



HELP



# SEC100: Annual Security Refresher Briefing

BEGIN

SAND2024-030370



# Introduction

Hello everyone,

I'm David Cain, your Corporate Classification Officer. I wanted to say a word as you prepare to complete your annual SEC100 training. I have worked at Sandia for 33 years, with the last 15 of those years in the Classification Office.


I admit, during my early years working in and with Nuclear Weapon systems and Components, I did not have a strong affinity for, or understanding of, Classification and Security. My way of dealing with Classified information was to avoid it at all costs. Honestly, I was afraid of it.

Now, of course, I see things differently. I realize that ensuring the security of our Nation's most valuable information assets is one of Sandia's highest priorities and must be one of mine, too. Francis Bacon said, "knowledge is power", and we all know that the key to knowledge is information. Just think, you and I are the keepers of the keys! It's our responsibility to ensure that our government's classified and sensitive information and materials are only accessible to those with the proper clearance and need-to-know. We have been given the awesome responsibility to prevent any who would seek to harm our Nation, from acquiring the information and materials necessary to do so. Many believe that this responsibility only belongs to the Classification Office and other Sandia Security Organizations. This is far from the truth. Effective security requires all Sandians, especially you! You are on the front lines in the battle to keep our Secrets, secret, our materials and facilities secure, and our country safe.

To do this, we have to know the policies and regulations that have been created with this purpose in mind. We must know how to identify classified information, so we can protect it properly. We must know the rules for securing and protecting vaults and Limited Areas. We must know what devices we can bring into secure areas and what we cannot. We need to know who to call when we think classified information has been put in unsecured venues.

Whether you're a Sandia veteran like myself who has taken SEC100 over 30 times, or you are new to Sandia and are taking it for the first time, let me encourage you to stop, take a breath, and concentrate on what the training is trying to teach you. Now, I say to you what Gandalf the Grey said to young Frodo Baggin's who held the Ring of Power - **"Keep it Secret. Keep it Safe."**

-David Cain



### Course Objective:

The annual security refresher briefing is required by DOE O 470.4B for all cleared members of the workforce (MOWs).

In this briefing, you will:

- Learn about Sandia-specific security incidents and how to prevent recurrence.
- Review your security responsibilities and best practices.
- Receive Counterintelligence and Security updates.

## INCIDENTS OF SECURITY CONCERN (IoSC) AT SANDIA

**Category A:** may involve the loss, theft, suspected compromise, or compromise of departmental assets.

**Category B:** may involve failure to adhere to security procedures where the likelihood of compromise is *remote* or *not suspected*.

DID YOU KNOW

Discussing the details of a classified security incident outside of a limited area, or via unsecured means, could result in *a subsequent security incident*.

## COURSE MODULES

REVISITING REAPPLICATION

CODEWORD "IRONMAN"

THINK BEFORE YOU CLICK

THE "WHERE" OF CLASSIFIED

COUNTERINTELLIGENCE UPDATE

SAFEGUARDS & SECURITY UPDATE

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING



Sandia sends approximately 8000 computing systems to Reapplication (Reapp) each year. Though discussed in past trainings, hard drives with classified data continue to be turned in to Reapp.

Notma Data just received her clearance and moved into her new office, which happens to be inside of a Vault-Type Room (VTR). The classified computer (CPU) that was left at her desk was at the end of its service life.

Believing she had adequately “wiped” the old CPU of all data, she submitted a Movelt ticket to have the it taken to Reapplication. A week later, Reapp contacted her manager to inform them that the CPU still contained classified data and was not disposed of properly. What should Notma have done instead?

Notma should have removed all classified markings from the CPU before sending it to Reapp.

Before sending the CPU to Reapp, Notma should have removed all memory from the CPU, reached out to CCHD to confirm that all memory that could have contained classified was removed, and consulted her CAS to ensure that it was disposed of properly.

Notma Data just received her clearance and moved into her new office, which happens to be inside of a Vault-Type Room (VTR). The classified computer (CPU) that was left at her desk was at the end of its service life.

Believing she had adequately “wiped” the old CPU of all data, she submitted a Movelt ticket to have the it taken to Reapplication. A week later, Reapp contacted her manager to inform them that the CPU still contained classified data and was not disposed of properly. What should Notma have done instead?

Congratulations, you chose wisely. Notma should have removed all memory from the computer, reached out to CCHD to confirm removal of memory, and consulted her CAS to ensure it was disposed of properly.



Several days passed. Notma received a phone call from a SIMP investigator. She was questioned about how the computer with its memory still intact made its way to Reapplication. Through the course of the inquiry, it was found that Notma did not follow Sandia policy when managing the destruction of materials potentially containing classified.

This incident was categorized as a Category B Incident of Security Concern (IoSC).

# DID YOU KNOW?

All classified computing systems must be evaluated and cleared of anything with potential to store classified information (e.g., hard drives) before being destroyed, reused, permanently removed from a VTR or safe, and/or sent to Reapplication.

To start the evaluation process, you must call CCHD (505-845-2243, option 1+1).

Only after CCHD personnel have verified that the computing system is cleared of classified can the equipment be managed as unclassified.

Reapplication is not authorized to receive classified matter.

## Think:

Do I need to **permanently** remove computing equipment from a Vault-Type Room (VTR) and/or a General Services Administration (GSA) security container (safe)?



## Assess:

Computing equipment that is in a safe or VTR may be classified matter because it may have processed classified information and/or been connected to a classified system or network.

Am I sure I can remove it from the safe or VTR?



## Protect:

Treat any and all classified processing equipment as classified matter. Do not remove this equipment from a VTR or safe without contacting CCHD for assistance.



## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN"

THINK BEFORE YOU CLICK

THE "WHERE" OF CLASSIFIED

COUNTERINTELLIGENCE UPDATE

SAFEGUARDS & SECURITY UPDATE

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING



Sandia's Security Incident Management Program (SIMP) conducted 1,445 inquiries in 2023. Of those, 258 were determined to be incidents, resulting **25 Category A** and **233 Category B** determinations.

Abe Centminded is responsible for his division's GSA Cabinet. Recently, he received a keypad magnet to help him remember the code for the cabinet. He determined that his code aligned with the word "Marvel". There is a marker board next to his GSA safe. To help him remember his codeword, he wrote "Ironman" on the marker board. Abe's manager saw the word written on the board one day and asked him about it. When he learned the reason behind the note on the board, he realized it was a violation of Sandia policy and security best practices. What should the manager do?

Abe's manager should immediately erase the password hint on the marker board and tell Assent not to do it again.

Abe's manager should take immediate steps to document the incident, make sure the hint is completely erased, change the code, and report the incident to SIMP.

Abe Centminded is responsible for his division's GSA Cabinet. Recently, he received a keypad magnet to help him remember the code for the cabinet. He determined that his code aligned with the word "Marvel". There is a marker board next to his GSA safe. To help him remember his codeword, he wrote "Ironman" on the marker board. Abe's manager saw the word written on the board one day and asked him about it. When he learned the reason behind the note on the board, he realized it was a violation of Sandia policy and security best practices. What should the manager do?

Congratulations, you chose correctly. Abe's manager should take immediate steps to document the incident, make sure the hint is completely erased, change the code, and report the incident to SIMP.

Abe Centminded discovered that his GSA Safe code aligned with the word "Marvel". Near his safe, he wrote the codeword "Ironman" on a whiteboard. Abe's manager saw the word on the board and asked him about it. When he learned of the reason behind the codeword, he realized it was a violation of Sandia Policy and security best practices.

SIMP conducted an investigation into the incident and determined the event was categorized as a Category A IoSC.



## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN" ✓

**THINK BEFORE YOU CLICK**

THE "WHERE" OF CLASSIFIED

COUNTINTELLIGENCE UPDATE

SAFEGUARDS & SECURITY UPDATE

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING



Sandia's information technology infrastructure receives over a million cyber attacks each day. Many come in the form of phishing attacks.

Luke S. Ligit is an Senior Management Assistant (SMA) for a division at Sandia. Recently he was tasked by his manager to replace a number of pieces of office furniture in the division's conference room. The project had supply chain issues from the start, and two weeks ago, Luke learned from the distributor that some of the items he had ordered were lost in transport. Today he received an email from UPS stating he needed to visit a hyperlinked website to provide additional shipping instructions to get the missing furniture delivered. Luke was about to click the link when he hovered over it and noticed the URL did not appear to be for a UPS website. What should Luke do?

Go ahead and click on it. Sandia has cutting edge virus and malware protections in place that will protect his computer from all attacks.

Forward the email to [spam@sandia.gov](mailto:spam@sandia.gov). He should also reach out to the vendor directly (not using the information in the email) to verify the validity of the email.

Luke S. Ligit is an Senior Management Assistant (SMA) for a division at Sandia. Recently he was tasked by his manager to replace a number of pieces of office furniture in the division's conference room. The project had supply chain issues from the start, and two weeks ago, Luke learned from the distributor that some of the items he had ordered were lost in transport. Today he received an email from UPS stating he needed to visit a hyperlinked website to provide additional shipping instructions to get the missing furniture delivered. Luke was about to click the link when he hovered over it and noticed the URL did not appear to be for a UPS website. What should Luke do?

Congratulations, you chose correctly.  
Luke should forward the email to [spam@sandia.gov](mailto:spam@sandia.gov) and contact UPS directly to confirm the legitimacy of the email.

Luke slowed down, considered the suspicious link in the email, and forwarded it to [spam@sandia.gov](mailto:spam@sandia.gov) so that they would be aware of the possible phishing attempt. He then searched the web for an official contact phone and email for UPS, contacted them, and verified that the email was not legitimate. He saved himself and Sandia many hours of trouble by being cautious to the possibility that the email was not really from UPS.

# DID YOU KNOW?

Adversaries are always looking for an opportunity to exploit our trust and good nature in an attempt to gain access to our information technology systems, execute denial of service attacks, and interfere with the vital work that we do here. Everyday, Sandia's automated systems stop millions of phishing and cyber attacks.

A very small percentage of these attacks still get through. It is your responsibility to be wary of unsolicited emails and always ***think before you click!***

## Think:

Have I confirmed that an unsolicited email is from a verified source?

Have I inspected the email address to confirm the displayed name and address are legitimate?



## Assess:

Inspect the body of the email for clues to its validity. Look for grammar, spelling, and other anomalies. Hover over links to view the URL and try to determine if it looks suspicious. View the sender's email address and compare it to the display name.



## Protect:

If something seems "off" with an email, forward it to [spam@sandia.gov](mailto:spam@sandia.gov) and utilize outside sources to validate the email and its contents. Until you know it's legitimate, don't click on it.



## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN" ✓

THINK BEFORE YOU CLICK ✓

**THE "WHERE" OF CLASSIFIED**

COUNTERINTELLIGENCE UPDATE

SAFEGUARDS & SECURITY UPDATE

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING





Every year, Sandians log millions of miles of travel on official business.

Sheridan Marriott was traveling off site to attend a classified meeting at the DC office. While he was at the meeting, he took notes that he believed should be classified as SRD. In his hurry to get to dinner with his team, Sheridan forgot to have the notes reviewed by a DC and dropped his notebook off in his hotel room. The next day, Sheridan realized that his classified notes were not properly secured or DC'd.

What should Sheridan do?

Sheridan doesn't need to do anything immediately because he is still out of town and he's certain that no one accessed his hotel room while he was out to dinner.

Sheridan should immediately contact Security Connection to notify SIMP that an Incident of Security Concern (IoSC) may have occurred.

Sheridan Marriott was traveling off site to attend a classified meeting at the DC office. While he was at the meeting, he took notes that he believed should be classified as SRD. In his hurry to get to dinner with his team, Sheridan forgot to have the notes reviewed by a DC and dropped his notebook off in his hotel room. The next day, Sheridan realized that his classified notes were not properly secured or DC'd.

What should Sheridan do?

Congratulations, you chose correctly.  
Sheridan should immediately contact Security Connection to notify SIMP that an Incident of Security Concern (IoSC) may have occurred.

Sheridan immediately reported the incident to SIMP via Security Connection at (505) 845-1321. The SIMP investigator took steps immediately to ensure that no further risk to the classified notebook could occur. Sheridan met with a Derivative Classifier from the DC office before going to the airport and was able to get the notebook's contents properly reviewed. They were even willing to scan and email the contents of the notebook on the SCN so that Sheridan didn't have to hand-carry the notebook back to New Mexico.

# DID YOU KNOW?

Although Sandia is in the process of developing off-site locations for the processing of classified matter, it is important to remember that classified should only be discussed, worked with, and stored in approved locations.

Always have a plan when traveling for classified meetings. Make all hand carry, DC, and storage arrangements ahead of time. Make sure your return plans allow you enough time to return any classified to its approved storage location. Engage with your CAS to make sure everything goes smoothly!

## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN" ✓

THINK BEFORE YOU CLICK ✓

THE "WHERE" OF CLASSIFIED ✓

**COUNTERINTELLIGENCE UPDATE**

SAFEGUARDS & SECURITY UPDATE

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING



To succeed in our mission to detect, deter, and mitigate threats to Sandia National Laboratories, the Office of Counterintelligence (CI) relies on the cooperation of the Sandia community that we support.

- [CI-Help@sandia.gov](mailto:CI-Help@sandia.gov)
- CA & NM: 505-284-3878



## Unusual Solicitation

Any attempt by any unauthorized persons to gain access to classified information is a matter of significant Counterintelligence concern and, per DOE/NNSA reporting requirements, should be reported immediately to Counterintelligence.

This applies equally to foreign nationals, as well as unauthorized U.S. citizens. Such attempts can be in the form of pointed and intrusive questions or more subtle elicitation.

This reporting requirement also applies to unusual situations that make you feel that you or a colleague is being targeted.

You must select each of the buttons to continue.



Unusual Solicitation



Foreign Travel



Insider Threat



Substantive  
Contact/Relationship



Social Media





## Foreign Travel

All clearance holders and applicants must report all personal/official foreign travel regardless of the sensitivity of the destination. As a clearance holder, foreign intelligence services may view you as a valid target by which to gain real or potential access to information of value to their governments. All uncleared personnel, to include foreign nationals, must report personal/official travel to sensitive countries only. Remember that while you are in a foreign country, you remain vulnerable to foreign intelligence service tactics.

Intelligence Services may:

- Surveil your movements (audio and video coverage of your hotel room, conference room, and dining facilities)
- Enter your hotel room or other quarters at will
- Compromise your electronic devices (tap your telephone, fax machine, or laptop computer)
- Use interpreters to monitor your conversations and behaviors

You must select each of the buttons to continue.



Unusual Solicitation



Foreign Travel



Insider Threat



Substantive  
Contact/Relationship



Social Media



## Insider Threat

Report to Counterintelligence, any individual who:

- Seeks unauthorized access to classified information, matter or special nuclear material without a Need To Know.
  - Asks about classified projects, materials, etc. without a valid NTK.
  - Attempts to have reasons for access to secure space that are not within the scope of work.
- Appears to be living well beyond their means.
  - Sudden and/or unexplained affluence, or sudden financial hardships.
- Has unreported foreign contacts or travel or you learn of delayed or unreported foreign contacts and/or travel.

Counterintelligence handles sensitive information with discretion to protect the good name and reputation of the person who is the object of your concern while balancing our responsibility to protect Sandia and national security.

Foreign intelligence services seek the cooperation of an authorized insider to defeat security measures.

You must select each of the buttons to continue.



Unusual Solicitation



Foreign Travel



Insider Threat



Substantive  
Contact/Relationship



Social Media



### Substantive Contact/Relationship

All Sandia MOWs, regardless of clearance and/or citizenship status, are required to report substantive contacts with foreign nationals. Substantive contact is a personal or professional relationship that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds (does not include family members).

Substantive contact can be professional, personal, or financial in nature and includes ongoing contact that is solely through electronic communication (e.g., email, telephone, or social media and professional networking sites). For Sandia, substantiative contact is defined as a personal or professional relationship that is enduring and involves substantial sharing of personal, business, or research information; and/or the formation of emotional bonds.

Non-U.S. citizens are considered Foreign Nationals; this includes "green card holders" or "lawful permanent residents."

You must select each of the buttons to continue.



Unusual Solicitation



Foreign Travel



Insider Threat



Substantive Contact/Relationship



Social Media



## Social Media

Remember that with the recent explosion of social media platforms, also comes an increase in the manipulation of them to exploit us for information. A definite uptick of spoofed accounts, fake relationships and the like have been seen. AI also takes this to the next level with its ability to manipulate photos that we place in the open media. Always stay vigilant to these possibilities and take steps to protect yourself from digital adversaries.

You must select each of the buttons to continue.



Unusual Solicitation



Foreign Travel



Insider Threat



Substantive  
Contact/Relationship



Social Media

## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN" ✓

THINK BEFORE YOU CLICK ✓

THE "WHERE" OF CLASSIFIED ✓

COUNTERINTELLIGENCE UPDATE ✓

**SAFEGUARDS & SECURITY UPDATE**

CLASSIFICATION UPDATE

ANNUAL SECURITY REFRESHER BRIEFING



# Safeguards & Security Update

The Safeguards and Security programs continue to seek ways to assist everyone at Sandia with their security responsibilities through policy updates, best practices, and information that can be used to protect members of the workforce (MOWs) at work and at home.

The resource documents below provide additional information for the security updates in this module.

- [Critical Information Lists](#)
- [Reporting Requirements & FAQs](#)
- [Controlled Articles at Sandia](#)



## OPSEC - Critical Information Update

Critical Information is *specific facts about Sandia's intentions, capabilities or activities vitally needed by adversaries to plan and act effectively*. Per SS013, *Critical Information Policy*, programs or centers are required to engage Sandia's OPSEC program to identify critical information specific to their work.

Unclassified government information determined by Sandia's OPSEC program to be critical information is **controlled unclassified information (CUI)** using the Operations Security category and is marked and controlled as CUI//OPSEC.

Practice OPSEC by being familiar with your critical information lists and controlling that information as CUI. All critical information lists can be accessed on the Critical Information List Library page. For more information, contact Sandia's OPSEC program at [opsec@sandia.gov](mailto:opsec@sandia.gov).

You must click each of the buttons to continue.



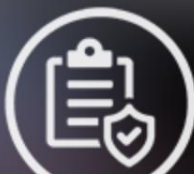
**OPSEC - Critical Information Update**



**Reporting Requirements**



**Controlled Articles & CARP**



## Reporting Requirements Reminder

In October 2022, the [DOE and Sandia Reporting Requirements of Security Interest](#) was updated. Notable changes include a requirement for security clearance holders to report **all foreign travel to any country** for any reason, and a requirement to report **unusual infusions of assets greater than \$10,000** (such as inheritance or winnings. Note that unusual infusions do not include every day occurrences such as sale of property, loans, stocks/tax refunds, etc).

As a Sandia-sponsored security clearance holder, it is important that you maintain an understanding of your reporting requirements, especially as they may have changed from the last time you reviewed them. For more information, see the [Reporting Requirements FAQ](#).

For questions, or to report, contact Security Connection | 505-845-1321 or 321 from any Sandia landline phone | [security@sandia.gov](mailto:security@sandia.gov)

You must click each of the buttons to continue.



OPSEC - Critical Information Update



Reporting Requirements



Controlled Articles & CARP



## Controlled Articles & CARP

A controlled article is any electronic device capable of recording information or transmitting data, including audio, video, radio frequency, infrared, and/or data link electronic equipment. Examples include video and photography cameras, recording equipment, transmitting equipment, and more.

Per SS007, Controlled and Prohibited Articles Policy, you may not use Sandia-managed controlled articles in Limited Areas or Vault-Type Rooms (VTR) without prior authorization using the Controlled Articles Registration Process (CARP).

For more information, visit [carp.sandia.gov](http://carp.sandia.gov) or contact [carp@sandia.gov](mailto:carp@sandia.gov).

You must click each of the buttons to continue.



**OPSEC - Critical Information Update**



**Reporting Requirements**



**Controlled Articles & CARP**

## CUI At a Glance

Controlled Unclassified Information (CUI) is government-owned, unclassified information that requires protections. Members of the Workforce are responsible for identifying and marking CUI that requires protection under a specific set of laws, regulations, or government-wide policies (LRGWP), also known as Authorities. As an authorized holder, YOU make the determination.

Information at Sandia may be Sandia-owned, or U.S. government-owned. CUI is government-owned information that falls under a category on the CUI Registry available at [cui.sandia.gov](http://cui.sandia.gov) on the Sandia Restricted Network. Before you can mark any CUI materials or information, you need to know what categories will apply – it could be one or multiple. Once you have identified applicable categories, the [CUI Marking Assistant](#) can help develop the CUI markings needed for the information. See the [CUI Marking Handbook](#) for examples of how to mark different media and documents.

Protect CUI against unauthorized disclosure. However, you can share CUI with individuals in furtherance of a lawful government purpose, and when the individual is eligible for access. For more information, contact [cui@sandia.gov](mailto:cui@sandia.gov).

## COURSE MODULES

REVISITING REAPPLICATION ✓

CODEWORD "IRONMAN" ✓

THINK BEFORE YOU CLICK ✓

THE "WHERE" OF CLASSIFIED ✓

COUNTERINTELLIGENCE UPDATE ✓

SAFEGUARDS & SECURITY UPDATE ✓

**CLASSIFICATION UPDATE**

ANNUAL SECURITY REFRESHER BRIEFING



# CLASSIFICATION UPDATE

A **Derivative Classifier (DC)** is an individual authorized to confirm that an unmarked document or material is unclassified, or determine that it is classified as allowed by their letter of authority. A DC can also determine that a previously marked document needs to be classified at a higher level and/or category.

A **Derivative Declassifier (DD)** is an individual authorized to declassify or downgrade Sandia-originated documents, equipment or material as allowed by his or her letter of authority. DDs are located in the Classification Office.

You can locate a DC or DD through the Jupiter application ([jupiter.sandia.gov](http://jupiter.sandia.gov)).

For Questions:

NM: [classificationdept@sandia.gov](mailto:classificationdept@sandia.gov)

CA: [CAClassDept@sandia.gov](mailto:CAClassDept@sandia.gov)

**DID YOU  
KNOW?**



**?**

When requesting a DC review, do not transmit on an unclassified network. Start on the Sandia Classified Network (SCN). If a DC determines your material to be unclassified, use the Downshift utility to move it to the Sandia Restricted Network (SRN).

# CLASSIFICATION UPDATE

You must request a DC review for:

- A newly generated document or material in a potentially classified subject area.
- An existing, unmarked document or material you believe may contain classified information.
- An existing, marked document or material you believe may contain information classified at a higher level or more restrictive category.
- A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix) taken from another classified document.
- Upgrading the classification level and/or category of information, documents, or material based on proper guidance.

# CLASSIFICATION UPDATE

Declassification review by a DD must occur when the document or material is:

- Prepared for declassification in full.
- Prepared as redacted versions.
- Requested under statute or Executive Order (i.e., declassification for public release).
- Referred to DOE by other government agencies that are or identified as potentially containing Restricted Data/Formerly Restricted Data/Trans-classified Foreign Nuclear Information.
- Marked for declassification prior to actual declassification to ensure that National Security Information (NSI) document or material does not contain classified information.
- An NSI document or material marked for declassification.

**DID YOU  
KNOW?**



**?**

You can locate a DD or a DC via Jupiter on the Sandia Restricted Network (SRN) at [jupiter.sandia.gov](http://jupiter.sandia.gov).

# CLASSIFICATION UPDATE

If you believe a DC determination is incorrect, you have the responsibility to challenge the determination.

For assistance with challenges, contact the Classification Office:

- In New Mexico: (505) 844-5574 / [classificationdept@sandia.gov](mailto:classificationdept@sandia.gov)
- In California: [CAClassDept@sandia.gov](mailto:CAClassDept@sandia.gov)

You are encouraged to resolve challenges locally in discussions with your DC and the Classification Officer. If it cannot be resolved you have the right, at any time, to submit a formal written challenge to the DOE Office of Classification Director. Request additional information from [outreach@hq.doe.gov](mailto:outreach@hq.doe.gov). Under no circumstances will you be subject to retribution for making such a challenge. See [Laboratory Policy SS002, Identifying Classified Information, Section 4](#) for Challenge procedures.

**DID YOU  
KNOW?**



?

You can locate a DD or a DC via Jupiter on the Sandia Restricted Network (SRN) at [jupiter.sandia.gov](http://jupiter.sandia.gov).

# CLASSIFICATION UPDATE

## The GEN-16 REVISION 2: "NO COMMENT" POLICY

The GEN-16 policy applies to classified information in the open literature. You can't prevent classified information that is outside of your control from appearing in the public but cleared individuals must not comment on it.

A comment is any activity (not just verbal) that would allow a person who is not authorized access to classified information to locate the information or confirm the classified nature or technical accuracy of the information.

Even if you didn't know the information is classified, you are responsible for not drawing attention to it. Never assume that information in classified subject areas found in public venues is unclassified.



On behalf of Safeguards and Security, keep up  
the good work PROTECTING WHAT IS OURS!

Thank you!

Just a few more steps to make sure you get  
credit for taking this briefing.  
Select the next button to continue.

## SEC100 Completion Record: 2023/2024

By completing this form, you acknowledge that you have read the Sandia National Laboratories 2023/2024 Annual Security Refresher Briefing and understand your security responsibilities.

Complete the information below and email to [securityed@sandia.gov](mailto:securityed@sandia.gov) to receive credit in the Sandia Learning Management System.

Full Name (print):	
SNL Org # or Company Name:	
Signature:	Date:
Email Address:	

**For security questions or to report:**

321 from a Sandia landline | 505-845-1321 from any phone  
[security@sandia.gov](mailto:security@sandia.gov)