SEC100: Annual Security Refresher Briefing

Sandia National Laboratories

SAND2020-8558 TR

Safeguards & Security Awareness Program

Security+ YOU

Think. Assess. Protect.

U.S. DEPARTMENT OF ENERGY NNSA

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

MEET KELLIE!

Hi, I'm Kellie and with my extensive experience and passion for safeguards and security, I will be your guide for the Annual Security Refresher Briefing. In this briefing we will review some common incidents that have occurred this year.

We have provided resource documents that include information and guidance to ensure you meet the DOE and Sandia requirements for Safeguards and Security.

INTRODUCTION

Today I want to talk about security.

Security is not just a program at Sandia – it's a culture and a mindset. As a national security laboratory, our work is vital to global peace and supports our country's central role in political and economic stability.

Sandia is relied upon to maintain secure operations. We have a responsibility to protect our nation's assets.
Lives are at stake. Sandia technology is in the hands of the American warfighter. If adversaries knew the details of these technologies, our military, and thus our Nation, could be in real danger.

This month is the 75th anniversary of the Manhattan Project, and we are reminded of the magnitude of our mission and the seriousness of protecting the information around it. Every day our adversaries look for opportunities to learn what we know and use it to gain military, commercial, and other advantages. If you have read about the history of the Manhattan Project, you know that our adversaries are always watching, waiting to capitalize on a moment of carelessness, complacency or even recruitment of an asset.

Their patience is great. Our vigilance must be greater. We cannot afford to let our guard down. The stakes are too high and consequences too grave.

Security, along with safety, must be a top priority. We have to pay attention to security every day, in every email, every conversation, every document.

Ultimately, security begins and ends with you and me. Each of us must take personal responsibility to understand the risks and requirements to protect people, information, facilities, and materials.

Think, assess, protect. The threat is real. You can make a difference by asking questions and reporting security concerns and anomalies immediately. As you go about your work, remember the men and women in uniform, their families, and people in other countries who live in fear of violence or oppression — all of them depend on us to take security seriously.

Thank you.

--James Peery

Course Objective:

Reinforce DOE and Sandia security duties and responsibilities related to physical and logical access to unclassified or classified information or matter through scenarios and resource documents to reduce the threat and address the biggest operational concerns associated with working at this laboratory.

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.

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

- **IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)**
- IMPROPER STORAGE OF CLASSIFIED
- IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE

Approximately 2% of Incidents of Security Concern (IOSCs) are a result of sensitive UCI not being protected according to DOE storage and protection requirements.

YOU HIRED WHO?

Jamie is a Sandia project lead on an Official Use Only/Export Controlled Information (OUO/ECI) and Unclassified Controlled Nuclear Information (UCNI) project. Work for the project was subcontracted out to Jesse Engineering Company (JEC).

Jamie discovers that JEC had foreign national personnel working on the project, which may have lead to unauthorized access to OUO/ECI and UCNI.

What Must Jamie Do?

- Jamie must ask the subcontractor to remove the foreign national personnel from the Sandia project.
- Jamie must report the foreign national's potential access to OUO/ECI and UCNI to the Security Incident Management Program (SIMP).

YOU HIRED WHO?

Jamie is a Sandia project lead on an Official Use Only/Export Controlled Information (OUO/ECI) and Unclassified Controlled Nuclear Information (UCNI) project. Work for the project was subcontracted out to Jesse Engineering Company (JEC).

Jamie discovers that JEC had foreign national personnel working on the project, which may have lead to unauthorized access to OUO/ECI and UCNI.

What Must Jamie Do?

- ☒ Jamie must ask the subcontractor to remove the foreign national personnel from the Sandia project.
- ☑ Jamie must report the foreign national's potential access to OUO/ECI and UCNI to the Security Incident Management Program (SIMP).

YOU HIRED WHO?

A SIMP inquiry was conducted and determined that JEC foreign national personnel had access to Official Use Only/Export Controlled Information (OUO/ECI) and Unclassified Controlled Nuclear Information (UCNI) documents and items.

This constituted a compromise of Departmental assets. JEC received an incident for improper protection of sensitive UCI.

Sandia reminded JEC that a Foreign National Request Security Plan (FNR SP) is required prior to allowing foreign national access to Sandia information, systems, or premises.

Did You Know?

Sandia and our contractors must conduct business in strict accordance with applicable laws, rules, regulations, and contract requirements. You are responsible for identifying, understanding, mitigating, and managing risk essential for mission success.

THINK, ASSESS, PROTECT

Click on each image to learn more.

You must click each of the icons to continue.

Think

Do I fully understand the type(s) of information that will be generated while working in this new project? OUO (such as Export Controlled Information [ECI]), UCNI, etc.?

Assess

Based on the type(s) of information, do all parties of the project understand the protection requirements?

Protect

I must ensure my projects include work controls to properly mark, store, disseminate, and destroy information according to the information's protection requirements.

- UCI Handout
- OUO101: Understanding Official Use Only
- IT012 Unclassified Controlled Information Policy (policy references included in IT012)
- SS009 Foreign Interactions Policy

BACK

Unclassified Controlled Information (IT012 -Unclassified Controlled Information Policy)

Unclassified Controlled Information (UCI) - information which disclosure, loss, misuse, alteration, or destruction could adversely affect national security, Sandia National Laboratories, or our business partners. It is the policy of DOE and Sandia to conduct as much research and development on an unclassified basis as possible to promote the free exchange of ideas, which is essential to scientific and industrial progress. DOE and other federal agencies require controls on the availability of certain scientific and technical information, classified or unclassified. Information identified as UCI must be marked accordingly.

First, determine if your information is:

Sandia-owned = Sandia Proprietary

Then, based on content, what type of proprietary information it is:

- Employment Related Records
- Confidential Financial/ Honeywell International Correspondence
- Legal Records
- Procurement Actions
- Technology Transfer
  - Such as:
    - IP license agreements
    - Protected CRADA Information
    - Certain intellectual property

U.S. Government-owned

Then, based on content/sponsor, what type of information it is:

- OUO
  - Exemption 1. Classified Information Only
  - Exemption 2. Circumvention of Statute
  - Exemption 3. Statutory Exemption
  - Exemption 4. Commercial/proprietary
  - Exemption 5. Privileged Information
  - Exemption 6. Personal Privacy
  - Exemption 7. Law Enforcement
  - Exemption 8. Financial Institutions
  - Exemption 9. Wells
- UCNI
- SGI
- U-NNPI
- Other U.S. Gov't Agency
  - Such as:
    - Dept. of Defense
    - Dept. of Homeland Security
    - Dept. of Transportation

No longer applicable for DOE or SNL

FOIA exemptions most commonly used at Sandia are 3-7

Do not use Exemption 8 at SNL

Personally Identifiable Information (PII) *can apply to both U.S. government-owned and Sandia-owned information and must include both types of markings.*

PII

OUO - Official Use Only **UCNI** - Unclassified Controlled Nuclear Info. **SGI** - Safeguard Info. **U-NNPI** - Unclassified Naval Nuclear Propulsion Info.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.AC04-85000.

02/2020 v12 | SAND2019-1004TR

U.S. DEPARTMENT OF ENERGY NNSA

Unclassified Controlled Information (IT012 -Unclassified Controlled Information Policy)

OUO is U.S. Government-owned unclassified controlled information that is exempt from public release under the FOIA (Freedom of Information Act) and has the potential to damage government, commercial or private interests if disseminated to persons without a NTK. Members of the workforce should be able to identify which subjects, program, processes, documents, emails, slideshow presentations, faxes, or any other forms within your organization or programs have the potential to include OUO information. Your program's Derivative Classifier should have guides that include OUO topics relevant to your organization's work. Once a document is identified as OUO, it should be properly marked as OUO and the appropriate FOIA exemption selected and applied to your information.

FOIA exemptions most commonly used at Sandia are 3 – 7 per IT017, Official Use Only Information Policy

FOIA Exemption	Category Name	What It Protects
Exemption 1	Classified	NEVER used for OUO. It is only used for classified information.
Exemption 2	Circumvention of Statute	***No Longer Applicable for DOE & SNL.***
Exemption 3	Statutory Exemption	Information whose disclosure is specifically protected by law and not otherwise controlled.
Exemption 4	Commercial/ Proprietary	Trade secrets, commercial or financial information, if release could impair the government's ability to obtain information in the future.
Exemption 5	Privileged Information	Interagency or intra-agency memos or letters not available by law to a party unless the party is in litigation with the agency.
Exemption 6	Personal Privacy	Information that could cause an individual personal distress or embarrassment, or expose them to identity theft.
Exemption 7	Law Enforcement	Information that if released could endanger the life or physical safety or disclose techniques and procedures for law enforcement investigations or prosecutions.
Exemption 8	Financial Institutions	Evaluation of a financial institution's stability. ***Do not use at SNL***
Exemption 9	Wells	Geological and geophysical information and data, resource maps, and new drilling techniques.

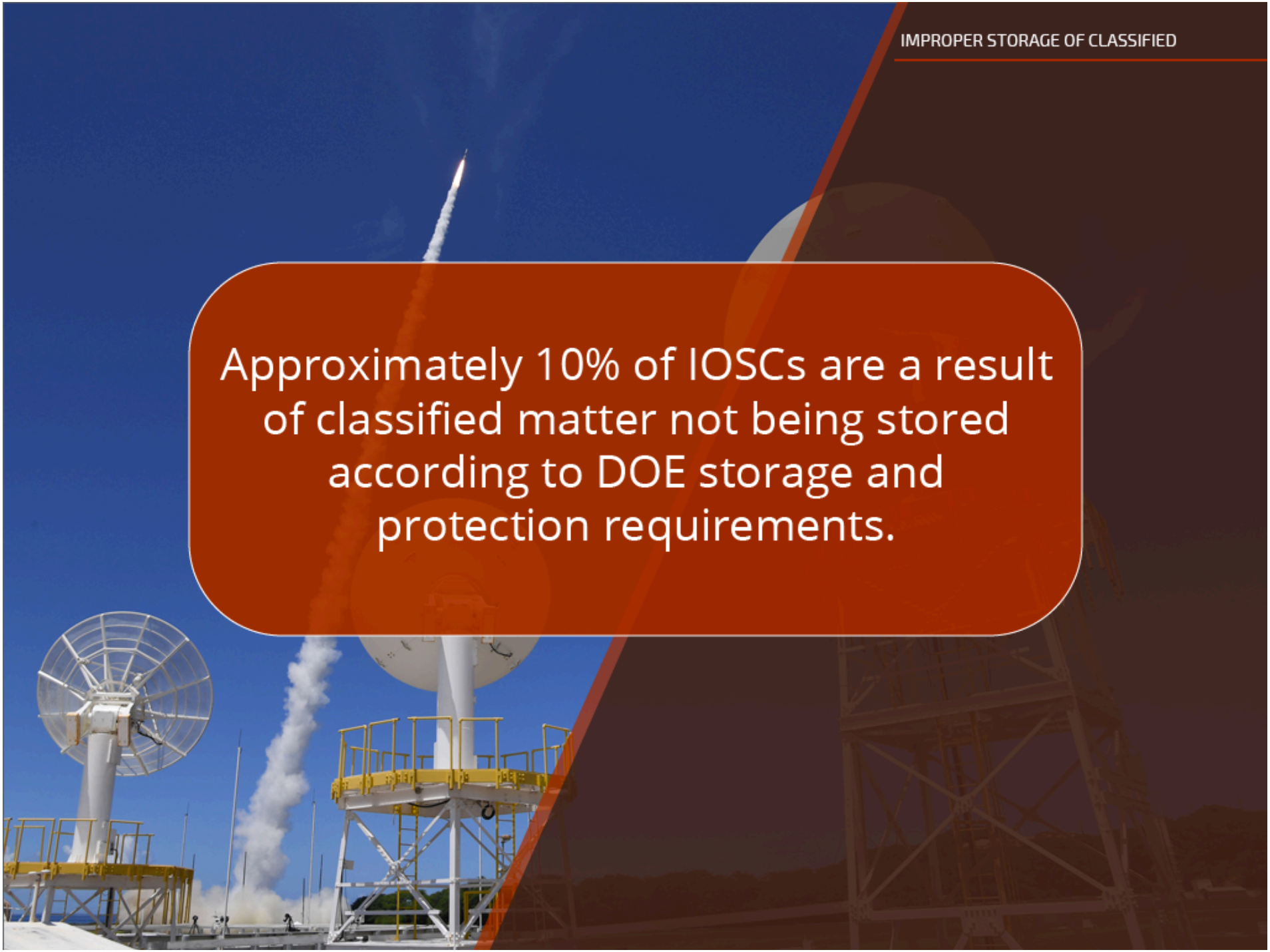
Email

Email containing UCI must also be protected and properly marked. Some types of UCI require use of an approved encryption method such as Entrust or FIPS 140-2 methods. Sandia has an internal UCI email marking assistant tool to help properly mark emails sent internally as well as emails sent outside the sandia.gov domain.

Share UCI only when it is necessary to support official Sandia business and apply Need to Know (NTK) when disseminating UCI.

COURSE MODULES

- IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- IMPROPER STORAGE OF CLASSIFIED
- IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE



Approximately 10% of IOSCs are a result of classified matter not being stored according to DOE storage and protection requirements.

AT THE END OF THE DAY

Bentley returns to work after 3 months of telecommuting to attend several meetings. She can't remember the safe combination, and meets with her Classified Administrative Specialist (CAS) to get her classified lab notebook from the safe.

Bentley attends several meetings and adds notes to her notebook throughout the day. At the end of the day, Bentley tries to return the classified lab notebook but the CAS has left for the day.

What Must Bentley Do?

- Bentley must lock up the classified notebook in her limited area office cabinet and close the door for the day.
- Bentley must contact someone with access to a repository approved to store the classified information (level, category, caveats) in her notebook.

AT THE END OF THE DAY

Bentley returns to work after 3 months of telecommuting to attend several meetings. She can't remember the safe combination, and meets with her Classified Administrative Specialist (CAS) to get her classified lab notebook from the safe.

Bentley attends several meetings and adds notes to her notebook throughout the day. At the end of the day, Bentley tries to return the classified lab notebook but the CAS has left for the day.

What Must Bentley Do?

- ☒ Bentley must lock up the classified notebook in her limited area office cabinet and close the door for the day.
- ☑ Bentley must contact someone with access to a repository approved to store the classified information (level, category, caveats) in her notebook.

AT THE END OF THE DAY

A SIMP inquiry was conducted when Bentley called the next day to self-report. It was determined that Bentley should have called Sandia's Protective Force or found an alternate storage method to secure her classified lab notebook.

Bentley received an incident for the improper storage of her classified lab notebook. During a formal review of the incident, she was coached by her manager and Deployed Security Professional (DSP) on the importance of properly securing classified information and reminded of the steps she must take every time to ensure proper storage before the end of the day.

Did You Know?

Sandia's Protective Force can assist with end of day storage solutions (e.g., if unable to return classified items to approved storage). For SNL/NM call Security Connection (505) 845-1321.
For SNL/CA call (925) 294-2300.

THINK, ASSESS, PROTECT

Think

Do I understand the protection/storage requirements for classified?

Assess

Do I know what steps to take if I am not able to access a storage repository when I need it?

Protect

I must plan ahead to ensure I can store classified in a GSA repository (i.e., safe or VTR) that is approved for the classification level and category of the information.

- Reporting Requirements
- SEC301 Classified Matter Training
- SS003 Classified Matter Protection and Control (CMPC) Policy

DOE and SNL Reporting Requirements of Security Interest

Instructions:

- The events and circumstances described below are reportable by the individuals specified in the spanning subheadings.
- All reporting must occur immediately or as soon as possible, but no later than two (2) working days after the event/circumstance.
- Contact Security Connection at 321 from Sandia landline, 505-845-1321 from any phone, or security@sandia.gov to begin the reporting process.

Members of the Workforce (MOWs)

All MOWs are required to report the events/circumstances specified below, when applicable. However, highlighted items are applicable only to clearance holders and clearance applicants.

1	General Requirements	Become aware of information that raises concerns of personnel security interest* about others who are applying for or in possession of a DOE security clearance. **Concerns of personnel security interest include but are not limited to the reportable circumstances cited in this guide.* *Note: Individuals who report circumstances about others may be asked to provide additional, corroborative information.*
2		Approached or contacted by any individual seeking unauthorized access to classified matter or special nuclear material (SNM).
3	Life Circumstances	Marry or cohabitate. *Note: A cohabitant is a person who lives in a spouse-like relationship or with a similar bond of affection or obligation, but is not a legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).*
4		Legal action taken for a name change.
5	Law Enforcement	Arrested or subject to criminal charges (including charges that are dismissed), citations, tickets, summonses, or detentions by federal, state, or other law-enforcement authorities for violations of law within or outside of the U.S. *Exception: Traffic violations for which a fine of up to $300 was imposed* need not be reported,* ***unless the violation was alcohol- or drug-related****.* **"Imposed" means agreement to pay the fine, or a court ruling to pay, exclusive of court fees or other administrative costs.*
6	Financial Matters	Personal or business-related filing for bankruptcy.
7		Garnishment of wages (e.g., due to debts, divorce, child support).
8	Citizen-ship	Change in citizenship (i.e., U.S. or foreign) or acquisition of another country citizenship(s).

Sandia National Laboratories

SAND2020-13375 O

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

9	Drug Use	Use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction.
10		Treatment for drug abuse.
11		Positive (i.e., unfavorable) drug test regardless of source (e.g., court-ordered, military, employment).
12	Alcohol Use	Treatment for alcohol abuse.
13	Mental Health	Hospitalization for mental health reasons.
14	Foreign Travel	Travel to a sensitive country for personal reasons. *Note: A list of sensitive countries is available at the Counterintelligence (CI) website. Although not required, keeping a record of personal foreign travel to a non-sensitive country is recommended as a reference for future clearance (re)investigations.*
15		Travel to any country where discussions with sensitive-country foreign nationals regarding sensitive subjects are anticipated or have occurred. *Note: This includes chance meetings where sensitive-country foreign nationals are in attendance.*
16		Travel to any country where sensitive subjects will be discussed.
17	Foreign Interaction	Substantive contact with **any** foreign national. *Note: "Substantive contact" refers to 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). The phrase also applies to associations that involve sharing of SNL business information.*
18		Contact with foreign nationals who make requests that could be attempts at exploitation or elicitation.
19		An immediate family member assuming residence in a sensitive country and/or when that changes (i.e., return to the U.S. or movement to any other country). *Note: A list of sensitive countries is available at the Counterintelligence (CI) website.*
20		Employment by, representation of, or other business-related associations with a foreign or foreign-owned interest or with a non-U.S. citizen or other individual who is both a U.S. citizen and a citizen of a foreign country.
21		Participation in research or talent recruitment programs that are sponsored or managed by China, Iran, North Korea, and Russia.
22		Participation in other activities (including employment, academic or professional appointments, grant programs and contracts) sponsored by China, Iran, North Korea, and Russia.
23	Workplace Circumstances	Incidents of Security Concern (IOSCs).
24		Waste, fraud, and abuse.
25		Property theft.
26		Use, possession, transfer, sale, or trafficking of illegal drugs.
27		Counterfeit/Suspect Items

SCI- and SAP-Briefed Personnel
Additional reporting requirements may apply. **SCI-holders** are directed to access the FIE Reporting Requirements webpage (restricted access). **SAP-briefed** personnel are advised to contact the applicable SAP security POC(s) within Org. 5114 for specific guidance.

Managers	
Items below are applicable to clearance holders and clearance applicants. Compliance with some items may already follow existing procedures that remain in force. Otherwise, contact Security Connection.	
A	Awareness of any circumstances cited under “Members of the Workforce” above.
B	Action taken to restrict or withdraw access to classified matter or special nuclear material (SNM) without DOE direction.
C	An offer of employment has been declined.
D	Failure to report for duty.
E	Individual's death.
F	Termination of employment.
G	Determination that a security clearance is no longer required.
H	Failure or refusal to cooperate with authorized and appropriate personnel-security-related requests.
I	Circumstances that temporarily eliminate the need for access to classified information or SNM for 90 calendar days or more (e.g., temporary change of duties, maternity or other extended leave, detail to another agency, military deployment).

Exceptional service in the national interest

Sandia National Laboratories

SEC301 Classified Matter Training

This training can be found in the Security Toolcart at the link below,

http://www.sandia.gov/security/_assets/documents/SEC301.pdf

SAND 2015-7085 TR

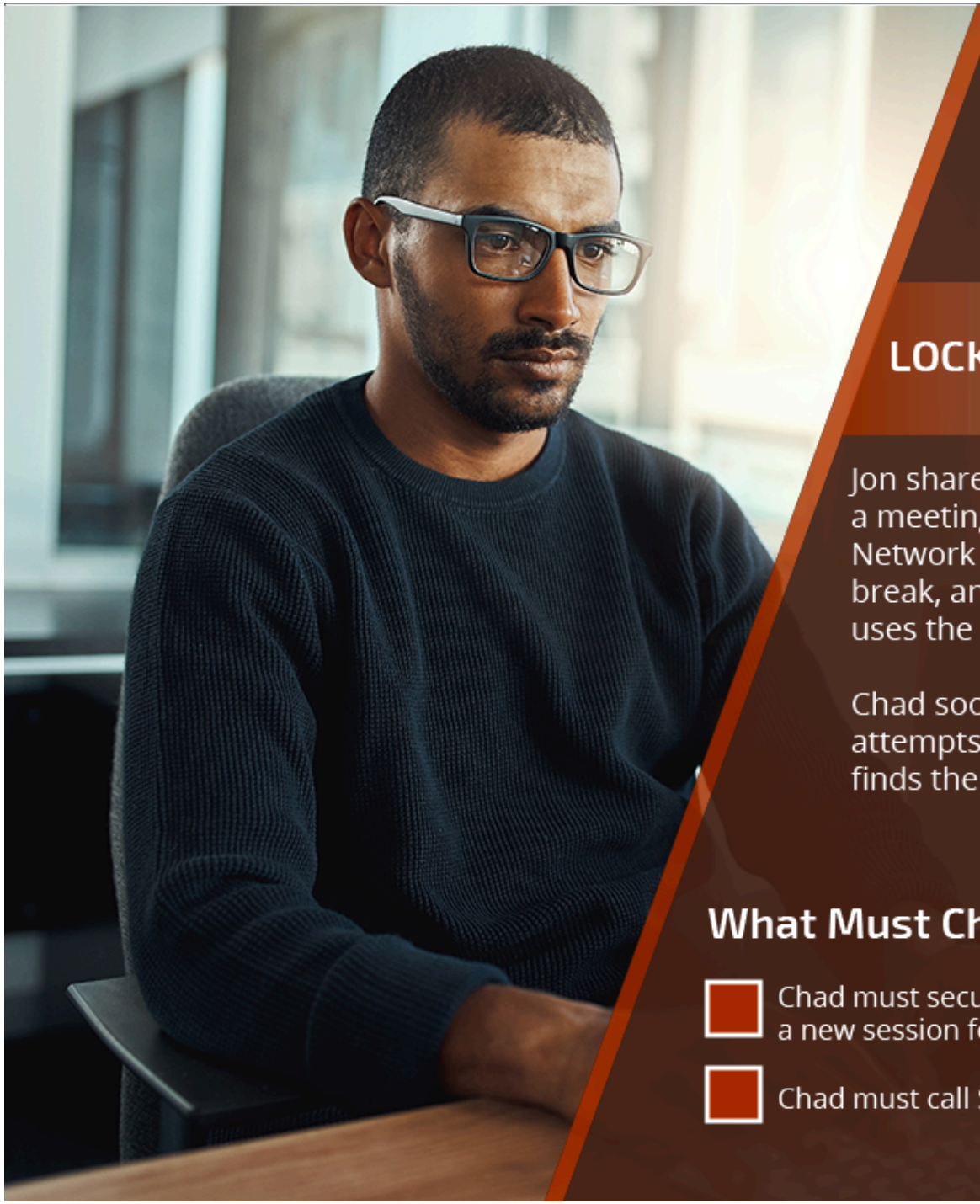
U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND NO. SAND 2015-7085 TR

COURSE MODULES

- ✓ IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- ✓ IMPROPER STORAGE OF CLASSIFIED
- IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE

Approximately 20% of IOSCs are a result of users not properly securing classified information systems.



LOCK BEFORE YOU WALK

Jon shares an office with Chad. While Chad is at a meeting, Jon logs into their Sandia Classified Network (SCN) terminal. Jon gets up for a break, and doesn't pay attention as he quickly uses the shortcut keys to lock his terminal.

Chad soon returns from his meeting and attempts to log on to the SCN terminal and finds the session active.

What Must Chad Do?

- Chad must secure the unattended session, then he can start a new session for his work.
- Chad must call SIMP to report the active session.

LOCK BEFORE YOU WALK

Jon shares an office with Chad. While Chad is at a meeting, Jon logs into their Sandia Classified Network (SCN) terminal. Jon gets up for a break, and doesn't pay attention as he quickly uses the shortcut keys to lock his terminal.

Chad soon returns from his meeting and attempts to log on to the SCN terminal and finds the session active.

What Must Chad Do?

- ☒ Chad must secure the unattended session, then he can start a new session for his work.
- ☑ Chad must call SIMP to report the active session.

LOCK BEFORE YOU WALK

A SIMP inquiry was conducted after Chad called SIMP to report. It was determined that because Jon was not paying attention, he had not correctly logged out and did not visually confirm the session was successfully secured.

Jon received the incident for the improperly secured information system and was advised to confirm the session is successfully secured every time (lock before you walk!)

Chad was commended for not leaving the kiosk unattended and his timely reporting to SIMP.

Did You Know?

Deployed Security Professionals (DSPs) help you work through security issues specific to your work. They can share best practices and other strategies to help ensure that classified is secured the right way every time. Call Security Connection at (505) 845-1321 to identify your DSP.

THINK, ASSESS, PROTECT

Think

Do I understand the requirements and best practices to properly use a classified terminal/kiosk?

Assess

What kind of damage could be done to national security if the classified information accessible through the classified network is left unsecure?

Protect

I must ensure I visually confirm the session has been secured every time (Lock Before You Walk).

- Lock Before You Walk Security Message
- IT002 Use Sandia's Information Technology Resources Policy

Security Message

#1 OPERATIONAL PRIORITY: SAFETY & SECURITY

Security+ YOU
Think. Assess. Protect.

LOCK BEFORE YOU WALK

Lock before you Walk

August 2019

Protect sensitive information and prevent security incidents—always secure your computer before walking away.

Shortcuts to secure your Windows computer

- Press Windows key + L on your keyboard
- Press "ctrl+alt+del" and select the "lock" option (Windows 10), or "lock this computer" (Windows 7)
- Windows 10: From Windows icon in lower left corner, choose your User icon, and then select "Lock"
- Windows 7: Windows "Start" option in lower left corner, expand the choices on "logoff" and select "lock"

(On a Zero Client – just "tap" the power button. This immediately disconnects your session. The power button will be "blue" to show it has remained ON, but disconnected.)

For questions or to report
321 from a Sandia landline | 505-845-1321 from any phone
security@sandia.gov

Reporting

- In a **classified** environment, report any unsecured workstation.
- In an **unclassified** environment, report if you suspect unauthorized access to sensitive, unclassified information.

Resources

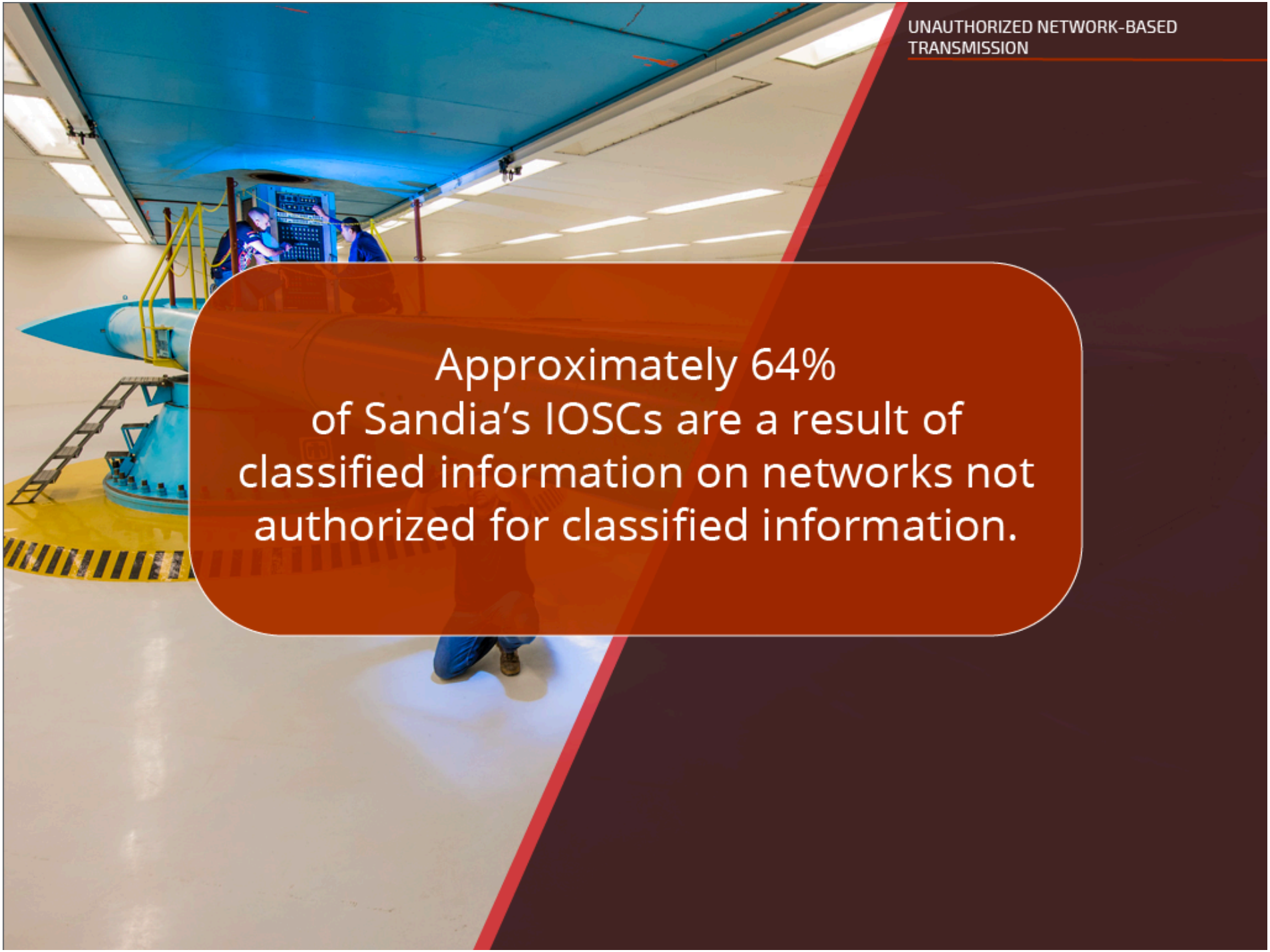
- Classified Computing Continual Service Improvement (3CSI)
- SS003 *Classified Matter Protection and Control (CMPC) Policy*
- IT002 *Use Sandia's Information Technology Resources Policy*
- Article 191 *Unattended Classified Desktops - Screen Locking and End-Of-Day Process*

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-14012 TR

NNSA ENERGY

COURSE MODULES

- ✓ IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- ✓ IMPROPER STORAGE OF CLASSIFIED
- ✓ IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE



UNAUTHORIZED NETWORK-BASED TRANSMISSION

Approximately 64%
of Sandia's IOSCs are a result of classified information on networks not authorized for classified information.

LADIES AND GENTLEMEN, TODAY'S PRESENTATION...

Elyse, a Sandia manager, is looking for a presentation to use for an upcoming meeting with new employees about her program.

Elyse discovers a presentation on the Sandia Restricted Network (SRN) that was authored by a retired Sandia employee from her organization. Elyse downloads the presentation to add some updates and identifies that the presentation contains classified information.

What Must Elyse Do?

- Elyse must remove the classified content to use it.
- Elyse must call SIMP to report her discovery.

UNAUTHORIZED NETWORK-BASED TRANSMISSION

LADIES AND GENTLEMEN, TODAY'S PRESENTATION...

Elyse, a Sandia manager, is looking for a presentation to use for an upcoming meeting with new employees about her program.

Elyse discovers a presentation on the Sandia Restricted Network (SRN) that was authored by a retired Sandia employee from her organization. Elyse downloads the presentation to add some updates and identifies that the presentation contains classified information.

What Must Elyse Do?

- ☒ Elyse must remove the classified content to use it.
- ☑ Elyse must call SIMP to report her discovery.

LADIES AND GENTLEMEN, TODAY'S PRESENTATION

A SIMP inquiry was conducted and determined that since 1997 numerous employees had access to different versions of the presentation. While some, including the author, were familiar with the classified subject area, no one questioned the classified content or sought a derivative classifier (DC) review.

All versions contained multiple levels and categories of classified and had been delivered in unclassified public venues, provided on unclassified electronic media, and recorded in a video stored on the SRN. Sandia National Laboratories received a civil penalty for numerous violations including Unauthorized Network Based Transmissions.

Did You Know?

Most security incidents can be avoided by engaging a DC early on. In this case, years of failure to seek a DC review of the presentation resulted in DOE Office of Enforcement issuing Sandia National Laboratories a Final Notice of Violation, imposing a substantial civil monetary penalty.

UNAUTHORIZED NETWORK-BASED TRANSMISSION

THINK, ASSESS, PROTECT

Think

Am I certain (knowledgeable and confident) that a presentation in a potentially classified subject area is unclassified before I use it?

Assess

Before I use the presentation, should I engage a subject matter expert DC for guidance to identify what is, or creates, classified?

Protect

I must be knowledgeable and confident that the information is unclassified before I use, edit, or disseminate it. I will use Review and Approval for presentations that include a widespread, public, unknown, or uncontrolled audience.

- Getting Started with Classified
- Understanding Classification
- SS002 Identifying Classified Information Policy

Getting Started with Classified

The purpose of the Classification Program is to identify information classified under the Atomic Energy Act or Executive Order (E.O.) 13526, so that it can be protected against unauthorized dissemination. Identifying Classified Information Policy (SS002) contains much of what you'll need to know when working with classified information at SNL. Below are some of the terms you'll hear regarding classified information.

Classified information – Information that is classified by statute or Executive Order.

Classified matter – Any combination of documents and material containing classified information. Access is restricted to persons with appropriate access authorizations (security clearances) and "need to know." Department of Energy (DOE) classification levels and categories are based on the potential for damage to national security, also known as the "risk." Levels, categories, and damage criteria define what protections are needed. As risk increases, so do protection measures, including the clearance level required for access to the information.

	Level		
Category	Top Secret (TS)	Secret (S)	Confidential (C)
Restricted Data (RD)	Q only	Q only	Q and L
Formerly Restricted Data (FRD)	Q only	Q and L	Q and L
Transclassified Foreign Nuclear Information (TFNI)	Q only	Q and L	Q and L
National Security Information (NSI)	Q only	Q and L	Q and L
Degree of Damage	Exceptionally Grave	Serious	Damage

Restricted Data (RD), all data concerning the design, manufacture, or use of nuclear weapons; production of special nuclear material; or use of special nuclear material in the production of energy.

Formerly Restricted Data (FRD), classified information that relates primarily to the military utilization of atomic weapons. Examples of FRD include nuclear weapon stockpile issues, nuclear weapon yields, and past and present weapon storage locations.

Transclassified Foreign Nuclear Information (TFNI), deals with specific intelligence information concerning certain foreign nuclear programs removed from the RD designation by agreement between DOE and the Director of National Intelligence.

National Security Information (NSI), all information concerning scientific, technological or economic matters relating to national security; programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems/installations; nonproliferation studies; foreign government information; and intelligence/counterintelligence information.

Protecting and Controlling Classified Information and Matter (SS003, Classified Matter Protection and Control [CMPC] Policy)

When working with classified information on a computer, use only computers connected to an approved classified network (e.g., Sandia Classified Network [SCN]) or an approved classified stand-alone system.

Information processed on a classified computing system must be marked and protected at the highest potential level and category for that information you believe it contains. If unsure, consult your DC or mark as "system high" until it is reviewed by an authorized Derivative Classifier, then the markings must be updated as necessary.

When exporting any data from a classified system to an unclassified one (whether electronically or by use of electronic media), an Authorized Transfer Point (ATP) must be used and approved processes must be followed.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-7610 O 04.2020 v7

U.S. DEPARTMENT OF ENERGY | NNSA

Security+ YOU
Think. Assess. Protect.

CALL SECURITY CONNECTION AT 505-845-1321

Getting Started with Classified

Derivative Classifier (DC) – An individual authorized to determine that a document, equipment, or material is unclassified or classified based on classification guidance or source documents, as allowed by his or her description of authority.

Only trained DCs determine whether documents, equipment, or material are classified, and to what level and category. DCs are trained on specific technologies/programs—what is not classified on one technology may be classified in other circumstances. Be sure to choose the right DC.

You must request a DC review (either a formal, or a programmatic review) for:

- A newly generated document or material in a classified subject area that may potentially contain classified information.
- An existing, unmarked document or material that you believe may contain classified information.
- An existing, marked document or material that 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.

Derivative Declassifier (DD) – An individual authorized to declassify or downgrade Sandia-originated document, equipment or material in specified areas as allowed by his or her description of authority.

DDs are located in the Classification Office.

Declassification review must occur when document/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 marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities.

You can find a DC or DD at the Jupiter website or call Security Connection

Classified Administrative Specialist (CAS) – An individual trained to mark, store, duplicate, destroy, and mail classified matter. **Work with your manager to identify your CAS.**

Classified Matter Protection and Control (CMPC) – assists staff and CASs with questions regarding marking, protection, storage, and transmission of classified information. **Work with your CAS or manager to address CMPC issues.**

Classification Office – assists DCs and staff with classification decisions. Reviews information for public release. If you think a DC determination is incorrect, you have the right and are encouraged to challenge the classification status of information by contacting the Classification Office. **NM (505) 844-5574 | CA (925) 294-2202**

DOE Office of Classification – If a classification challenge can't be resolved locally, Sandia's Classification Officer will submit a challenge in writing to the Director, DOE Office of Classification. You also have the right to submit a formal written challenge directly to the Director. Under no circumstances will you be subject to retribution for making such a challenge. **Request information from outreach@hq.doe.gov.**

You must use the formal Review and Approval (R&A) process if you intend to release information to an uncontrolled, widespread, unknown, or public audience. This includes information intended for release to congress.

Work with your **Cyber Security Representative** to identify **secure forms of communication** (e.g., for classified computing).

If you see unattended classified matter, secure it and report it to Security Connection.

WHEN SHOULD YOU HAVE A DOCUMENT REVIEWED?

Documents must be reviewed before they are:

- finalized,
- sent outside of the organization or working group on which you are serving, or
- filed permanently.

Prior to getting a review, you should protect and mark the document at the highest potential classification level, category, and caveat (Sigmas 14, 15, 18 and 20) of information that you believe is in the document.

Working papers and/or living documents are documents or drafts that are being revised frequently. These documents must have "Draft" or "Working Papers" on the front cover until final.

They must also include classification markings for the highest potential classification level, category and caveat of the information you believe is in the document.

Regardless of type, a document must be reviewed and finalized no later than 180 days after creation, or in the case of working papers/living documents, 180 days after the last revision; additionally, the originator of the document must be listed.

Remember, if you are not certain that what you have created has already been determined to be unclassified, you must get it reviewed by a DC before putting it in unclassified venue.

WHO IS AUTHORIZED TO CONDUCT CLASSIFICATION REVIEWS?

As required by DOE Order 475.2B, *Identifying Classified Information*, only Derivative Classifiers (DCs) may conduct a review of information for classification. If you are creating information in areas mentioned in this brochure (documents, emails, etc.,) be sure to get a DC review.

DCs must:

- ✓ Be trained in derivative classification.
- ✓ Be authorized in specific subject areas.
- ✓ Have access to current classification guidance for subject areas of authority.
- ✓ Be appointed by the local Classification Officer.

Sandia National Laboratories Classification Department Locations

New Mexico
P. O. Box 5800, MS 0175
Albuquerque, NM 87185-0175

California
P.O. Box 969, Mail Stop 9021
Livermore, CA 94551-0969

E-mail: classificationdept@sandia.gov
Classification Helpline: 505-844-5574

Security Questions?
Call **321**
Security Connection
505-845-1321
security@sandia.gov
THINK. ASSESS. PROTECT

Understanding Classification

Per Laboratory Policy, all information in a potentially classified subject area must be reviewed by a Derivative Classifier (DC) before it is used in unclassified venue.

At Sandia, *Classification* is the act or process by which the sensitivity of documents or material is determined, based on established classification guidance or other legal statute.

As Members of the Workforce handling classified information, your primary responsibility is to ensure that documents or materials you originate, modify, or possess in a classified subject area are reviewed by a Derivative Classifier.

This brochure will help you determine if your information is in a Classified Subject Area, and provide details regarding the requirement for reviews.

SAND2019-14822 TR

Security+ YOU
Think. Assess. Protect.

WHAT IS A CLASSIFIED SUBJECT AREA?

A classified subject area is a subject area for which a classification guide has been issued (e.g. nuclear assembly systems, safeguards and security, Strategic Petroleum Reserve). The guides indicate what specific information in a given subject area is classified. At Sandia, common classified subject areas include:

Areas related to weapons:

- Nuclear Weapon (NW) production and military use
- NW Use Control
- NW Safing, Arming, Fuzing and Firing
- NW Design of Nuclear Components
- NW Materials
- NW Vulnerability and Hardening
- NW Boosting and Transfer Systems
- NW Detonation Systems
- NW Initiators (Neutron Generators)
- NW Weapon Outputs
- NW Weapon Science
- Inertial Confinement Fusion
- Nuclear Explosion Monitoring
- Improvised Nuclear Devices
- Subcritical Experiments
- Fissile Material Disposition
- Chemical/Biological Defense Information
- Radiological Emergency Response
- Non-Nuclear Testing
- Nonproliferation of Weapon Information

Areas related to security:

- Intelligence/Counterintelligence
- Transportation Safeguards System
- Safeguards and Security

Weapons Programs:

B61-3/4/10 • B61-7 • B61-11 • B61-12 • B83-1
W76-0,1 • W78 • W80-1,4 • W84 • W87 • W88

CLASSIFICATION LEVELS AND CATEGORIES

Only an Original Classifier can make a determination that *Information* is classified. Those determinations are captured in classification guidance. Sandia DCs are only authorized to apply that guidance when making classification determinations for *documents* and *material*.

Classification guidance uses three levels (**Top Secret, Secret, and Confidential**), according to the damage that would be caused if released, and four categories to describe the type of information; those categories are:

Restricted Data (RD), controlled by the AEA regarding information concerning design and manufacture of nuclear weapons, fissile materials, naval nuclear propulsion, and space power systems.

Formerly Restricted Data (FRD), also controlled by the AEA, relates primarily to the military utilization of nuclear weapons. Examples of FRD include nuclear weapon stockpile quantities, nuclear weapon delivery, nuclear weapon yields, and past and present weapon storage locations.

Transclassified Foreign Nuclear Information (TFNI), controlled by both the AEA and E.O. 13526, regarding specific intelligence information concerning certain foreign nuclear programs that is comparable to US RD or design-related utilization information.

National Security Information (NSI), controlled by E.O. 13526, is information concerning all other kinds of classified information. Examples of NSI include safeguarding of nuclear materials or facilities, vulnerabilities or capabilities of systems/ installations, nonproliferation studies, foreign government information, and intelligence and counterintelligence information.

WHAT ARE SOME "RED-FLAG" INDICATORS?

In addition to the known classified subject areas, there are "Red Flag" indicators that may help you determine if your information warrants additional sensitivity considerations.

If your documents contain any of these 'indicators', be aware that there may be classification considerations that warrant DC review:

- Neutron generator (NG) design and performance details (NG timing, etc.)
- Timer/driver design and performance details
- Firing set design and performance details
- Gas transfer system design and performance details
- Fuzing/Height of Burst (HOB) design and performance details
- Weapon use control features
- Data and photos from lab or flight tests
- Critical weapon association concerns (including part and MC numbers)
- Unique materials used in weapon application
- Unfavorable component or weapon statement
- Weapon performance or quality details
- Production quantities/issues or concerns
- Shipment schedules (dates or times)
- Weapon quantities/locations
- Weapon or component cutaways/models or drawings
- Assembly models or drawings
- Radiation hardness levels
- Flight trajectories and profiles
- Weapon retirement dates
- Nicknames and code words
- Weapon outputs and testing
- Configuration of components within the weapon

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

CALL SECURITY CONNECTION at 505-845-1321

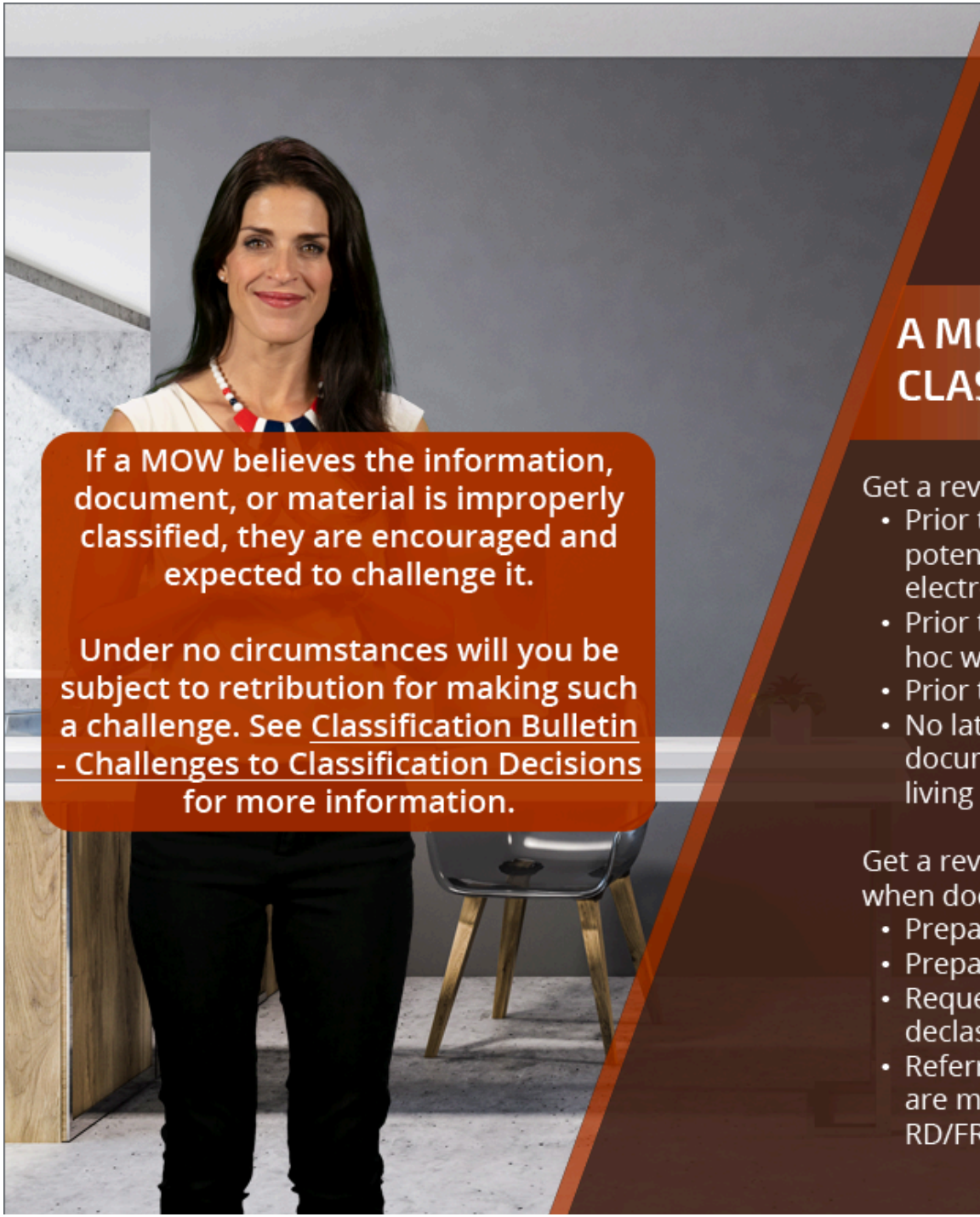
When requesting a DC review, do not transmit the information on an unclassified network. Start on the SCN, then Downshift.

A MESSAGE FROM THE CLASSIFICATION OFFICE

A **Derivative Classifier (DC)** is an individual authorized to determine that a document, equipment, or material is unclassified or classified based on classification guidance or source documents, as allowed by his or her description of authority.

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

You can locate a DC or DD through the Jupiter application (Jupiter.sandia.gov).



If a MOW believes the information, document, or material is improperly classified, they are encouraged and expected to challenge it.

Under no circumstances will you be subject to retribution for making such a challenge. See Classification Bulletin - Challenges to Classification Decisions for more information.

A MESSAGE FROM THE CLASSIFICATION OFFICE

Get a review by an appropriate DC for classification:

- Prior to finalizing a working paper or document in a potentially classified area (whether hard copy or electronic).
- Prior to releasing it outside of the activity (e.g., ad hoc working group or program).
- Prior to filing it permanently.
- No later than 180 days after creation of the document, or 180 days after the last revision (if a living document).

Get a review by an appropriate DD for declassification when documents 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 marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities.

Classification Office Did You Know??

Security+ YOU
Think. Assess. Protect.

July 23, 2020

Challenges to Classification Decisions

Members of the Workforce are encouraged and expected to challenge the classification of information, documents, or material that they believe may be improperly classified. Under no circumstances shall a challenger be subject to retribution or repercussions for making a classification challenge.

Do you have a document (or material) that you have reason to believe has been mis-classified? See the below:

Information, Documents, or Materials Improperly Classified

Members of the Workforce identifying documents or materials believed to be improperly classified are encouraged and expected to challenge the classification by:

- Submitting the document/material for review by a Derivative Classifier (DC) who is knowledgeable in the subject area for confirmation.
- If confirmed, the DC can upgrade the document or material as appropriate, using the process in SS002, *Identifying Classified Information*. For a downgrade, the DC must contact the Classification Office to initiate the downgrade process.
- If a DC is not available or you disagree with the DC's determination, you may initiate a challenge following the Sandia Protocol. Information regarding the challenge process is provided below.

Appeal a Classification Decision

Members of the Workforce who disagree with a DC decision are encouraged and expected to challenge the classification decision by working through the Sandia Protocol, which are shown here (at the end of this document). Also, Members of the Workforce are encouraged to:

- Contact the Classification Officer to discuss the issues if you cannot resolve the issue with the DC. Many times, the Classification Officers can help resolve the questions around the DC's decision.
  - The Classification Officer will be Sandia's final arbiter.
- If you disagree with the results of the Classification Officer consultation, the Classification Officer will assist you in raising the concern to the DOE Director, Office of Classification.

Note:

- Members of the Workforce can, at any time, submit a classification challenge directly to the DOE Director, Office of Classification without following the protocol.

Challenges to Topics in Classification Guides

Members of the Workforce who believe the ***information itself*** as shown in a classification guide is improperly classified, and should be a different level, category or unclassified sensitivity (e.g., UCNI or OUO) must first (using the Sandia Protocol):

- Discuss the issue with a knowledgeable DC subject matter expert. Topics in a classification guide have been determined to be classified at certain levels and categories by an Original Classifier at DOE (or other government agencies, depending on the guide).
- If the DC agrees or you believe there is sufficient reason for discussion, contact the Classification Officer to begin a pre-challenge process discussion.

Classification Offices

The Sandia Protocol:

The steps in the Sandia Protocol for conducting a challenge to a classification decision are:

- Discuss the issue with a knowledgeable DC.
- If the DC agrees that there is an issue, the DC will present it to the Classification Officer.
  - If you disagree with a DC review decision and you cannot resolve it with a discussion with your manager and/or the DC, and you believe there is sufficient grounds, you are encouraged to contact the Classification Officer to resolve the challenge.
    - The Classification Officer will be the final arbiter for local DC review decisions.
- If the Classification Officer agrees that there is an issue in classification guidance that cannot be resolved locally, a Formal Challenge will be submitted to HQ DOE.

Note:
The Member of the Workforce can go directly to the DOE Office of Classification at any time in this process. See SS002, *Identifying Classified Information*, for more information.

Resources:

SS002, *Identifying Classified Information*

S&S-MAN-051, *The DC Handbook*

For questions or assistance with this topic:

Classification Department Helpline: 505-844-5574
Classification Department Entity Account: classificationdept@sandia.gov
The above information can also be used to leave messages for the SNL/CA Classification Office during non-office hours.

SNL/CA Classification Department: 925-294-2202
SNL/CA Classification Department website:
https://wp.sandia.gov/div8kops/information-protection/classification-office/

General Security questions: Security Connection, (505) 845-1321 (or 321 from any Sandia landline)
Website: https://security.sandia.gov/

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

A MESSAGE FROM THE CLASSIFICATION OFFICE

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 individual must not comment on them.

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.

COURSE MODULES

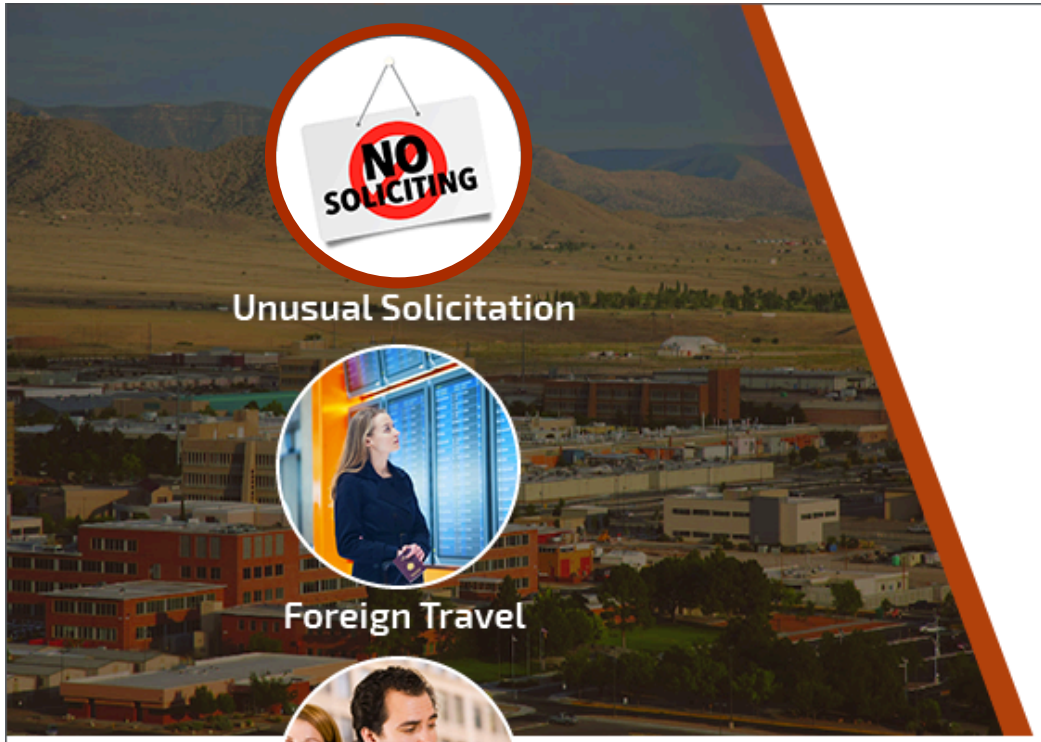
- IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- IMPROPER STORAGE OF CLASSIFIED
- IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE

COUNTERINTELLIGENCE UPDATE

To succeed in our mission to detect, deter and mitigate threats to Sandia National Laboratories, the Office of Counterintelligence (CI) must earn and retain the trust and cooperation of the Sandia community that we serve.

Counterintelligence depends on you to review the following CI updates and read the resource documents provided in this section to understand the importance of your responsibilities as it relates to our mission success.

- CI Topics Newsletter
- Spy of the Month
- CI-Help@sandia.gov
- CA & NM: 505-284-3878



Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

COUNTERINTELLIGENCE UPDATE

Unusual Solicitation

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

This applies equally to sensitive foreign nationals, non-sensitive foreign nationals, as well as unauthorized U.S. citizens. Such attempts can be in the form of pointed 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 by a foreign intelligence service or international terrorist group.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

COUNTERINTELLIGENCE UPDATE

Foreign Travel

Travel to sensitive countries must be reported (regardless of clearance level and/or citizenship). Foreign intelligence services perceive your DOE clearance as actual and/or potential access to information of value to foreign governments. You are vulnerable to the tactics of a foreign intelligence service while in their country.

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

COUNTERINTELLIGENCE UPDATE

Insider Threat

Report to Counterintelligence, any individual who:

- Seeks unauthorized access to classified information, matter or special nuclear material without a Need To Know
- Appears to be living well beyond their means
- Has unreported foreign contacts 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 and balance our responsibility to protect Sandia and national security.

Foreign intelligence services seek the cooperation of an authorized insider to betray the trust of his or her colleagues. This is also the case for international terrorist groups who would target well defended, sensitive facilities like Sandia.

Unusual Solicitation

Foreign Travel

Insider Threat

Substantive Contact/Relationship

COUNTERINTELLIGENCE UPDATE

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, associations that involve meeting and sharing Sandia information or ongoing contact that is solely through electronic communication (e.g., email, telephone, or social media networking sites).

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

CI TOPICS

Sponsored by The SNL Office of Counterintelligence Newsletter #73 April 3, 2020

Pentagon linguist faces espionage charges after allegedly sharing secrets with Hezbollah

A linguist who worked for the Pentagon is facing espionage charges for allegedly sharing highly sensitive classified information with a foreign national who has apparent connections to the terror group Hezbollah, the Justice Department announced Wednesday.

The information allegedly shared by Mariam Thompson, 61, included details regarding secret human assets working for the U.S. and military personnel, prosecutors said.

"If true, this conduct is a disgrace, especially for someone serving as a contractor with the United States military. This betrayal of country and colleagues will be punished," Assistant Attorney General for National Security John Demers said in a statement.

Source: Getty Images

For the full story, click the link:

Pentagon linguist faces espionage charges after allegedly sharing secrets with Hezbollah

UK says Russia's GRU behind massive Georgia cyber-attack

A huge cyber-attack which knocked out more than 2,000 websites in the country of Georgia last year was carried out by Russia, according to Georgia, the UK and the US.

The UK government says that the GRU (Russian military intelligence) was behind the "attempt to undermine Georgia's sovereignty".

Foreign Secretary Dominic Raab described it as "totally unacceptable".

Russia's Foreign Ministry denied any involvement, the RIA news agency said.

The UK's National Cyber Security Centre (NCSC) found that the GRU was "almost certainly" behind the attacks, which affected pages including Georgia's presidential website and the country's national TV broadcaster. It said the attack was the first significant example of GRU cyber-attacks since 2017.

For the full story, click the link:

UK says Russia's GRU behind massive Georgia cyber-attack

CI Topics is a monthly publication that seeks to raise CI awareness with intelligence related topics that are relevant to Sandia or DOE.

This publication incorporates open source news articles from various sources. Viewpoints contained in this document are not necessarily shared by the Office of Counterintelligence.

Our goal is to provide timely, useful and relevant information on intelligence related topics and events happening in the world.

Inside this issue:

Mexican National Arrested In South Florida For Being Agent Of Russia	*2*
Australia spy chief warns of "unprecedented" foreign espionage threat	*2*
Awareness Corner	*2*
Interesting Reads	*3*
Movies to Watch	*3*

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND No. SAND2020–3870 O

Mexican National Arrested In South Florida For Being Agent Of Russia

A Mexican national has been arrested in South Florida for being an agent of a foreign power.

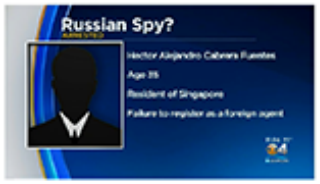
The U.S. Department of Justice said Hector Alejandro Cabrera Fuentes, who is a resident of Singapore, was working on behalf of Russia.

According to court documents, a Russian government official recruited Fuentes in 2019, directing him to rent a specific property in Miami-Dade.

After several trips to Moscow, the DOJ said Fuentes met with his Russian handler in February of 2020, where he was ordered to scout a U.S. government source's vehicle.

Fuentes was reportedly told to "locate the car, obtain the source's vehicle license plate number, and note the physical location of the source's vehicle."

Court documents show Fuentes, who was to meet with the Russian official again in April or May, traveled to Miami on Feb. 13 from Mexico City.



For the full story, click the link:

Mexican National Arrested In South Florida For Being Agent Of Russia

Australia spy chief warns of "unprecedented" foreign espionage threat

Australia is under an "unprecedented" threat of foreign espionage and interference, one of the country's most senior spy chiefs said in a rare speech, citing the case of a "sleeper agent" who spent years building business links.

Australian Security Intelligence Organisation (ASIO) Director-General Mike Burgess said several nations were working hard to influence lawmakers, government officials, media figures, business leaders and academics.

"It is higher now, than it was at the height of the Cold War."

"The level of threat we face from foreign espionage and interference activities is currently unprecedented," Burgess said at ASIO headquarters in Canberra on Monday evening as he unveiled the agency's annual threat assessment.

For the full story, click the link:

Australia spy chief warns of "unprecedented" foreign espionage threat

CI Awareness Corner:

James Olson Presentation: To Catch a Spy: The Art of Counterintelligence

In January, Sandia had the pleasure of hosting James Olson, Professor at the George Bush School of Government and Public Service at Texas A&M University, former Chief of Counterintelligence at the CIA and author of *The Moral Dilemmas of Spying* and *To Catch a Spy: The Art of Counterintelligence*, to Sandia.

Professor Olson discussed his book *To Catch a Spy: The Art of Counterintelligence*. Using his experiences gained during his career in the CIA he explained what the art of counterintelligence is and lessons he learned along the way.

Professor Olsen previously visited Sandia and presented on his book *The Moral Dilemmas of Spying*.

You can check out both of these recordings and others on the Resources page on the CI website.

On the website you can find information regarding reporting requirements and other related topics.

If you have any questions, please do not hesitate to contact CI at 505-284-3878 or

Phone: 505-284-3878
E-mail: cihelp@sandia.gov

Office of Counterintelligence

Visit our web page for more information.

Interesting Reads

Omand, David and Mark Phythian. Principled Spying: The Ethics of Secret Intelligence. 2018.

Intelligence agencies provide critical information to national security and foreign policy decision makers, but spying also poses inherent dilemmas for liberty, privacy, human rights, and diplomacy. Principled Spying explores how to strike a balance between necessary intelligence activities and protecting democratic values by developing a new framework of ethics.

David Omand and Mark Phythian structure this book as an engaging debate between a former national security practitioner and an intelligence scholar. Rather than simply presenting their positions, throughout the book they pose key questions to each other and to the reader and offer contrasting perspectives to stimulate further discussion. The authors disagree on some key questions, but in the course of their debate they demonstrate that it is possible to find a balance between liberty and security. (amazon.com)

Ritter, Nikolaus. Cover Name: Dr. Rantzau. 2019.

Cover Name: Dr. Rantzau is a gripping diary-like personal account *of espionage during the Second World War and is one of very few historic memoirs written by an ex-Abwehr* officer. Detailed is how *Colonel Nikolaus Ritter, following a brief World War I career and over ten years as a businessman in America, returned to Germany in spring of 1935 and became Chief of Air Intelligence in the Abwehr.*

Katharine Ritter Wallace, the daughter of Col. Ritter, presents the first English translation of the German World War II memoir. With a combination of collected documents, correspondences, personal notes, communications with peers, and from memory, this captivating account by an espionage agent reveals an insider's glimpse of the German intelligence service and of a handler's expansive and diverse agent network. (amazon.com)

Movies to Watch

Shadow Wolves. 2019.

A rogue NSA agent joins an elite group of Native American trackers who call themselves the Shadow Wolves as they engage in missions to protect justice in America and abroad. (imdb.com)

SAND No. SAND2020-3870 O

SAND2020-5358 O

Spy of the Month

Turab Lookman

May 2020

This month we are going to switch things up. This case is not a spy story. This month we are going to look at the case of Turab Lookman. Lookman was a physicist at Los Alamos National Laboratory until 2019. He was charged in 2019 with making false statements regarding his foreign ties. Not everyone who has the ability to cause damage to US interests is a spy. This is a reminder for all to be aware of their foreign interactions and ensure adherence to reporting requirements.

Turab Lookman was born in India in 1952. At the age of 13 he moved to the United Kingdom where he stayed through his college years. He received his PhD in theoretical physics from Kings College, London. After Lookman completed his studies he moved to Canada and then to the US. At the time of his arrest he was living in Santa Fe, NM.

In 1999 Lookman was hired by LANL as a physicist and obtained is US citizenship in 2008. Lookman's expertise was in computational physics of material, complex fluids and nonlinear dynamics. During his time at LANL, Lookman became very well known for his work worldwide and recognized by the laboratory. In 2009, LANL awarded Lookman the Fellows Prize for Outstanding research and in 2016 he received the Distinguished Postdoctoral Mentor Award. He was also awarded one of the laboratory's highest scientific honors, when he was named laboratory fellow in 2017. In addition, he had co-authored two books and more than 250 publications in his field.

The indictment alleged that Lookman had made false statements on his employment questionnaire about participating in Thousand Talents Program for personal gain, during a debriefing with a LANL counterintelligence officer, and to an investigator from the National Background Investigation Bureau/Office of Personnel Management during a clearance investigation.

Lookman was arrested on May 23, 2019 by the FBI after a grand jury indictment. He was charged with three counts of making false statements regarding his ties to China's Thousand

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

Talents Program. The Thousand Talents Program was developed by the central government of China in 2008. The program was created in order to recruit international experts in scientific research, innovation, and entrepreneurship. The Thousand Talents Program has been using incentives, such as salaries and professional support to build relationships with scientists for China to have better access to foreign technology and intellectual property. The purpose is to achieve China's strategic goals as determined by the State Council which in turn is controlled by the communist party.

Sometime before November 2017, Lookman was reportedly asked by a foreign national to apply to the Thousand Talents Program. He applied and was accepted into the program sometime before June 2018.

In May 2019, Lookman plead not guilty to federal charges of lying about his involvement with funding from the Chinese government. He repeatedly denied his involvement with the Thousand Talents Program even though he initially admitted to joining for "personal compensation. He was released on $50,000 bail. The prosecutor stated that if Lookman fled it would be a "national security disaster."

In January 2019, the Department of Energy issued a memo announcing its intent to identify new guidelines and restrictions on personnel from participating in foreign government talent recruitment programs. The memo addressed the value of DOE collaborations with foreign entities, it stated that the intent of the new policy is to "limit real or potential exploitation" of the scientific and research community in the U.S. Just a few weeks after the arrest of Lookman, the Department of Energy released the new DOE order which contains the requirements that govern participating in foreign government talent recruitment programs.

On January 24, 2020 the FBI reported that Lookman had plead guilty in a federal court in Albuquerque. He plead guilty to making false statements about his involvement in the Thousand Talents Program. Lookman admitted to lying to a counterintelligence official from LANL in 2018. He was not in custody at the time and is awaiting sentencing. Lookman could possibly face up to five years in prison and a $250,000 fine.

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

Resources:

https://www.justice.gov/usao-nm/pr/former-los-alamos-national-laboratory-scientist-charged-making-false-official-statements

https://www.justice.gov/usao-nm/pr/former-los-alamos-national-laboratory-scientist-charged-making-false-official-statements

https://www.apnews.com/ae09d224679546ed8e23e89b820b1eeb

https://www.scmp.com/news/china/diplomacy/article/3012095/us-lab-scientist-faces-charge-lying-about-china-contact

https://www.abqjournal.com/1320008/former-lanl-scientist-indicted-for-making-false-statements.html

https://en.wikipedia.org/wiki/Thousand_Talents_Plan

https://www.energy.gov/management/downloads/pf-2019-25-doe-order-4861-department-energy-foreign-government-talent

https://physicstoday.scitation.org/do/10.1063/PT.6.2.20190620a/full/

https://www.justice.gov/usao-nm/pr/former-scientist-los-alamos-national-laboratory-pleads-guilty-federal-court-making-false

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

COURSE MODULES

- IMPROPER PROTECTION OF UNCLASSIFIED CONTROLLED INFORMATION (UCI)
- IMPROPER STORAGE OF CLASSIFIED
- IMPROPERLY SECURED INFORMATION SYSTEM
- UNAUTHORIZED NETWORK-BASED TRANSMISSION
- COUNTERINTELLIGENCE UPDATE
- SAFEGUARDS & SECURITY UPDATE

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 yourself at work and at home.

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

- Contact Tracing security message
- Customs & Border Patrol Seize Counterfeit COVID-19 Test Kits
- ACD 470.6 Security Message
- Protecting Information While Working Remotely security message

SAFEGUARDS & SECURITY UPDATE

No Vouching | Suspect/Counterfeit Items | Mobile Devices at Sandia | Security at Home

NO VOUCHING

With the exception of vehicle gates, vouching is NOT allowed at gates, turnstiles, doors equipped with automated access controls (badge readers).

Sandia's change to the vouching policy helps achieve the following goals:

- Personnel Safety: Responds to potential COVID threats by: 1) providing traceability of personnel to identify people potentially exposed and areas to be sanitized; and, 2) providing positive identification of those entering while complying with face mask requirements
- Security: The no-vouching policy demonstrates due diligence as part of Sandia's commitment to protect sensitive and classified information.

For questions or to report

321 from a Sandia landline | 505-845-1321 from any phone

security@sandia.gov | Chat: securitychat.sandia.gov NEW

SAFEGUARDS & SECURITY UPDATE

No Vouching | Suspect/Counterfeit Items | Mobile Devices at Sandia | Security at Home

SUSPECT/COUNTERFEIT ITEMS

Teleworking from home increases your risk because you are likely to buy items to make working at home more comfortable (i.e., adapters, computing equipment, electrical products). Purchase of these items increase the risk of receiving suspect/counterfeit, or fraudulent items (S/CI-FI's).

S/CI-FIs are often substandard, do not meet basic safety requirements (although they may state they do), and may not work as expected (even if it appears to). A S/CI-FI iPhone may appear to work as expected until it suddenly overheats and catches on fire. This can be true of any S/CI-FI lithium-ion battery or charger, which can be extremely unreliable or unstable.

There are also significant security concerns with S/CI-FIs as some are provided with malicious software, applications, or hardware that would not be normally included with their genuine counterpart.

Email sqasci@sandia.gov or visit counterfeit.sandia.gov (site available on SRN and SCN)

SAFEGUARDS & SECURITY UPDATE

No Vouching | Suspect/Counterfeit Items | Mobile Devices at Sandia | Security at Home

Mobile Devices at Sandia

Mobile devices (including Sandia, government, or personally owned) such as cell phones, tablets, E-readers, smart watches, fitness trackers, etc., are not permitted in Secure Space across Sandia to reduce the compromise of sensitive and classified information.

- ANY mobile devices brought into Secure Space must be reported to SIMP [self-report tool: SIMP.sandia.gov] immediately.
- Mobile devices can only be stored in designated approved storage areas.
- Mobile devices may not enter, or be carried through, Secure Space to reach approved storage.
- No classified discussions are allowed outside of Secure Space.

For questions or to report

321 from a Sandia landline | 505-845-1321 from any phone

security@sandia.gov | Chat: securitychat.sandia.gov NEW

SAFEGUARDS & SECURITY UPDATE

No Vouching | Suspect/Counterfeit Items | Mobile Devices at Sandia | Security at Home

SECURITY AT HOME

When working from home, you must take steps to ensure Sandia information, including unclassified, is protected appropriately.

- Home is not an approved space for classified. Be careful with what you work on, discuss, or bring home.
- Do not allow unauthorized individuals, including family, to access Sandia computers or resources.
- Secure your computer or session every time (log out, lock, power down, etc.) to ensure information is only accessible by those with NTK.
- Do not print Sandia information from personal printers. Work digitally. If working with printed UCI, store it in a locked cabinet, desk, or an alternative that equivalently controls access.
- Distractions and changes in your routine can lead to security mistakes.

For questions or to report

321 from a Sandia landline | 505-845-1321 from any phone

security@sandia.gov | Chat: securitychat.sandia.gov NEW

Security Message

#1 OPERATIONAL PRIORITY: SAFETY & SECURITY

Security+ YOU
Think. Assess. Protect.

April 2020

Contact Tracing (COVID-19)

Following each confirmed case of COVID-19 at a Sandia site, Sandia coordinates with state and federal health officials to retrace the individual's steps to identify all locations visited. Everyone with confirmed contact with the individual who tested positive is contacted by the Sandia Medical Clinic within 24 hours. This process—known as ***contact tracing***—is important in mitigating further spread.

To improve Sandia's *contact tracing* ability, two important security changes are being implemented:

Badge reader activation

Technical Security is activating access controls to all equipped buildings for 24/7 operations. This means that badge readers which are normally active only during evening and weekend hours will now be active 24/7. Since a PIN is not required, no direct, physical contact with the readers is necessary. Swipe or present your badge to gain access.

Change to vouching policy

Effective April 27, Members of the Workforce must not 'vouch' others into pedestrian access points (gates, turnstiles, etc.). Each individual should swipe or present his/her badge at each access point when entering buildings and other security areas. Process SS008.1 *Site Access* will reflect this change on April 27.

Vouching passengers in the same vehicle will still be permitted at vehicle gates.

Together, these measures will enhance Sandia's ability to identify any individual who may have come into contact with someone who has tested positive for COVID-19.

For questions or to report a security concern:

Security Connection

321 from Sandia phone
505-845-1321 from any phone
security@sandia.gov

Violations of Laboratory Policy should always be reported.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-7253 O

NNSA ENERGY

CBP Officers Seize Fake COVID-19 Test Kits at LAX

Release Date: March 14, 2020

Suspected Counterfeit Test Kits Mislabeled as "Purified Water Vials"

LOS ANGELES - U.S. Customs and Border Protection (CBP) officers assigned to Los Angeles International Airport (LAX), International Mail Facility (IMF), intercepted a package containing suspected counterfeit COVID-19 test kits arriving from the United Kingdom.

On March 12, 2020, CBP officers discovered six plastic bags containing various vials, while conducting an enforcement examination of a parcel manifested as "Purified Water Vials" with a declared value of $196.81. A complete examination of the shipment, led to the finding of vials filled with a white liquid and labeled "Corona Virus 2019nconv (COVID-19)" and "Virus1 Test Kit". The shipment was turned over to the U.S. Food and Drug Administration (FDA) for analysis.

"Protecting the health and safety of the American people is a top priority for CBP," said Carlos C. Martel, CBP Director of Field Operations in Los Angeles. "This significant interception, at a time when the U.S. is in the midst of a National Emergency, demonstrates our CBP officers' vigilance and commitment to ensure dangerous goods are intercepted and not a threat to our communities and our people."

Authorized diagnostic testing for COVID-19 is conducted in verified state and local public health laboratories across the United States. The American public should be aware of bogus home testing kits for sale either online or in informal direct to consumer settings.

"CBP commits substantial resources to detect, intercept and seize illicit goods arriving in the air package environment," said LaFonda Sutton-Burke, CBP Port Director at LAX. "Smugglers are constantly attempting to take advantage of consumers by disguising their illicit goods as legitimate shipments."

U.S. Customs and Border Protection is the unified border agency within the Department of Homeland Security charged with the management, control and protection of our nation's borders at and between official ports of entry. CBP is charged with securing the borders of the United States while enforcing hundreds of laws and facilitating lawful trade and travel.

Last modified: March 14, 2020

Security Message

#1 OPERATIONAL PRIORITY: SAFETY & SECURITY

November 2020

Security+ YOU

Think. Assess. Protect.

Questions about the coming Mobile Device requirement?

Q: How will I know where Secure Space is?

A: Installation of new Secure Space building signs is almost complete, so chances are good that you can see them around buildings in the limited areas. This should give you a good idea of where Secure Space begins. Keep in mind that most building space within Sandia limited areas—with the exception of vestibules or entry areas approved for internal storage—will become Secure Space.

Q: I know that ALL mobile devices will be prohibited in Secure Space after Dec. 2. Does that include my Sandia iPad? My Sandia laptop?

A: Smart phones, smart watches, iPads, and E-readers are all examples of mobile devices that will be prohibited in Secure Space. However, Sandia computing devices that use a Windows or macOS operating system (laptops including Ultrabook, Surface, Mac) are NOT impacted by the requirement and are therefore permitted.

Q: What about one-way pagers?

A: One-way pagers don't meet the definition of a mobile device, so they are permitted in Secure Space. You can find the full definition of mobile device in Policy IT004 Manage Controlled Electronic Devices and Media Policy.

More questions?

- Check out the FAQ at PEDs.sandia.gov or talk to your Deployed Security Professional.
- Join a **Mobile Device Q&A Cafe** 2-3 p.m. MST Thursdays in November and December to hear the latest updates from Physical Security and Facilities regarding the implementation at Sandia. Sessions will begin with a brief overview presentation of status and updates, followed by Q&A.

Advanced Change Directive (ACD) 470.6 applies to ALL mobile devices

PEDs.sandia.gov

Mobile Device Q&A Cafes

Currently scheduled dates:
Nov. 19, Dec. 3, Dec. 10, Dec. 17

Add the Nov. 19 café to your calendar

Visit Mobile Device Q&A Café for meeting links

Key Dates

Dec. 2, 2020—Secure Space activated; grace period begins

Jan. 31, 2021—Grace period ends; Sandia is in full compliance with requirement

Questions? Security Connection
security@sandia.gov
321 from a Sandia landline
505-845-1321 from any phone

All archived Security Messages are available on the S&S WordPress site.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-13429 O

Security Message

#1 OPERATIONAL PRIORITY: SAFETY & SECURITY

Security+ YOU
Think. Assess. Protect.

March 2020

Protecting information when working remotely

In response to the Coronavirus, many members of the workforce will be working from home. It is important that you take steps to ensure that Sandia information is protected appropriately.

Getting set up

- Follow the Telecommuting Guidance on how to access Sandia's systems. For information about using peripherals with Sandia computers, see the CIO Home Desktop Guidance. Questions to cio@sandia.gov.
- Talk with your manager if you need equipment or other resources to work from home.
- Pay close attention to communications from CIO/IT, Cyber and Security for updates or additional guidance as the situation evolves.

Working with sensitive information

Unclassified Controlled Information (UCI) including Official Use Only (OUO) / Personally Identifiable Information (PII)

- Ensure the information is only accessible to those who have need to know (NTK).
- When not working on it, store UCI in a locked cabinet or desk, or an alternative that equivalently controls access. (Note: Work digitally; avoid printing or working from hard copies.)
- If UCI cannot be disposed of offsite in accordance with requirements in Policy IT012, return it to SNL.

Do not take classified home.

Resources

- IT003 Protect Sandia's Information Technology Resources Policy
- IT017 Official Use Only Information Policy
- IT012 Unclassified Controlled Information Policy
- IT023 Personally Identifiable Information Policy
- SS002 Identifying Classified Information Policy
- HR012 Time Charging Policy
- Family Guide to Security at SNL

For questions or to report a security concern

Security Connection | security@sandia.gov
321 from Sandia phone
505-845-1321 from any phone

Other tips for working from home:

- **If possible, establish a 'work station' where information and resources can be protected.**
- **If you are doing work (such as Webmail) on a personal or shared computer, always log off when you are finished. Never leave a session open where others might have access.**
- **Assess your own risks. You might want to create your own 'site security plan.' Keep in mind that distractions and changes in routine can lead to mistakes in handling information.**
- **Do not allow other individuals, including children, to use Sandia computers or resources.**
- **If appropriate, share your work schedule with family members, as well as any concerns you may have, and solicit their support. It may be helpful to discuss your plans and answer questions they may have.**

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-7254 O

NNSA ENERGY

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

Thank you!

That wraps up the Annual Security Refresher Briefing!

SEC100 Completion Record: 2020/2021

By completing this form, you acknowledge that you have read the 2020/2021 Annual Security Refresher briefing and understand your security responsibilities.

Complete the information below and email to securityed@sandia.gov or fax to 505-844-7802 to receive credit in TEDS.

If you would like confirmation of completion, provide your email address below:

Print full name:	
SNL Org# or Company Name:	
Signature:	Date:
Email address:	

For questions or to report

321 from a Sandia landline | 505-845-1321 from any phone

security@sandia.gov | Chat: securitychat.sandia.gov

NEW

SEC100 Feedback Form

You feedback is important to us.

Please complete this evaluation form and email to securityed@sandia.gov or fax to 505-844-7802 to receive credit in TEDS.

Rate the following on a scale of 1 to 5, with 1=poor and 5=excellent.

The ease of use for this learning.	1	2	3	4	5
The organization of the information presented.	1	2	3	4	5
The usefulness of the information presented.	1	2	3	4	5
Your level of knowledge to this topic BEFORE using this tool.	1	2	3	4	5
Your level of knowledge to this topic AFTER using this tool.	1	2	3	4	5

Enter feedback below.

What was the most valuable about this briefing?

What information needs to be corrected, inserted, removed or updated?

What could be done to improve or enhance this briefing?

For questions or to report
321 from a Sandia landline
505-845-1321 from any phone
security@sandia.gov | Chat: securitychat.sandia.gov