work in classified may involve one or many of the different types of classified matter. It's imperative that you are always familiar with the sensitivities of information that you are dealing with. If you are ever unsure, consult your DC or your manager.

When working with your DC, it is very important that you always communicate in person, or via a secured means. Do not discuss classified on an unsecured phone or on an unclassified computer because discussing potentially classified information using an unsecured method could result in a potential compromise of classified information and a security incident.

On-the-Job Training
Now that you have a better understanding of the requirements involved in creating classified, let's work through a scenario that Justin encounters as he takes the necessary steps to send classified emails at Sandia.

Resources
Depending on what type of classified you work with we encourage you to take a look at the resources below and considering bookmarking them in your web browser favorites.

Module 4: Protecting Classified

Learning Outcomes
In this module, we're going to be discussing who's allowed to have access to classified matter, how to control and protect classified in various situations and the requirements associated with DOE's "No Comment" policy. Let's get started.

In this module, we're going to be discussing who's allowed to have access to classified matter as well as how to control and protect classified in various situations. Let's get started.

Access to Classified Matter
Controlling access to classified information is critical to protecting our nation's security. There are many adversaries that have a desire to gain possession of our country's classified information. Every individual with a security clearance shares the important responsibility of ensuring that classified or potentially classified matter is protected. This also includes adhering to Sandia's policy for controlled articles, especially mobile devices when entering a limited area. IT004, Manage Controlled and Electronic Devices and Media Policy, provides more detailed policies for devices and prohibited capabilities.

Classified markings drive how we protect information. They provide a visual indicator that classified is present and help prevent us from leaving it unprotected. The markings also help us identify what security clearance is required to have access.

Before you share classified information with somebody, you must make sure that the individual has the appropriate security clearance and need-to-know. Let's talk briefly about both.

Security Clearances
The security clearance types issued at Sandia are L and Q clearances. While DOE can issue Top Secret, Secret, and Confidential security clearances like other federal agencies, the Q- and L-level access authorizations are specifically required for Restricted Data.

This matrix shows the different combinations of levels and categories, and what clearance is required to access each. Your manager determines what clearance you need by identifying what type of classified your job may handle when he or she submits the request for your clearance.

An individual's clearance can be identified from their badge. Cleared members of the workforce will have either an HSPD-12 Federal Credential or local Sandia badge that indicates an L or Q clearance. Only DOE issued HSPD-12 Federal Credentials indicating a clearance or local Sandia badge may be used at Sandia.

If the individual works for a different federal government entity, they may have a different clearance such as Secret or Top Secret. When those individuals are physically on a Sandia site for a classified project, an incoming classified visit request must be processed. This validates that they have the

appropriate active clearance for their visit. Those individuals will have visitor badges that display the highest classification level and category they are permitted to access. Understanding the different clearances and access authorizations can be challenging. You may find it helpful to print this matrix and post in your office as a quick reference.

Interim Security Clearances and Temporary Security Clearance Upgrades
Obtaining a Q or L clearance can be a lengthy process. In an effort to minimize mission impacts due to pending background investigations, the Department of Energy allows Sandia to utilize two clearance-related options. These options are an Interim Security Clearance and a Temporary Security Clearance Upgrade. Each option is available only in unique circumstances where individuals would not otherwise be able to meet their mission deliverables.

Individuals with either are required to self-identify prior to engaging in classified activities. Both have strict access limitations and neither have visually identifiable indications on the badge, so precautions must be taken when working with these individuals. Click here for details on those restrictions.

Need-to-Know --RENEE
An appropriate security clearance is not all you need; you must also have a need-to-know to access information to perform official business. Before giving somebody access to classified, you are responsible for ensuring their need-to-know is valid. Need-to-know can be granted by the item's point of contact which could be the creator, the project lead, the manager, or it could be you. An example of controlling need-to-know in the computing environment, would be to utilize access controls, such as metagroups, so that only specific individuals can access the information.

Special Access Authorization
As we discussed in module 1, there may be instances where you encounter a caveat marking that identifies an access restriction, such as NOFORN, or additional special authorizations before access can be granted.

Some of these special access authorizations are tied to a specific program. One common example at Sandia is sigma information. The different Sandia Use Control Offices own requirements associated with accessing sigma information. Check the applicable Use Control Office website on the SRN for details on their policies and requirements.

Another example of a special access authorization is Sensitive Compartmented Information or SCI. Access to this information requires fulfilling additional requirements before you can access SCI. If you work with SCI and have questions, speak with your Program Security Officer. They will be able to explain in more detail the additional access-related restrictions for that information.
For other special program requirements, talk to your manager.

Controlling Classified
Federal policy requires that classified be strictly controlled and protected from unauthorized physical, visual, auditory, cyber, or other access. When conducting classified work, you are responsible for making sure that only those with appropriate clearance, need-to-know, and any other applicable special access authorizations have access. You are responsible for making sure that appropriate measures are taken so that classified is protected at all times.

The physical location where classified is stored and processed is an important first line of defense in protecting classified. Classified work must occur within a limited area or higher security area. This helps ensure that unauthorized access can be prevented. Basic precautions such as closing window blinds, closing doors, posting signs, and adding barriers can be taken to further prevent inadvertent access. Signage and barriers help notify others within the limited area not to enter unannounced. They are also helpful reminders so that you don't mistakenly leave classified out and unsecured. If you MUST conduct classified work outside of a Limited Area, you must have an approved security plan designating the proposed area as a Temporary Limited Area or TLA prior to starting the work. Contact Physical Security for more information.

Within a limited area, some areas have been designated as Secure Space that have additional requirements related to mobile devices. For more information on these areas, see the webpage for Mobile Devices and Portable Electronic Devices at Sandia.

Controlling auditory access can be challenging. This requires being mindful of the volume of spoken and projected classified discussions. This includes simple classified conversations as well as classified video teleconferences, also called VTCs.

Classified discussions may be impromptu or may occur during a scheduled meeting. They may also occur during conversations using approved classified phones or electronically on an approved classified computing system using instant messaging. Regardless of the situation, there are some key requirements to be mindful of prior to engaging in a classified discussion.

To ensure classified discussions are heard only by authorized individuals, they must take place within a Limited Area or higher security area. Discussions must only take place where access can adequately be controlled so that only those with the appropriate clearance and need-to-know can hear. This means classified discussions must not occur in hallways, bathrooms, or other common areas within the limited area where access cannot be controlled. It also means that you must be mindful of how loud you are talking when discussing classified and be aware of the equipment and its capabilities in your location to make sure that nothing prohibited is present before you discuss classified.

Physical Classified Matter

When physical classified matter such as documents, media or classified material are removed from approved storage, an appropriately cleared individual with need-to-know must always maintain control of the items. Such items must remain in that individual's possession at all times and can only be relinquished to an individual with the same access authorization.

When you need to take classified documents out of approved storage, they are required to be protected between a cover and a backing sheet with the appropriate classification markings. Your CAS can help you locate these sheets.

We have already discussed classified computing and making sure any classified or potentially classified work is conducted on approved classified systems. When working on these systems, you must ensure visual access to the screen or computer monitor is restricted. You must follow specific rules for classified computing systems, such as making sure the computer is never left unattended when it is not locked.

Preparing to Work with Classified

Before beginning work on classified, you must ask yourself some basic questions to make sure that you don't put yourself in a situation where you are unable to protect the classified matter.

1. First, do you have access to storage? Before you begin to work on classified, always make sure you will have access to approved storage once you complete your work. Classified is not permitted to be taken offsite to your personal residence or any other location not associated with official business.

   Talk to your CAS before doing classified work to ensure that approved storage is available when you conclude your work. If a situation occurs where you have classified in your possession and have no way to store it, at Sandia NM or Sandia CA, you can contact the Protective Force to obtain assistance with temporary storage. At SNL remote sites, contact your site Facility Security Officer.

2. Next, where will you perform your work? Be sure you are physically located in an approved area prior to beginning work. If your work involves potential for classified, avoid conducting work offsite or in an unapproved location. People who work in classified subject areas but try to keep things at an unclassified level are at a high risk of a security incident.

3. And lastly, will your work involve a classified meeting? If you are going to host a classified meeting, whether it's scheduled or an impromptu discussion, there are important verifications that must occur before starting. This includes ensuring the location is within an approved area, making sure prohibited articles or equipment are not present, and confirming participants have the appropriate clearance, need-to-know and any other access-related authorizations for the classified discussion.

Emergency Situations

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

Once you have evacuated and it is safe to do so, locate security response personnel and discretely inform them you either have classified in your possession or that you left classified out and unattended.

When the building is safe for re-entry, you will be allowed to re-enter before the other building occupants to either secure the classified in your possession or return to the area where you left classified out. This will ensure you either store what you have on you or, if you left something out, you will be able to inspect the area to make sure that what was left out is still accounted for.

Report Incidents of Security Concern

As a clearance holder, reporting incidents of security concern is one of your most important responsibilities. You must immediately report any of the following to the Security Incident Management Program (SIMP) at 505-845-1321:

- Suspected or identified unauthorized disclosure of classified matter
- Potential or actual compromise of classified matter
- Improperly protected classified matter OR

- Loss of classified matter

It's important that you immediately report any of these occurrences. This will ensure immediate actions can be taken to mitigate the situation.

Do not provide details of the incident on the telephone, email or voicemail as you do not want to inadvertently reveal classified information on an unauthorized telephone line or unclassified computer. You must take careful action to avoid further compromise and cooperate with the SIMP Inquiry Official investigating the security incident.

If you encounter classified information in the public domain, be sure to adhere to Lab Policy SS002, Identifying Classified Information. You may also consider talking with your manager about taking the online training CLA138-LB, "No Comment Policy" Subject Matter Briefing.

On-the-Job Training
Now that you have a better understanding of what is involved in protecting classified, help Justin decide how to best protect his handwritten notebook when he needs to leave his desk.

Module 5 - Storage of Classified

Learning Outcomes
In this module we're going to be taking a look at the requirements and procedures that you must follow when storing classified as well as the processes for protecting classified combinations that allow you to open locked classified storage. Let's get started.

Authorized Ways to Store Classified
Did you know there are only a few authorized ways to store classified? By having a security clearance, there is a potential you may create or be given documents or materials that are classified. It's important that you understand the basic requirements that come with storing classified matter. This module will include helpful resources to ensure you have the tools you need to secure classified matter appropriately.

So, first things first, when physical classified matter is not in the possession of an authorized individual, it must be stored in an approved location. If the classified is an electronic file, it must reside and be stored on approved classified computing systems or equipment. If computer or equipment have data storage capabilities, they must also be stored in an approved location when not in use.

GSA-Approved Safes
One approved method for storing classified is a GSA-approved safe. A GSA-approved safe is a heavy steel cabinet that contains one to five drawers, and at least one combination spin-dial lock. To be GSA-approved, these safes meet strict federal specifications for protection of classified matter. GSA-safes are effective in storing documents, media, and smaller parts, pieces and equipment. At Sandia, these safes must be located in a limited area or higher security area. These are not to be modified as physical alterations will likely void the GSA approval.

VTRs and Vaults

Another approved method for storing classified is a vault-type room, also known as a VTR. This is an area used for storing classified matter that due to its size, nature, or operational necessity cannot be stored within a GSA-safe.

VTRs meet very specific physical security federal requirements. A few examples of these requirements include a level one security lock, which in most cases is a combination spin-dial lock on the primary door. VTRs also are required to have alarm systems that are monitored by the Pro Force at Sandia New Mexico and Sandia California, and by approved authorities at Sandia remote locations. The size of a VTR can vary from a small room to a large laboratory, a hangar or even an entire building. All VTRs have a point of contact called a VTR Custodian, who can help if you have questions about a specific VTR.

Actual vaults also exist at Sandia. Just like VTRs, these windowless enclosures have specific physical security requirements that include alarms and specific locks at the primary entry points. Since vaults are rare at Sandia, we'll continue in this module speaking specifically to VTRs and GSA-approved safes.

With appropriate approvals, VTRs can be used for "open storage." This means classified matter can be left out inside the VTR. This is helpful for mission needs that involve prolonged tests, and/or storage of classified items that are larger in size. If an individual who does not have appropriate clearance or need-to-know for the classified matter is present inside the VTR, the classified items must be secured ahead of time, so the escorted visitor does not have visual or physical access.

VTRs may have additional security and access requirements including logging and other specific local processes. The VTR Custodian can help you with those processes.

Safes and VTRs must be kept secured when not under direct supervision of an authorized individual. If you ever find a safe or VTR that is unsecured and not under the control of an authorized individual, you must immediately secure it and call SIMP.

Access to VTRs and GSA-Safes

Most VTRs and all GSA-safes will have a combination spin-dial lock. Individuals who know the combination must have the appropriate clearance and need-to-know for the contents inside. All individuals with knowledge of the combination are required to be documented. These individuals must be listed on a federal form called SF 700, Security Container. The people listed on this form are also the emergency contacts who would be contacted if the safe or VTR were ever found unsecured.

If additional space is needed to record individuals with knowledge of the combination, they must be recorded on the Sandia corporate form called the SF 2900-ADD, *Addendum to the SF 700 Form*. Access to VTRs is managed using an application called WebCAT. WebCAT has the capability to provide a printed list that captures the names of the individuals with knowledge of the combination and can be used in place of the addendum form. These forms documenting all individuals with knowledge of the combination must be printed and posted on the inside of the door for VTRs, or inside the drawer of the safe with the lock.

If you are given access to a safe or VTR, you must know the highest classification it is approved to store. This will determine what clearance is required to have access. Classification may also determine Pro Force patrol frequency and response times.

If you ever have classified or potentially classified matter in your possession and do not have access to a VTR or a GSA-safe, contact your manager or your CAS to find an approved location. At Sandia NM or Sandia CA, you can also contact Pro Force who can assist with short-term storage. Please always remember that classified must never be stored in unapproved locations. This includes your home, your office, and your car. Storing classified in an unapproved location must be immediately reported to SIMP.

Combinations

Each spin-dial lock to a VTR or safe must have a unique combination. The combination itself is considered classified and must be protected at the highest classification it protects. Since the combination is considered classified, you must never write it down on anything that cannot be protected as classified. When sharing the combination with an authorized individual, you must do so in an area approved for classified discussions. Sharing the combination over unclassified email, or on an unclassified phone line is strictly prohibited.

Access to safes and VTRs must be carefully managed. If an individual no longer needs access, the combination must be changed. For example, the combination would need to be changed when a person is terminated, retires, no longer has a need-to-know for the contents, or no longer has the appropriate clearance for the contents inside. Contact your CAS or VTR Custodian if you need assistance with changing a combination to a VTR or safe.

All individuals who work with classified, including those with access to safes and/or VTRs, are responsible for ensuring that all CMPC policies are followed. This includes making sure that all classified placed inside the VTR or safe is appropriately marked, that the holdings are kept to only the minimum needed for operations, and that the safe or VTR is appropriately secured.

Unsecure/Open Safes and VTRs

If you are working on a classified project, and do not have access to a safe or VTR, be sure you arrange for approved storage to be available when you complete your work. Again, it is important to remember that you must never store classified in an unapproved location such as your office, car, or personal residence.

If you do have access to a safe or VTR, the process to open each may vary as there are different types of locks. Contact your CAS or VTR Custodian to discuss the process to unlock your safe or VTR.

Securing and Checking the Safe or VTR

When not in use and unattended, safes and VTRs must be secured and locked. To lock a safe, simply ensure all drawers are securely closed and turn the spin dial lock a minimum of four revolutions counterclockwise and then four revolutions clockwise to extend the safe's locking bolt. Be sure to try to open the drawers after locking them to make sure the lock was engaged.

Methods used to lock VTRs are dependent on the configuration of your VTR. Information on how to lock a VTR can be found in Sandia's VTR lab policy SS004. If you work in a VTR, you can take additional training found in TEDS called, SEC180, VTR Training, which will provide you with more details about the requirements associated with VTRs. Your VTR Custodian can also assist with local processes.

Each time a VTR or safe is unlocked and locked, the individual doing so must record the action on the SF 702, *Security Container Check Sheet* by providing the time, date, and their initials on the form. This form must be affixed outside the safe drawer or door with the lock or in a conspicuous location nearby.

At the conclusion of operations, which can be at any point during the day, the VTR and safe must be checked to ensure it was secured appropriately. The individual who performs this check must initial on the appropriate line in the "checked by" column on the form. Sandia previously had a policy that required the individual performing the check be different than the individual who locked the safe or VTR. This is no longer the case. Some areas may implement more stringent checking policies locally. Talk to your CAS or VTR Custodian for your local processes.

What can be stored in safes and VTRs?
All classified matter stored within a safe or VTR must be appropriately marked. You can learn more details about classified marking by taking SEC303, Classified Marking Training, an online class that can be found in TEDS.

Unclassified matter can also be stored inside a VTR or safe. However, it must be marked to distinguish it from classified information when such a distinction is required or otherwise serves a purpose, such as commingled storage. If unclassified and classified project matter is stored together for convenience, there may be confusion as to what is classified and what is unclassified if not clearly marked. Federal policy does require that all media stored in a VTR or safe, classified or unclassified, be marked appropriately. Items susceptible to theft such as money, precious metals, and medical items must NOT be stored with classified.

Remember
At this point you may feel like you're drinking from a fire hose when thinking about storing classified. So let's summarize the key points:

1. When not in an authorized individual's control, physical classified must be stored in a GSA-safe or VTR. If you don't have access to either, contact your CAS or VTR Custodian. If it's during non-operational hours, at Sandia New Mexico or California, call your Pro Force. If you are at a Sandia remote site, contact your Facility Security Officer.

2. GSA-safes and VTRs must always remain appropriately secured when not in direct control of an authorized individual. If you ever find a safe or VTR that is unsecured and not under the control of an authorized individual, you must immediately secure it and call SIMP.

3. If you store classified, as a cleared individual you must ensure all CMPC requirements are met. These include ensuring your matter is appropriately marked in a safe or VTR approved for that classification.

4. If you have access to a safe or VTR, the combination providing access must be treated as classified. Documentation must be present providing a listing of everybody with knowledge of the combination.

5. There are cases where the locks may differ on VTRs and GSA-safes. Talk to your VTR Custodian or CAS for assistance on how to unlock, lock and perform checks on VTRs and safes in your area.

6. Electronic classified matter (such as data, digital files, etc.) can only be stored on a computing system authorized for classified.

On-the-Job Training
Now that you have a better understanding of the requirements for storing classified, help Justin determine the best option for storage based on his situation.

Resources
For more detailed information, check out these resources.

Module 6 - Moving Classified

Learning Outcomes
In this module, we'll be discussing how to securely move classified matter including details on internal and external movement of classified as well as requirements for packaging classified and how to securely receive classified that is sent to you. Let's get started.

Movement of Classified Matter
Movement of classified matter from one location to another involves risk. There are very specific requirements that must be followed when moving classified to help ensure it is always protected. To be sure that you are always following the requirements, work with your CAS when planning for and moving classified. If you work in the Field Intelligence Element, which is also called the FIE or in a Special Access Program, often referred to as SAP, work closely with your Program Security Officer.

Internal Movement
Let's start with internal movement of classified. Internal movement is when classified is moved from one location to another within the same Sandia site. To ensure classified is always protected, work with your CAS to make sure that the following considerations are addressed:

1. **First, verify that the location is authorized to receive the classified matter:** Your CAS can help confirm that the destination is authorized to store the classification of the item being moved. As we discussed earlier, storage requirements for classified vary and are dependent on the classification of the item. Some classified material may also be hazardous, so it's important to check with the destination that will receive the material BEFORE moving classified to make sure that the recipient is authorized to securely and safely receive it.

2. **Secondly, ensure there is space available in approved storage:** Your CAS can help coordinate with the recipient to ensure that the destination location has enough approved space to store the incoming classified matter. Classified at Sandia comes in different sizes and shapes and it's important to confirm space is available before initiating movement.

3. **You will also need to identify the appropriate method to move the classified:** When moving classified internally, there are multiple options that are dependent on the size, shape, and complexity of the classified item. Logistics organizations at both Sandia sites in California and New Mexico are available to assist you in moving classified securely. See the Logistics Move-It website for more information. For internal movement from one Sandia location to another location at the same Sandia site, individuals with authorized security clearance access also have the option to move the item themselves.

4. **Finally, you will need to prepare the package and create a receipt:** Your CAS can help make sure that your classified matter is packaged appropriately to ensure it is protected from inadvertent exposure while in transit. They can also help prepare receipts when required to document successful delivery.

External Movement:
Moving classified outside of the Sandia site introduces even more security risk. Due to this higher risk, requirements are more rigorous to ensure that the classified is always protected and delivered to an approved location. As with internal movement, it is highly recommended that you work with your CAS to make sure that all requirements are met.

Prior to moving classified externally, your CAS can help ensure that you are able to answer the following questions:

1. **Is the external facility approved to receive classified?** Sandia collaborates with various external entities that are approved by the government to process and store classified. These can include federal agencies and government contractor sites, as well as private corporations. Sandia has an internal database called the Classified Matter Channel Directory, or CMC for short, which provides a listing of the external facilities to which Sandia is authorized to send classified. The CMC lists the work agreements or contracts that authorize the specific Sandia organizations to work with the facility as well as the approved classification levels and categories. When moving physical classified items outside the Sandia site, the receiving entity must be listed in the CMC directory and be approved to receive the classification of what is being sent.

2. **Where do I send the classified?** The CMC directory also includes very specific shipping and mailing information as well as special instructions for each location listed. This information has been vetted and approved by the federal government. It's imperative that the information contained in the CMC directory be used to send classified. **Do not** google the address or rely on your customer to tell you where to send classified. **Always** use the information in the CMC directory for the appropriate shipping method being used.

3. **Is a receipt required?** When moving classified that is Secret or higher outside the Sandia site, a receipt is required to document successful delivery. The recipient will confirm that all items listed on the receipt are accounted for. When a recipient returns the signed receipt, it must be retained by the CAS in their CWS records.

4. **How do I package the classified?** Classified sent outside the Sandia site must be double wrapped. This means an envelope inside of another envelope, or a box inside of another box. Both double wrapped layers must be sealed to ensure signs of tampering can be easily detected. This includes all flaps and seams of the envelope or box. The Logistics organizations at Sandia New Mexico and Sandia California can assist with packaging.

5. **How do you plan on sending the classified?** The CMC directory also provides the approved methods of physical transmission that the facility has been authorized to use. Individuals at Sandia New Mexico and Sandia California must use Sandia's Logistics services and must never go directly to the United States Post Office or other commercial overnight express locations to send

classified. The exact procedures may vary slightly at the different Sandia sites, so individuals must always work with their CAS to ensure that only approved processes are used.

6. **Have you notified the recipient?** Making sure that the recipient knows that classified is being sent will help ensure that they are prepared to receive and store the classified as well as return receipts confirming successful delivery.

Remember, the CMC directory must always be used when sending classified to an external site. Work with your CAS if you need help finding a facility, adding a facility, adding a contract, or have any additional questions.

Handcarrying Classified

When moving classified externally away from your Sandia site, the handcarry method should only be used as a last resort. Handcarry is when an individual personally takes the classified from their local Sandia site to an approved offsite location.

At Sandia New Mexico, this could be movement to a customer who resides on Kirtland Air Force Base in New Mexico. At Sandia California an example would be when there is a need to move classified across the street to Lawrence Livermore National Labs. Handcarries may also include more complex situations that involve an individual having to drive to a faraway location, or possibly use airport travel to deliver an item.

Handcarry must only be used as a last resort because there are many uncontrolled risks associated with this method, risks not only to the classified being moved, but also to the individual performing the handcarry. Uncontrollable factors that increase the risk may include traffic accidents, medical issues and flight cancelations or delays.

Prior to performing a handcarry, the individual must complete the “Annual Handcarry Briefing” (SF-2902-AHB) with their manager. This briefing provides instructions for the handcarrying traveler, including rules for basic protection as well as contingency instructions if an unexpected issue comes up during travel.

When handcarrying classified via commercial airlines, be aware that some classified items cannot be put through TSA’s X-Ray machines. There is a process available for alternate screening, but you must plan ahead. Coordination is required with both the Sandia Field Office and TSA and approvals can take up to two weeks. This process is also required for unclassified items that are visually sensitive. An example would be an unclassified 3-D model of a weapon. Work closely with your CAS to ensure all handcarry requirements are completed prior to travel.

Preferred Methods of Transmitting Classified

There are multiple methods for moving classified both externally and internally. Each have various levels of risk.

The preferred method of moving classified that involves the least amount of risk is the use of an approved classified computing network. As we discussed earlier in the course, classified computing networks may be used to exchange classified in various ways. Some examples include:

1. Sending classified email as an easy way to communicate information between individuals in a secure fashion.

2. Sharing classified collaborative space as an effective way to store and share larger volumes of information digitally in a secure, controlled area on an approved classified computing system.

3. Using classified videoconferencing as an effective way to have secure meetings or discussions involving classified.

Sandia has useful resources to help with all of these. The Classified Computing Continual Service Improvement or 3CSI website provides many creative ways to effectively use approved classified tools to meet your classified mission needs. The videoconferencing website also provides guidance on policies and processes associated with setting up and conducting classified meetings.

Another method to transmit classified is by approved classified phone and fax. These classified phone lines are approved for certain classifications. See the Sandia phones website, specifically sections about "Secure phones" authorized for classified discussions. You can also work with your manager to identify your COMSEC POC who can provide assistance on what phones may be used and how to use them.

How to Receive Classified

Now that you know all about what sending classified involves, let's briefly discuss expectations for when classified is received.

If you are working with an external customer who wishes to send classified to you and asks you for information about your local Sandia site, always use information listed in the CMC directory. The mailing and shipping information, including any special instructions, must always be used to make sure that classified sent to Sandia is always protected.

When classified is received from an external entity at Sandia New Mexico and Sandia California, the Logistics organization will work with your CAS to ensure that the matter can be successfully delivered to your local area and stored appropriately. When you receive classified, pay careful attention to the packaging to make sure that there are no signs of tampering while the item was in transit. If there are signs of tampering, immediately contact SIMP.

When opening your package, verify that all classified items contained are listed on the applicable receipt. While reviewing the items, make sure that they are all marked appropriately. If any issues arise, immediately contact the sender and resolve as soon as possible. If all items are accounted for and marked correctly, the receipt must be signed and returned to the sender confirming successful delivery. Be sure to include your CAS in this process to ensure that a copy of the signed receipt is kept in the CWS's records.

Remember:

It's very important to be as diligent and careful as possible when moving classified either internally or externally. Partnering with your CAS can help ensure that you are complying with all the requirements related to movement.

If you are personally moving classified from one location to another, whether it's within the same Sandia site, or using handcarry outside your Sandia site, it's important to always practice good OPSEC. This means:

- Never call attention to yourself or to the fact that you are moving classified.
- Do not conduct any personal business while in route.
- and always remember, classified or potentially classified information **is not permitted** to be taken home.

On-the-Job Training
Now that you have a better understanding of the requirements related to securely moving classified, help Justin decide how to best share classified outside Sandia with visitors from another lab.

Resources:
For more detailed information, check out these resources.

Module 7 - Destroying Classified

Learning Outcomes
In this module, we're going to be discussing what to do with classified when it is no longer needed. We'll take a look at the options that are available for destroying classified and who can assist you in working with destruction of classified. Let's get started.

What do you do with classified when it is no longer needed?
The total volume of classified assets at Sandia should always be kept to a minimum because the more we have, the more time and money we must spend to protect it. We also need to avoid maintaining unnecessary classified matter because a higher quantity of classified documents and materials increases the chances of a possible security incident.

This means that excess copies and obsolete or unneeded classified should be destroyed as soon as it is practical to do so. However, it is also important for you to know which items must be maintained by Sandia for a specific period of time. So, before destroying classified matter, contact the recorded Information Management group or refer to the Sandia Records Retention and Disposition Schedule to make sure that your classified doesn't fall into one of the categories that Sandia is required to retain.

There are multiple ways to destroy classified matter. The destruction method will depend on:

- The Classification of the documents or materials
- The amount of classified matter
- And the type of classified matter that you need to destroy

Destroying Non-Accountable Classified
Anyone who is authorized to deal with classified (meaning someone with a clearance and need-to-know)

can destroy non-accountable classified matter, provided that they know the correct procedure for doing so and follow approved processes.

Destroying Accountable Classified
Accountable classified has additional requirements for destruction. So, work closely with your CAS when destroying accountable to ensure that all the appropriate processes are followed.

Destroying Smaller Quantities of Classified Documents
When you need to destroy smaller quantities of classified documents, you can use an approved Classified Document Shredder. Before shredding your classified, it's important that you follow this simple process:

1. First, make sure the document is not accountable by checking to see if it has a barcode sticker. If it does have a barcode sticker, stop and work with your CAS to the destroy the document appropriately and ensure that the inventory database for accountable classified is updated accordingly.

2. Once you have determined that the document to be shredded is non-accountable, then you will need to check the shredder for a sticker that says: "Equipment Approved for Destruction of Classified". The National Security Agency has specific requirements for how large the residue from the shredder must be. This sticker confirms that the shredder's residue meets that requirement, which is 1mm x 5 mm.

3. When you've confirmed that the shredder has been approved by CMPC and that the document does NOT have a bar code sticker, shred your documents and inspect the residue. To inspect the residue, you must sift through the container of shredded paper to make sure that 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 very important to ensure that the residue meets federal size requirements each time an approved classified shredder is used. The shredder residue must always be inspected after shredding, even when unclassified documents are shredded in a classified shredder. Shredders can malfunction and failure to follow these steps could result in a possible security incident. Any residue that is larger than 1 mm by 5 mm is still considered classified and cannot be left unattended.

When you need to destroy a large volume of classified documents, work with your CAS to submit a request to have your items picked up. At Sandia New Mexico, these classified items are kept in red destruction bags, which must be stored in an approved repository until they are picked up.

Destroying Optical Media
Classified optical media, such as CDs, DVDs and Blu-ray, require specialized optical shredders to meet destruction requirements. Federal policy has recently changed for destruction of DVDs and Blu-Ray. Residue requirements for these items is smaller than requirements for CDs. Authorized equipment will have an approval sticker identifying which types of optical media can be destroyed. When shredding optical media, follow the instructions included on the "Classified Optical Shredding Requirements" posters which are displayed near approved optical shredders. If you wish to use a corporate resource,

like the red bag pick-up at Sandia New Mexico, you must identify which type of discs you need to have destroyed.

Destroying Classified Cyber Media

Classified Cyber Media, such as hard drives, laptops, VHS tapes, operational technology, etc. may only be destroyed using equipment and processes that are approved by the CMPC program. You will need to work with your CAS to identify options to dispose of any classified cyber media.

Destroying Classified Material

Classified material refers to assets that do NOT have data storage capabilities. Examples are parts, pieces, components, 3-D models, etc. Material may be classified due to its size, shape or materials used. Classified Material may be disassembled into separate parts that are not classified or altered by shredding, pulverizing, incinerating, etc. so that it no longer reveals classified and classified can no longer be retrieved. When you need to destroy classified materials, you need to consult an authorized DC because he or she must use classification guidance to determine if the material in its new, disassembled or altered state is indeed unclassified. If a DC is unable to do so, work with your CAS to utilize disposition methods that are approved by CMPC.

Permanent Burial

One of the approved methods to get rid of most classified material and media is permanent burial. There are some items that are not permitted to be sent for permanent burial due to their classification and/or program requirements, so be sure to work closely with your CAS so that these items can be sent to the appropriate Classified Work Station where they will be shipped to a federally approved permanent burial site.

On-the-Job Training

Now that you have a better understanding of the requirements related to properly destroying classified, help Justin determine the correct process to follow for shredding classified documents.

Resources

See the Classified Workstation Manual for information on options for destruction of various types of classified matter. And, as always, you can consult your CAS with questions you may have.