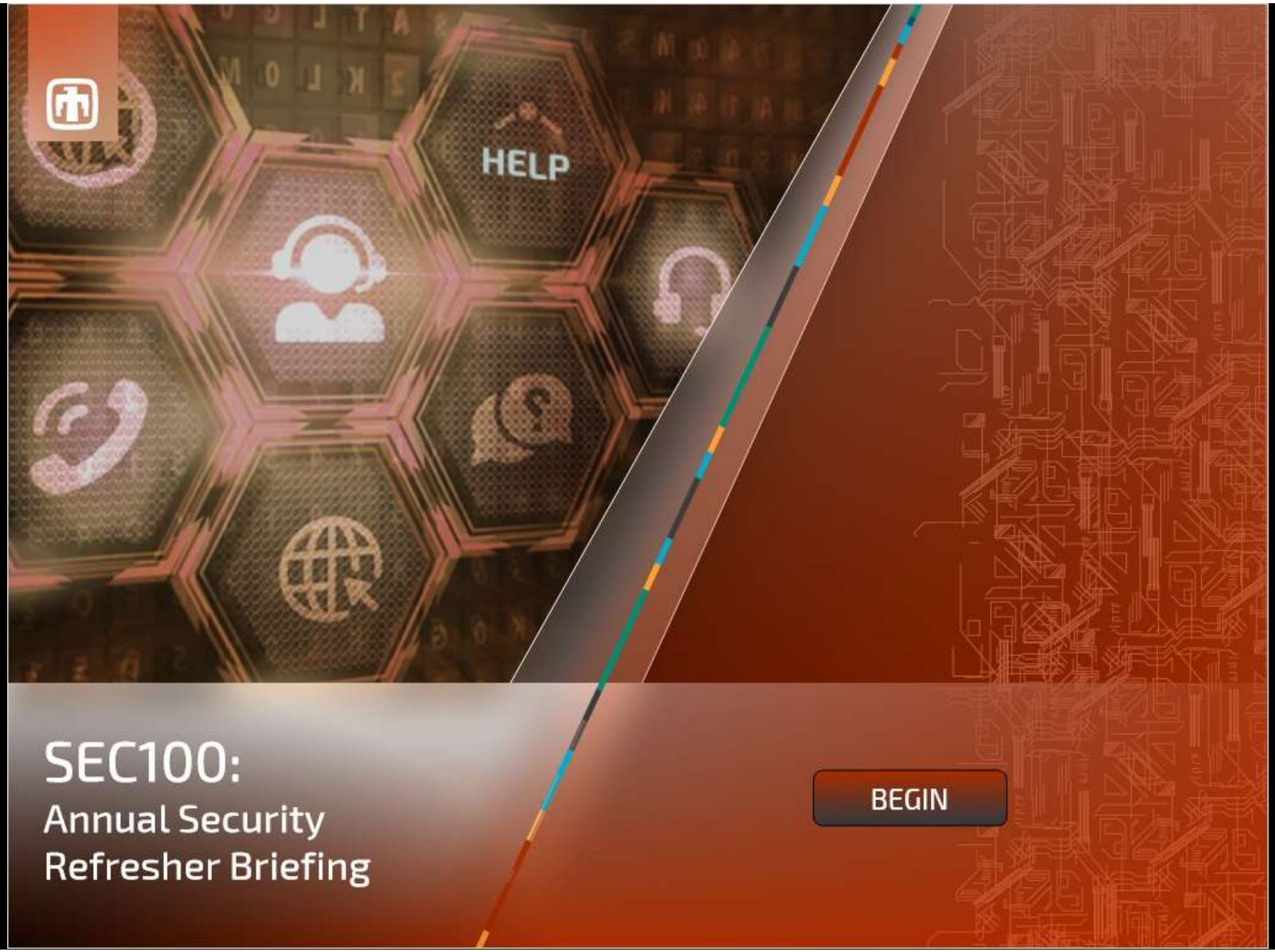
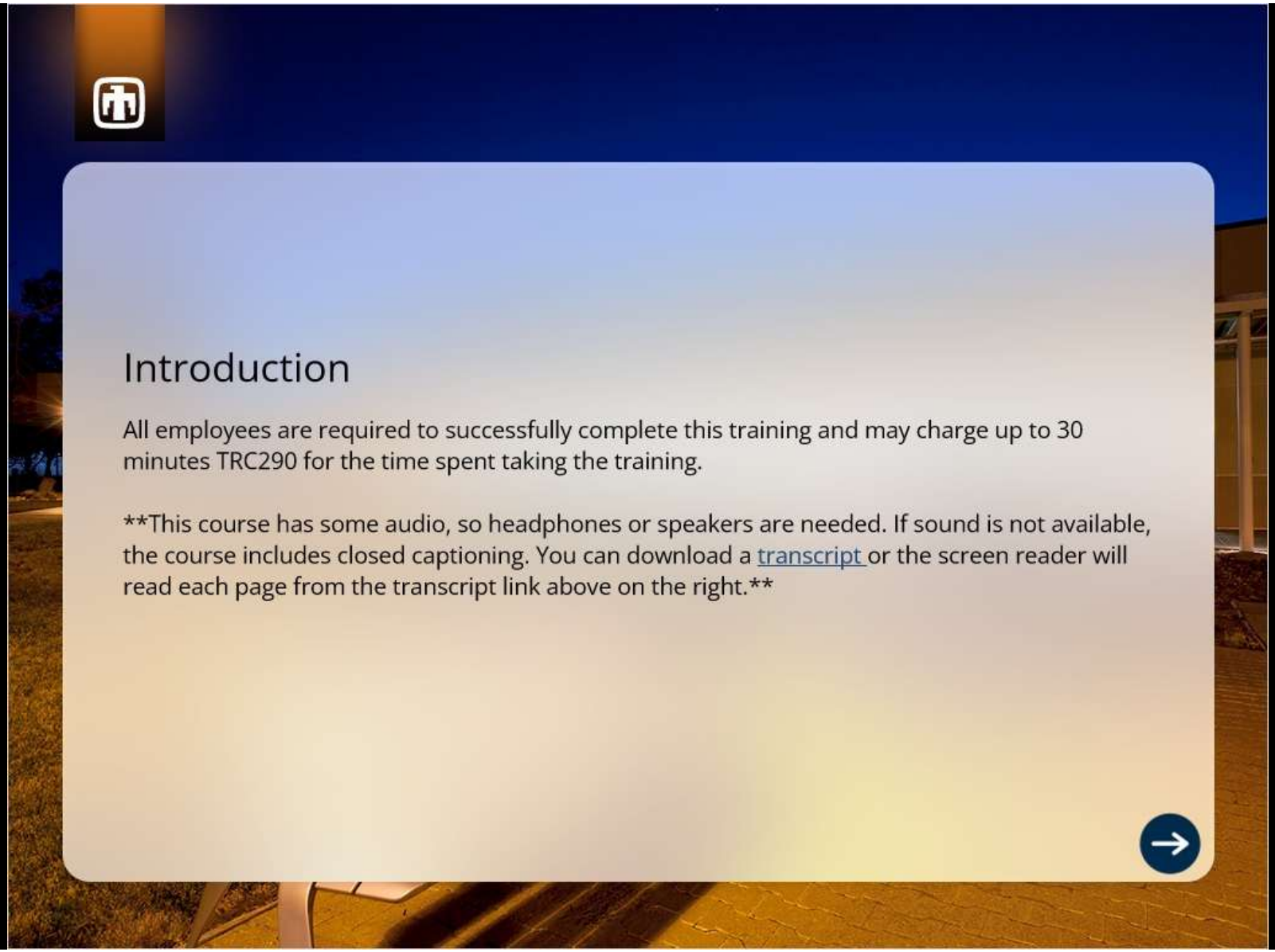

HELP
SEC100:
Annual Security
Refresher Briefing
BEGIN


Introduction
All employees are required to successfully complete this training and may charge up to 30 minutes TRC290 for the time spent taking the training.
This course has some audio, so headphones or speakers are needed. If sound is not available, the course includes closed captioning. You can download a transcript or the screen reader will read each page from the transcript link above on the right.

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.

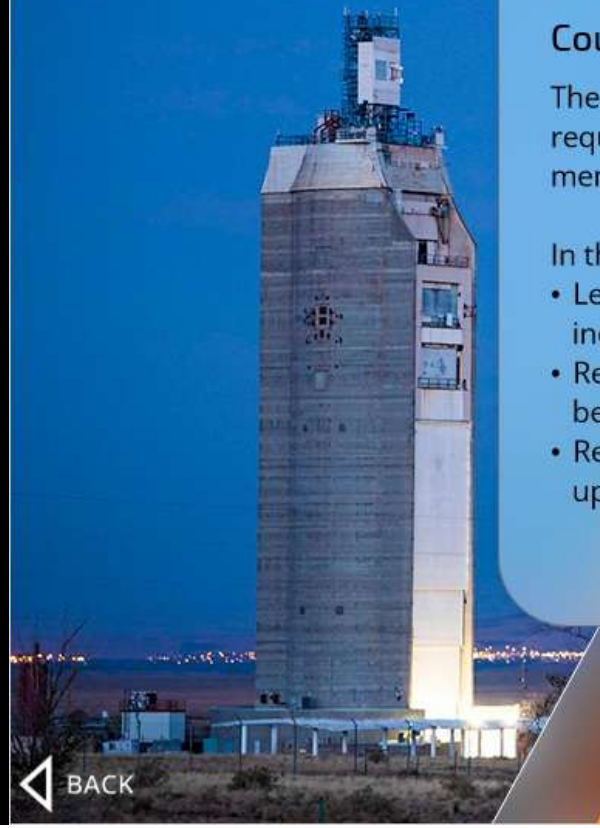
I admit, during my early years working in and with Nuclear Weapon systems and Components, I did not have a strong affinity for, or understanding of, Classification and Security. My way of dealing with Classified information was to avoid it at all costs. Honestly, I was afraid of it.

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 470.4C 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.

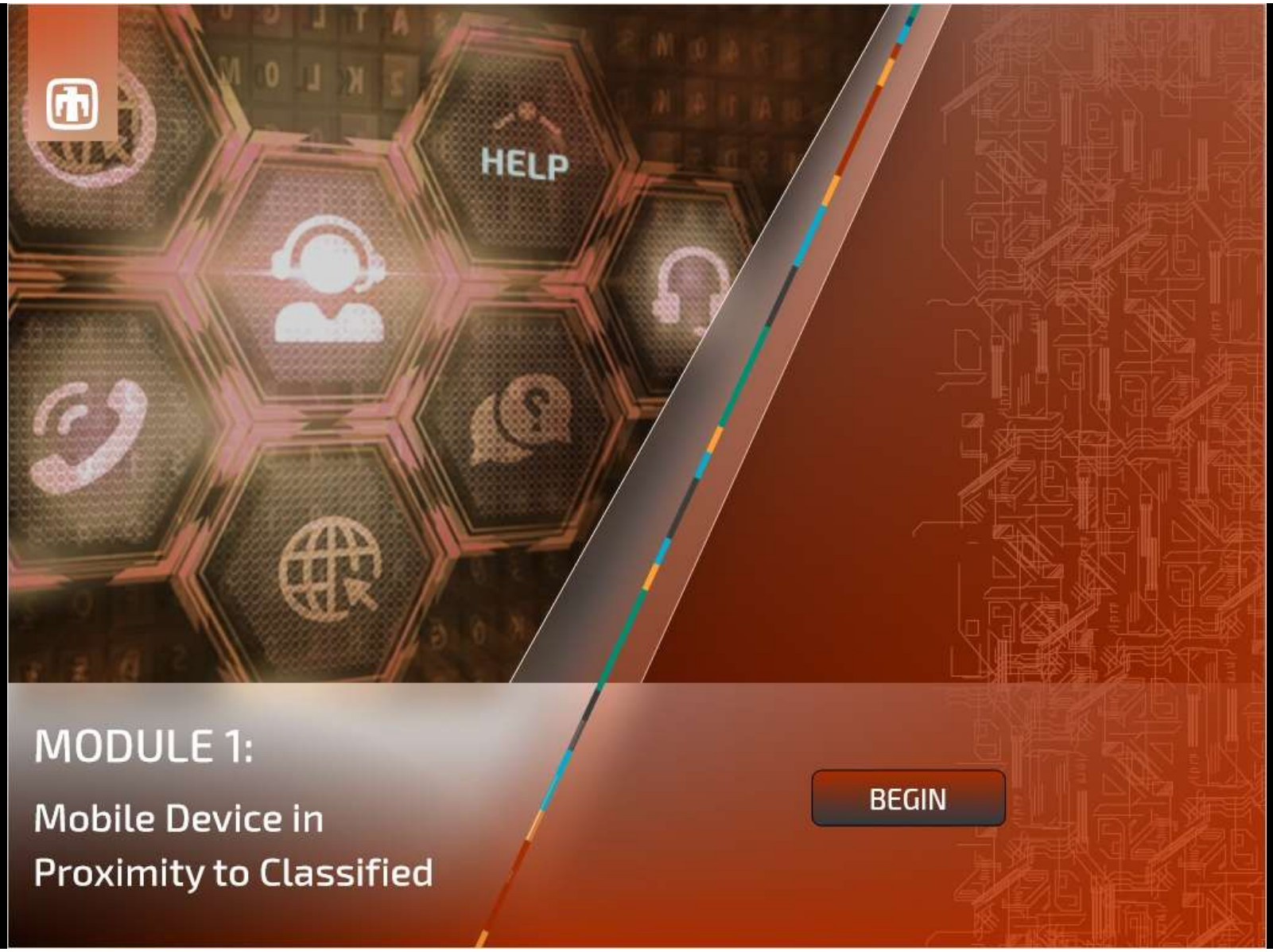
INCIDENTS OF SECURITY CONCERN (IoSC) AT SANDIA

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.*


HELP
MODULE 1:
Mobile Device in
Proximity to Classified
BEGIN

Can my cell phone be used as a listening device?

Yes, your phone can listen to you through authorized apps that use the microphone or through malicious spyware. Legitimate apps may request microphone access for functions like voice commands or recordings, while unauthorized spyware can secretly access the microphone without visible signs.

Technically, most phones can listen, but the specifics of how and why they do, as well as the use of collected information, are often unclear. Due to vulnerabilities associated with mobile devices, their use is prohibited in Secure Spaces as mandated by federal requirements.

Statistics FY25:

- Controlled Articles: 1 Cat-A, 900 Cat-Bs
- MD in Proximity to Classified Discussion: 23 Cat-Bs

Joe D. Scent, a Technologist at Sandia National Laboratories, attended a classified meeting at Los Alamos National Laboratory and followed security protocols by leaving his mobile phone in his backpack in his government vehicle.

After returning to Sandia, he was focused on organizing his meeting notes and accidentally brought his backpack into his Secure Space office. During an impromptu discussion about the classified visit, Joe remembered that his mobile phone was in the backpack.

What should Joe do?

- Joe should wait for confirmation from colleagues before reporting the incident; to determine how sensitive the information was in the impromptu meeting.
- Joe does not have to report the situation because the impromptu meeting was in Secure Space and everyone in attendance had the proper clearance level and need-to-know for the information.
- Joe should report the incident to the Security Incident Management Program (SIMP) immediately to ensure a timely assessment of the situation.

Joe D. Scent reported the incident to the Security Incident Management Program (SIMP), which could not rule out the compromise of classified information due to an active transmission near a classified discussion. As a result, the incident was classified as a Category A Incident of Security Concern (IOSC). If there had been no active transmission, it would have been a Category B IOSC.

To address the situation, a Root Cause Analysis (RCA) was conducted to identify contributing factors and implement corrective actions. The analysis revealed critical insights into human performance indicators that can lead to an IOSC, highlighting that changes in routine, distractions, and time constraints significantly affect adherence to security protocols, emphasizing the need for thorough checks for prohibited and controlled articles before entering the Limited Area.

DID YOU KNOW?

If you suspect a violation of security policy or believe that classified information may have been compromised, please contact the Security Incident Management Program (SIMP) to initiate the reporting process:

- Dial **321** from a Sandia landline
- Call **505-845-1321** from any phone
- Email SIMP@sandia.gov

To create a Mobile Device Self Report, please visit SIMP Self Report.

For additional information: Policy SS007, Prohibited and Controlled Articles Policy, Policy SS008, Control Access to Information and Facilities, Policy IT004, Manage Controlled Electronic Devices, Training MD100: Mobile Device Usage, Mobile Devices and Secure Space, and PEDs at Sandia.

Causes of Security Incidents

Causes of Security Incidents

Task Demands	Individual Capabilities	Work Environment	Human Nature
Time pressure	Unfamiliarity with task / first time evolution	Distractions / Interruptions	Stress
High Workload	Lack of Knowledge	Changes / Departures from routine	Habit patterns
Simultaneous, multiple tasks	New technique not used before	Confusing displays or controls	Assumptions
Repetitive actions / monotony	Imprecise communication habits	Workarounds / OOS instruments	Complacency / Overconfidence
Irrecoverable Acts	Lack of proficiency / inexperience	Hidden system response	Mindset
Interpretation of Requirements	Indistinct problem-solving skills	Unexpected Conditions	Inaccurate risk perception
Unclear goals, roles, and responsibilities	'Unsafe' attitude for critical tasks	Lack of alternative indication	Mental shortcuts (biases)
Lack of unclear standards	Illness / Fatigue	Personality Conflicts	Limited short-term memory

Recognize when you're at risk and take a moment!

Think:

Are there any items in proximity to classified that are capable of recording/ transmitting information?

Assess:

Assess the risk.

Consider the potential damage that inadvertent disclosure may cause to you, the laboratory, research, our business partners, and ultimately, national security.

Protect:

Inquire with others if they possess any controlled articles.

Remind colleagues that controlled articles are not permitted near classified discussions or in Secure Spaces.

Conduct a thorough check to ensure you do not have any controlled articles in your possession.


HELP
MODULE 2:
The Importance of Timely Incident Reporting
BEGIN

In FY25, Security Connection received approximately 4,964 reports. Timely reporting of incidents is essential, as delays can result in serious consequences, including the potential compromise of classified information. All reporting must occur immediately or as soon as possible, after the event or circumstance, unless otherwise indicated.

Joe Smoe, an employee at Sandia National Labs with Sigma 15 access, was selected for a polygraph examination. Shortly after receiving the notification, he recalled instances where he had inadvertently brought his mobile device into secure areas, where classified discussions may have occurred. Concerned about potential security events, Joe contacted the Security Incident Management Program (SIMP).

When questioned by SIMP about whether his mobile device had an active transmission during those times, Joe could not definitively confirm or deny it. Due to the length of time when these events occurred, the Inquiry Official could not rule out a compromise and categorized the incident as a Category A Incident of Security Concern.

What should Joe Smoe have done upon realizing he brought his mobile device into a secure area?

- Wait until after the polygraph examination to report the incident.
- Immediately report the incident to the Security Incident Management Program (SIMP).
- Ignore the situation since he was unsure if any classified discussions occurred.
- Discuss the situation with his colleagues before reporting it.

Two months after the initial report, Joe received a notification from the Security Incident Management Program (SIMP) regarding the situation. SIMP conducted a thorough inquiry into the reported incidents, during which the Inquiry Official (IO) assessed the information provided by Joe and the circumstances surrounding his mobile device usage in secure areas. Due to Joe's delayed reporting, the IO could not definitively rule out the possibility of a compromise of classified information. This uncertainty surrounding the potential exposure of sensitive data led to heightened concern, resulting in the incident being categorized as a Category A Incident of Security Concern (IOSC).

More...

This case highlights the vital necessity of timely reporting in maintaining security integrity. Delays in reporting can not only jeopardize an employee's security clearance but also pose significant risks to their continued employment at Sandia National Labs. It is imperative that all employees prioritize security protocols and promptly report any incidents to ensure swift action and risk mitigation. By doing so, we collectively uphold the safety and confidentiality of our operations.

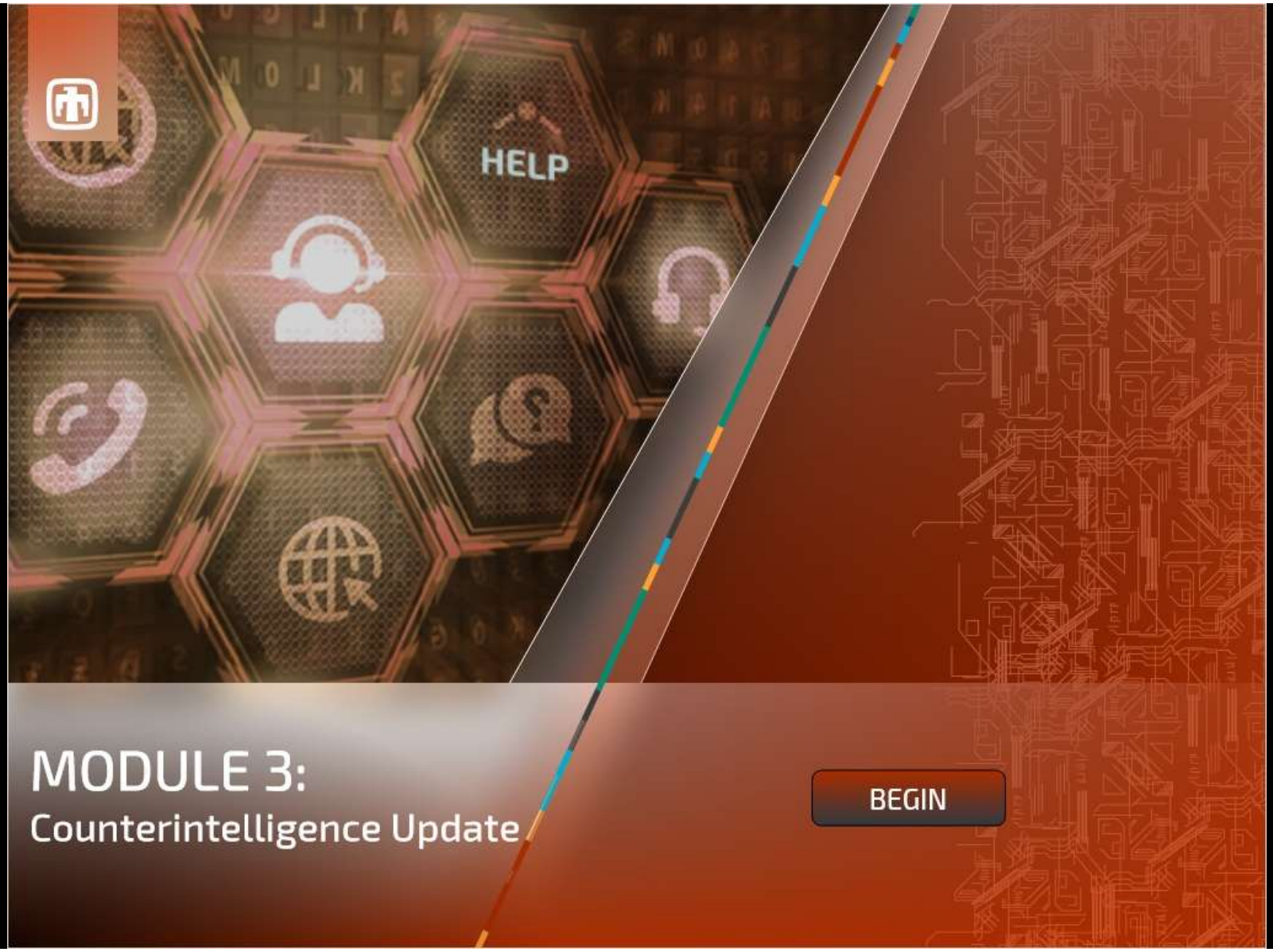
Back

DID YOU KNOW?

All MOWs are required to report the events and circumstances highlighted in the DOE and Sandia reporting requirements: DOE and Sandia Reporting Requirements of Security Interest. This includes various situations such as workplace incidents, law enforcement encounters, personal life circumstances, financial matters and other reporting obligations.

To begin the reporting process or if you have any questions regarding your reporting responsibilities, you can contact Security Connection at:

- **321** from a Sandia landline
- **505-845-1321** from any phone
- **security@sandia.gov** via email


HELP
MODULE 3:
Counterintelligence Update
BEGIN

Counterintelligence Update

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
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.

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

Unusual Solicitation
Foreign Travel
Insider Threat
Substantive Contact/Relationship
Social Media

Insider Threat

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

Report any individual to Counterintelligence who:

- Seeks unauthorized access to classified information, matter or special nuclear material without a Need-To-Know (NTK).
- Asks about classified projects, materials, etc. without a NTK.
- Attempts to access secure spaces not within the scope of work.
- Appears to be living well beyond their means or has sudden, unexplained affluence.
- Has unreported foreign contacts or travel.

Counterintelligence handles sensitive information with discretion to protect while balancing our responsibility to protect Sandia and national security.

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 contacts are defined by Sandia as personal or professional relationships that are enduring and involve substantial sharing of personal, business, or research information, and/or the formation of emotional bonds. They can be professional, personal, or financial in nature and include any ongoing contact that is solely through electronic communication (e.g., email, telephone, social media, or professional networking sites). Immediate family, defined as parents, siblings, spouses, and in-laws, are not reportable.

Substantive relationships with individuals who are Lawful Permanent Residents or "Green Card" holders are reportable. Individuals carrying dual citizenship with the U.S. do not need to be reported are not reportable.

Unusual Solicitation
Foreign Travel
Insider Threat
Substantive Contact/Relationship
Social Media

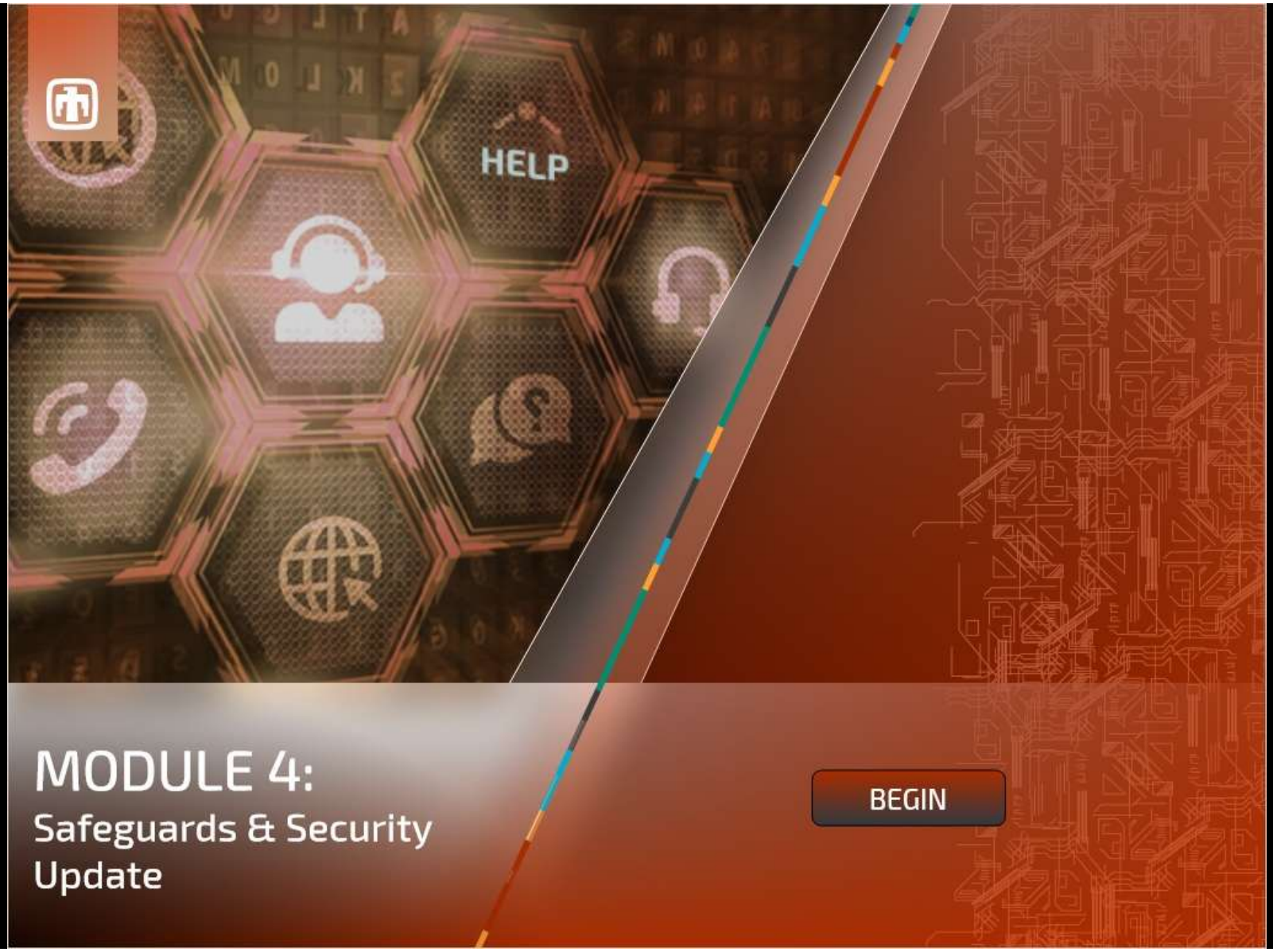
Social Media

Think before you post! Our adversaries are very interested in your social media activity.

- Limit the information you post, and don't post about foreign travel until you return home.
- Review your privacy settings to restrict your audience.
- Ensure you know everyone on your friends list in real life.
- Look out for fake accounts and unknown friend requests.
- Be wary of odd questions or requests to move to a different communication platform.

Also keep in mind that adversaries may manipulate or fabricate information seen on social media platforms. Be sure to verify outrageous information using trusted sources before reacting impulsively, especially as AI-generated content is becoming more common.

Unusual Solicitation
Foreign Travel
Insider Threat
Substantive Contact/Relationship
Social Media



MODULE 4:
Safeguards & Security Update

BEGIN

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 so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives. Per SS013, Critical Information Policy, all Sandia programs are required to have Critical Information List coverage, as formally vetted and published in the Critical Information List Library.

Critical information, as established in the aforementioned process, must be protected by all MOW as controlled unclassified information (CUI) using the Operations Security category by marking and controlling as CUI//OPSEC.

Sandia Critical Information Lists can be accessed via the Critical Information List Library. For more information, contact Sandia's OPSEC program at opsec@sandia.gov.

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.

Controlled Articles & CARP

Controlled articles are portable electronic devices (PEDs), both government and personally owned, that have a camera and/or microphone and are capable of transmitting data or recording information. Examples include video and photography cameras, recording equipment, transmitting equipment, and more.

Per SS007, Controlled and Prohibited Articles, Policy, you may not introduce controlled articles into Limited Areas or Vault-Type Rooms (VTR) without prior authorization using the Controlled Articles Registration Process (CARP). See Controlled Articles at Sandia for more information.

For more information, visit carp.sandia.gov or contact carp@sandia.gov.

CMPC Reminder

In an emergency situation, the health and safety of personnel takes precedence over the need to secure classified matter.

Protect classified matter in one of the following ways:

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

If the classified matter cannot be protected as described above or a classified storage repository is left unsecured during evacuation:

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

OPSEC: Critical Information Update

Reporting Requirements

Controlled Articles & Carp

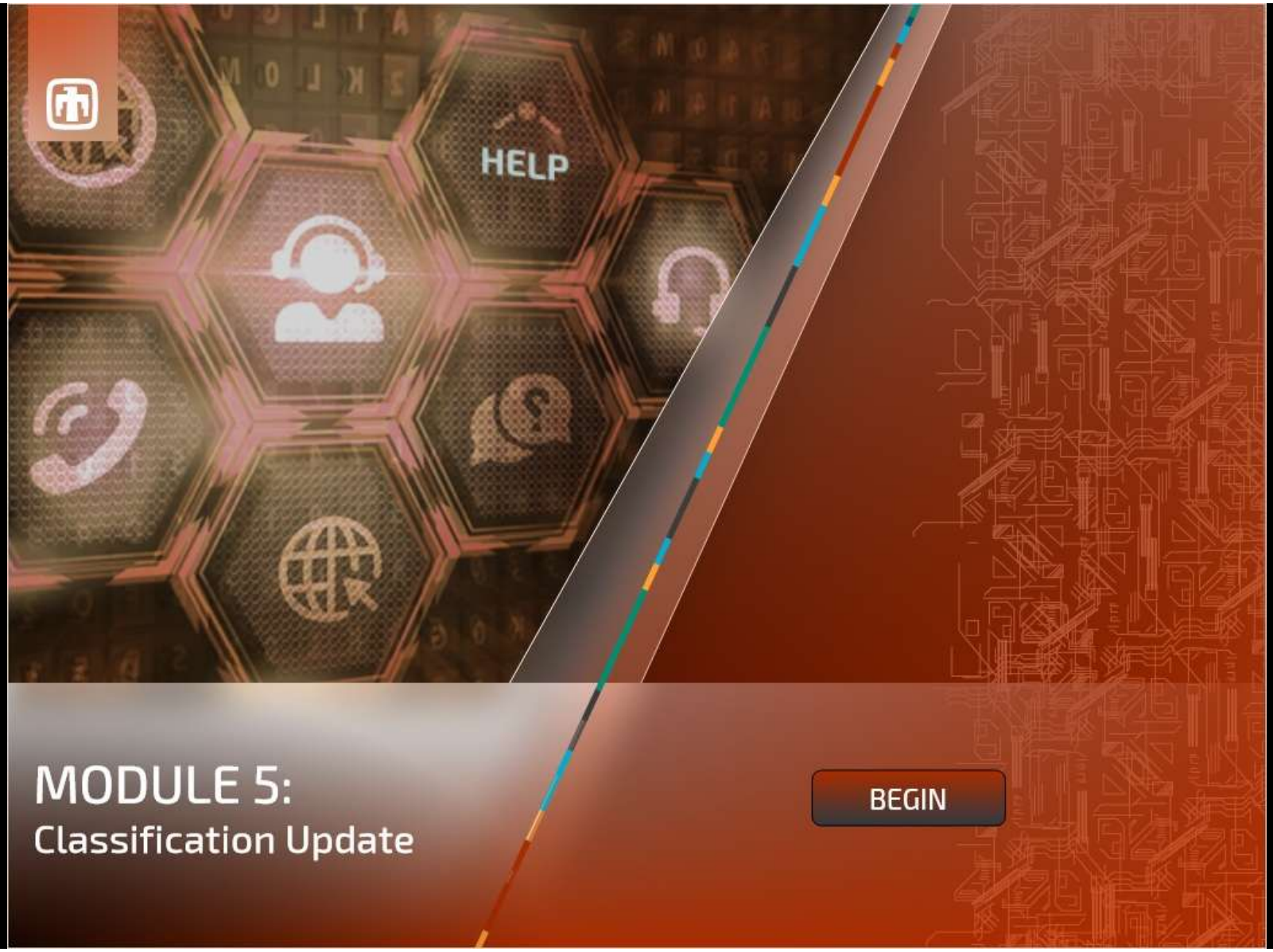
CMPC Update

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 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.


HELP
MODULE 5:
Classification Update
BEGIN

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).

For Questions:
NM: classificationdept@sandia.gov
CA: 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 means a determination by appropriate authority that information or documents previously determined to be classified no longer require protection against unauthorized disclosure in the interests of national security. A declassification action may be taken when classification guidance has changed, or a Date or Event has passed. Only a Derivative Declassifier (DD) may declassify Sandia-generated information.

For Additional Information See KBA 642 in the Security Connection Knowledge Base.

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.

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
In California: 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. 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.

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.

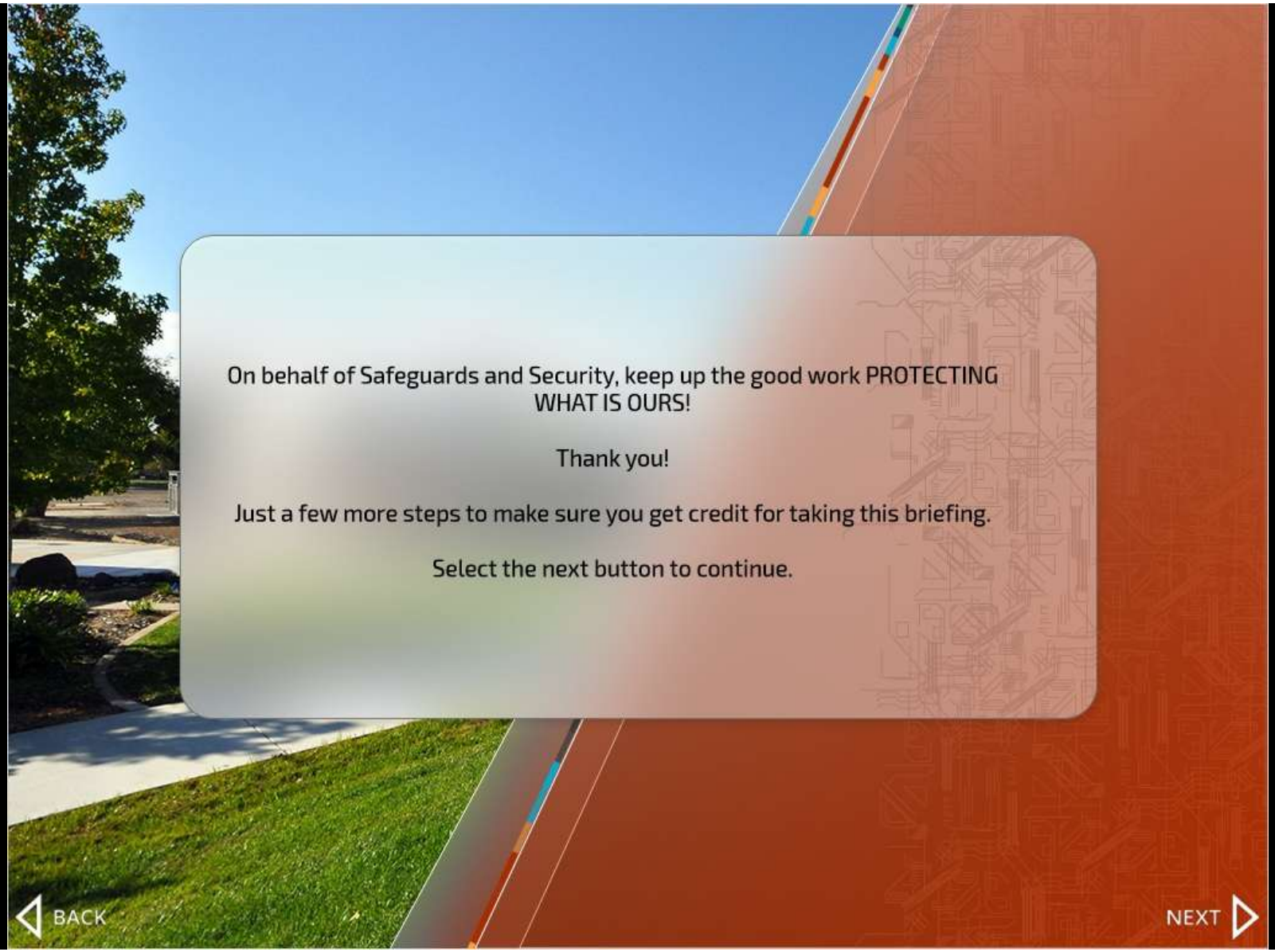
CLASSIFICATION UPDATE

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.
BACK
NEXT

SEC100 Completion Record: 2025/2026

By completing this form, you acknowledge that you have read the
Sandia National Laboratories 2025/2026 Annual Security Refresher Briefing
and understand your security responsibilities.

Complete the information below and email to 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