



Sandia  
National  
Laboratories



*SEC 150*

# COMPREHENSIVE SECURITY BRIEFING



*Security+*  
Think. Assess. Protect. **YOU**



U.S. DEPARTMENT OF  
**ENERGY**



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.

SAND2023-005770 06.20.2023 v.12

## Introduction

Welcome to the **SEC150: Comprehensive Security Briefing** pdf booklet!

SEC150 is a **DOE-required** briefing required for all clearance holders and applicants that must be completed prior to being granted *access* to classified information, matter or area. This booklet meets minimum DOE requirements for access, though Sandia members of the workforce are **still required to complete the instructor-led briefing**.

## Course Content

- Working At This Laboratory
- Control Site Access
- Control Security Area Access
- Control Information Access
- Security Incidents
- Counterintelligence
- Resource Documents

## Course Objective

**At the conclusion of this briefing, you will be familiar with the following topics:**

- Basic classification security policies and principles
- Classified information or matter protection elements
- Personnel Security elements
- Counterintelligence Threats and requirements
- Individual responsibilities, to include what and when to report subjects impacting your ability to maintain a security clearance
- Legal aspects for security clearance holders

**“We have an incredible privilege to work on the nation’s hardest national security problems; with that comes an awesome responsibility to protect our nation’s secrets.”**

**We look forward to working with you at Sandia National Laboratories. We hope you’re as excited as we are about what we do.**

## Who We Are

### Sandia is known for:

- Clean rooms
- Sandia foam
- Hybrid technology
- Pulsed power
- Biofuels
- Nanotechnology

### Sandia consists of:

- Sites in NM, CA, NV, HI, D.C.
- 7 remote sites
- 17 leased sites
- 900+ buildings
- 6,026,145 building gross ft<sup>2</sup>
- 20,510 acres of land



**Other countries and companies are very interested in knowing what we know.**

### 42 FFRDCs

Federally Funded Research and Development Centers

### 26 R&D

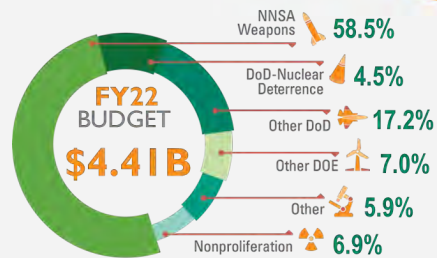
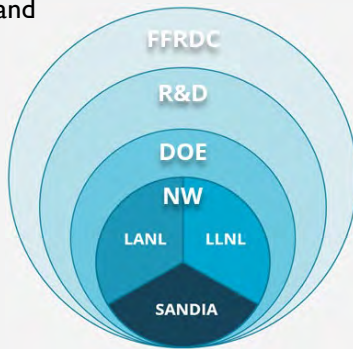
Research and development labs

### 16 DOE

DOE-sponsored FFRDCs

### 3 NW

Nuclear weapons laboratories



## Protecting What is Ours

### THINK

Recognize and acknowledge that you are at risk.


### ASSESS

Evaluate your routines and your environment. Where are you vulnerable?


### PROTECT

Adopt security measures and work controls and make security a part of everything you do.

**You must be diligent both on and off site.**



You leave for work and can't recall if you closed the garage... so you go back and check. Yet we have situations where people suspected they left a safe open but went home anyway.



You keep your wallet in a safe place. But we find passwords taped to the back of monitors and under keyboards.



## CONTROL SITE ACCESS

### Identify your Site Access Needs

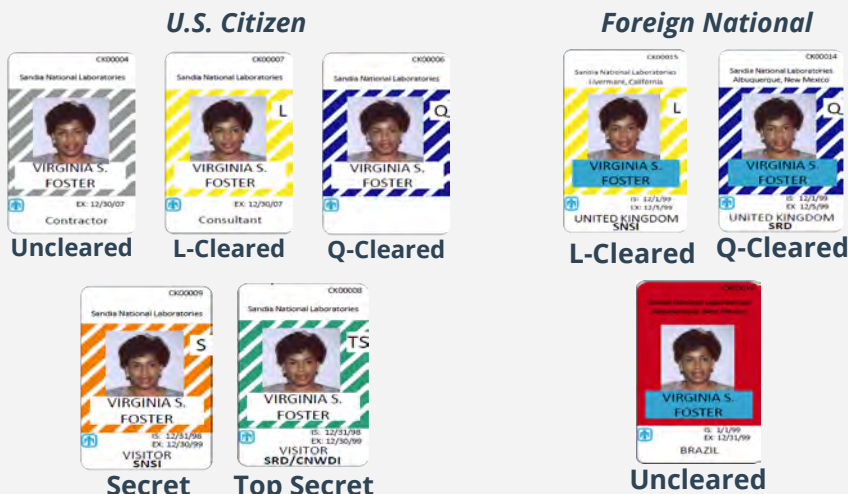
Controlling site access to a Nuclear Weapons Research Laboratory is an essential part of everyone's responsibility for safeguarding nuclear materials. In this section we will cover Site Badges and Responsibilities, Maintaining Your Clearance, and DOE and Sandia Reporting Requirements.

Below are some common badges you may see at Sandia. Control site access by ensuring the badge:

- is an appropriate site-specific badge, DOE standard badge, or federal credential
- picture matches the badge holder
- is not expired
- displays the appropriate clearance level

## SNL DOE Security Badges

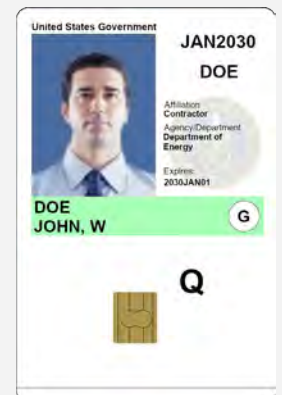
### SNL Local Site-Specific Only (LSSO) Badges



LSSO badges are only for specific sites. At SNL, they are required if you don't have a DOE-issued HSPD-12 credential.

Uncleared Foreign National LSSO badges are **red** for easy identification.

### HSPD-12 Federal Credential



DOE-issued HSPD-12 Federal Credentials are the most common form of identification at SNL.

Some DOE entities issue **uncleared** federal credentials that do not display a clearance level. Don't assume that people with federal credentials have clearances. If you don't recognize the person or badge, play it safe and don't allow them access.

MOWs who have been granted an **Interim Security Clearance (ISC)** or **Temporary Security Clearance Upgrade (TSCU)** are not allowed access to some forms of classified, yet their badges look the same as if they were granted a regular Q clearance. MOWs who have been granted an ISC or TSCU have been briefed on their requirements, responsibility to self identify, and limitations for access to information.

## CONTROL SITE ACCESS

### Badge Responsibilities

To ensure everyone knows who you are and if you belong here it is important to know your badge responsibilities.

#### WEAR YOUR BADGE:

- Conspicuously
- Photo Side Out
- Front of Body
- Above the waist
- Over outerwear

#### RENEW YOUR BADGE IF:

- It has expired
- Physical appearance significantly changes
- Clearance status or level changes
- Badge becomes faded or damaged
- Name legally changes

#### RETURN YOUR BADGE:

- If badge authorization expires
- When site access is no longer required or authorized (e.g. termination)
- As directed by SNL authorities (e.g. manager, Protective Force, Personnel Security)

#### DO NOT:

- Allow your badge to be altered, photocopied, or photographed
- Use your badge as identification for unofficial purposes
- Wear your badge offsite unless at a DOE-affiliated location



### REPORT:

Lost or stolen badges must be reported *immediately* to Security Connection.

**HSPD-12 badges must be listed on the traveler's International Hand Carry application prior to leaving the United States.**

## CONTROL SITE ACCESS

### Maintaining your access

The Department of Energy (DOE) Personnel Security Program establishes requirements that ensure DOE's missions are accomplished in a secure environment by men and women in whom both the Department and the American people may place their complete trust and confidence.

All individuals' initial and continued eligibility for security clearances are determined against the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (National Guidelines).

See **Understanding the Clearance Process** in **RESOURCE DOCUMENTS**.

## Your Reporting Requirements

All clearance holders are required to report certain events

Timely reporting is required!

Don't be afraid to report!

You can't be coerced or blackmailed under a healthy reporting culture.

It's better to have reported correctly than to be found to be hiding information.



### Some reportable events:

Arrests, citations, tickets, summonses

Any positive drug test

Drug abuse or treatment for drug or alcohol abuse

Involvement in or knowledge of a security incident

Theft, waste, fraud, abuse

Foreign Interactions

Foreign travel

Marriage and/or cohabitation

Name change

Filing for bankruptcy

Change in citizenship

Financial windfalls/debts

See the **DOE and SNL Reporting Requirements of Security Interest** in **RESOURCE DOCUMENTS**.

## CONTROL SECURITY AREA ACCESS

### Security Area Types at Sandia

Once you've been issued a badge, you have a responsibility for understanding the type of area that you will need physical and administrative access to. Below are types of Sandia-controlled premises and a brief description of those areas. Increasing controls are required as the sensitivity increases. You are responsible for controlling access to those areas. See **Who & What Can Go Where** in **RESOURCE DOCUMENTS**.

#### PUBLIC AREA

Areas that are accessible to the general public, during operational hours.

#### NON-PUBLIC AREA

A building, office, or other structure that is not open to the public, does not meet requirements for a PPA, but requires the use of a DOE-standard or local site specific only (LSSO) badge.

#### PROPERTY PROTECTION AREA (PPA)

Area established to protect individuals and government buildings, facilities, and property against damage, destruction, or theft.

#### LIMITED AREA (LA)

Area designated for the protection of classified matter and/or Category III quantities of Special Nuclear Material (SNM).

#### VAULT TYPE ROOM (VTR)

A Safeguards and Security (S&S) approved area that includes approved Level 1 security locked door(s) and protection provided by intrusion alarm system.

General Access Area (GAA)		Property Protection Area (PPA)	Limited Area (LA)	Vault Type Room (VTR)
Public	Non-Public			
Badge <i>not</i> required	Badge <b>REQUIRED</b>	Badge <b>REQUIRED</b>	Badge <b>REQUIRED</b>	Badge <b>and</b> access list <b>REQUIRED</b>
Clearance <i>is not</i> required	Clearance <i>is not</i> required	Clearance <i>not</i> required	Clearance <b>REQUIRED</b>	Clearance <b>REQUIRED</b>
Uncleared: escort <i>not</i> required	Uncleared: escort <i>not</i> required	Uncleared: escort <i>not</i> required	Uncleared: <b>ESCORT REQUIRED</b>	Uncleared/Unauthorized: <b>ESCORT REQUIRED</b>

## CONTROL SECURITY AREA ACCESS

### Your Responsibilities

Everyone *must* swipe or present their badge to gain access.



#### NO VOUCHING OR PIGGYBACKING

Do not **vouch** other individuals through **pedestrian** access-control points (gates, turnstiles, doors, etc.) at a **security area boundary**.



#### NO TAILGATING

Do not **follow** another individual through a **security area boundary** without that individual's knowledge.



#### System overlapping

Entering an area via an automated access-control device while another person **holds the door open**, thereby **ensuring** that each person entering the area is both **authorized and appropriately recorded** by the automated access-control system.

## CONTROL SECURITY AREA ACCESS

### Escorting Uncleared Individuals

An **uncleared** individual must be **escorted at all times** in a limited or more restrictive area.

An **escort** is an appropriately cleared U.S. citizen able to maintain **positive control** over the uncleared individual (who do not have the proper need-to-know or access authorizations for the security area), and be **knowledgeable of safety and security requirements** applicable to the areas being accessed (e.g. controlled and prohibited articles). Escorting is an **additional responsibility** – do not escort if you are not comfortable doing so; when transferring escort duty to another, ensure that the new escort **accepts** this responsibility.



Escorts and their uncleared escortees must display the applicable **'E' and 'U' card**. Sandia's escort ratio is **1 cleared escort for every 8 uncleared** individuals.



Escorts for foreign nationals **must** be listed on the **Foreign National Request Security Plan**.



## CONTROL SECURITY AREA ACCESS

**Controlled Articles**

A **controlled article** is a portable electronic device, both SNL and personally owned, that is capable of **recording** information or **transmitting** data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment).



- Recording Equipment
- Transmitting Equipment
- Bluetooth, cellular, and Wi-Fi-enabled devices
- Video and photography cameras

Any device (whether Sandia-issued or personally owned) consistent with the definition of a controlled article must have **prior authorization** before it may be introduced to any **limited or more restrictive area**.

**If in doubt – leave it out!**

**Certain items are authorized in policy:**

- Government-owned laptop computers, storage devices, or peripherals
- Mobile devices
- Test, measurement and diagnostic equipment
- Radios/CD Players/MP3 players without recording or transmitting capabilities
- One-way pagers and vehicle key fobs

**Items in the above list are the only personally owned controlled articles allowed in the Limited Area.**

**Any other Sandia-issued controlled article not listed above** must be registered through the **Controlled Articles Registration Process (CARP)** prior to **introduction** in any Limited or more restrictive area.

## CONTROL SECURITY AREA ACCESS

### Prohibited Articles

A ***prohibited article*** is any kind of item that can produce injury to persons or damage property, or is otherwise not allowed by federal law and/or Sandia policy.



- Firearms
- Explosives
- Dangerous weapons
- Instruments or material likely to produce substantial injury/damage to persons or property
- Alcohol
- Personal chemical protection sprays (pepper spray)
- Hazardous radiological, chemical, or biological materials
- Any other item prohibited by law (e.g., illegal drugs & paraphernalia)

### Exceptions:



Alcoholic beverages may be temporarily stored in an **unopened, sealed container** in a locked **personally owned vehicle**



Personal pocket or utility knives (e.g. Leatherman tools) are allowed if blade length is less than **< 2.5 inches**

No weapon type knives (hunting, switchblades)

Food preparation knives are exempt

**Prohibited Articles** are **NOT ALLOWED** on any Sandia-controlled premises (including the parking lots.)

## CONTROL SECURITY AREA ACCESS

**Mobile Devices and Secure Space**

**Mobile Devices** are prohibited from entering **Secure Space** at any time.

A **mobile device** is a portable *computing* device that:

- has a small form factor such that it can easily be carried by a single individual; and
- possesses onboard sensors that allow the device to capture audio or video information; and
- does not use a desktop operating system safeguarded by an NNSA Cyber Security Program; and
- is designed to operate without a physical connection (e.g., wirelessly); and
  - possesses local, non-removable data storage; and
  - is powered-on for extended periods of time with a self-contained power source

**Examples of mobile devices include cell phones, tablets, smart watches/fitness trackers, e-readers, gaming systems, and *more*.**



## CONTROL SECURITY AREA ACCESS

**Mobile Devices and Secure Space**

**Mobile Devices** are prohibited from entering **Secure Space** at any time.

A **Secure Space** is defined as:

National Nuclear Security Administration (NNSA) secure space includes all material access areas (MAAs), protected areas (PAs), vault-type rooms (VTRs), special designated areas, and areas requiring recurring technical surveillance countermeasures (TSCM) services.

NNSA secure space also includes limited areas (LAs), or any portion thereof, to include an individual room within which any national security system (NSS) is physically present. Sufficient electromagnetic and acoustical isolation may be used to segregate secure spaces within larger LAs.

**Secure Space is clearly signed at its boundaries with these signs, or similar – look for them!**





## CONTROL SECURITY AREA ACCESS

**Mobile Devices and Secure Space**

**Mobile Devices** are prohibited from entering **Secure Space** at any time.

Members of the Workforce may bring and use mobile devices in a Limited Area, as long as they do not enter a secure space and follow these rules:

- Mobile devices brought into the limited area must have **Bluetooth** and **WiFi disabled**



- Mobile devices brought into the limited area cannot be left **unattended** in any location except for a **marked, approved storage location** (see example).



- Sandia-managed mobile devices may be taken anywhere outside of Secure Space, **including offices**, but must be removed and placed in approved storage prior to discussing classified information.
- Personally owned mobile devices are only allowed in limited area '*common areas*', including **building hallways, restrooms, break rooms, approved storage locations, and outside**
- **You** assume the risk for the device and its use while on Sandia-controlled premises.

## CONTROL SECURITY AREA ACCESS

**Medically Necessary Portable Electronic Devices**

Medically necessary portable electronic devices (MEDPEDs) are **not permitted in a limited or more restrictive area** until approved following an evaluation for **technical security vulnerabilities**.

You must request an evaluation for your medical electronic devices from Sandia Telecommunications Security at least 30 days before access is needed.

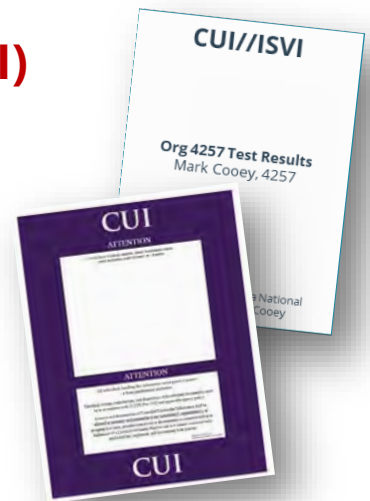
Approved devices may be brought into limited areas only in accordance with mitigations or guidance as provided following the evaluation. Until a MEDPED is approved, it is **not authorized** to enter a limited area.

To request a technical review, use the tool at [medpeds.sandia.gov](https://medpeds.sandia.gov) or contact [medpeds@sandia.gov](mailto:medpeds@sandia.gov).

## CONTROL INFORMATION ACCESS

**Controlled Unclassified Information (CUI)**

You may work with or encounter **government-owned** information that is **required** by law or policy to be safeguarded as **controlled unclassified information (CUI)**.

**Controlled Unclassified Information (CUI):**

Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that **laws, regulations, or Government-wide policies (LRGWP)** requires or permits an agency to handle using safeguarding or dissemination controls.

CUI may only be disseminated to those requiring access in furtherance of a **lawful governmental purpose**, and whom are authorized under the applicable LRGWP (if applicable.)

**Lawful Governmental Purpose (CUI):**

Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement). An employee's LGP may be defined by DOE policy, position descriptions, or contractual requirements.

## CONTROL INFORMATION ACCESS

**Protection and Control of CUI**

CUI must be handled in accordance with the dissemination and safeguarding requirements outlined in Sandia policy and/or the authorizing LRGWP:

**IDENTIFY**

Members of the Workforce are responsible for identifying **Controlled Unclassified Information** that requires protection under an **LRGWP**.

There are many CUI categories that may apply - consult the CUI homepage at [cui.sandia.gov](http://cui.sandia.gov) for the most current list.

**MARK**

All information containing CUI must be marked appropriately with the required **CUI banner** marking and '**Controlled By**' markings.

To assist you with marking CUI, Sandia has created the **Marking Assist Tool** available in Microsoft Teams on the SRN or at [markingassist.sandia.gov](http://markingassist.sandia.gov).

**PROTECT**

CUI that is not under the **direct control** of an authorized user must be protected through implementation of at least one physical barrier (e.g., a locked door).

CUI may only be processed on electronic systems **approved** for protection of CUI, and controls must exist to prevent **unauthorized** access to CUI (e.g., metagroup controls).

**DISSEMINATE**

CUI may only be disseminated to those requiring access in furtherance of a **lawful governmental purpose** who are authorized under the applicable LRGWP.

Ensure that **physical CUI sent via mail** is marked appropriately, but does not indicate the presence of CUI on the outside of the package.

Encrypting and digitally sign **email** with your HSPD-12 badge or an approved alternative.

Consider the sensitivity of the CUI merits optional encryption if discussed over the **telephone**.

**DISPOSE**

CUI must be destroyed in accordance with Sandia policy. Cross-cut shredders that produce **1 mm x 5 mm particles or smaller** (and existing grandfathered shredders) may be used, or though the **use of a white destruction bag**.

**CUI Specified** information must be destroyed in accordance with any destruction requirements identified in the applicable LRGWP.

For more information, visit the CUI homepage at [cui.sandia.gov](http://cui.sandia.gov) and take **CUI-100DE, CUI Training**, in TEDs.



## CONTROL INFORMATION ACCESS

**Legacy information, including Official Use Only (OUO)**

You may also come across information marked under the previous Sandia sensitive unclassified information standards, including **Official Use Only (OUO)**.

This information must be **protected as CUI**, and is only releasable to those with a valid ***need-to-know***.



**If reused, shared, or updated**, this information must be evaluated for CUI and re-marked if applicable. If you are unable to update the document for any reason, use of the [SF 901, CUI Cover Sheet](#) is acceptable.

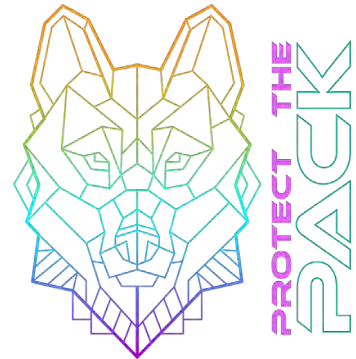
*Note:* Re-use means incorporating, restating, or paraphrasing information from its originally designated form into a newly created document. Existing documents not updated, shared, or reused after February 28, 2023 are *legacy* documents.

## CONTROL INFORMATION ACCESS

**Operations Security (OPSEC)**

In addition to protecting information that you are required to by law, you must also practice **good OPSEC**.

OPSEC is the process of denying an adversary **critical information**.



**Critical Information:** Specific facts about intentions, capabilities, and activities vitally needed by adversaries to plan and act effectively to guarantee failure or unacceptable consequences for mission accomplishment.

Once identified by the OPSEC Program, critical information is published in a library as a **critical information list (CIL)** including the **general Sandia CIL**.

More specific CILs are required at the center level, but you may have program or specific critical information lists – ask your manager or visit [opsec.sandia.gov](https://opsec.sandia.gov).

**For more information, see Critical Information Lists (CILs) in RESOURCE DOCUMENTS.**

## CONTROL INFORMATION ACCESS

**Protecting What is Ours****Critical Information is CUI.**

Even information you didn't consider to be sensitive may be identified as critical information.



Consult your **Critical Information List (CIL)** for a list of topics (note that more than one CIL may apply).

If the information contains critical information as identified in the CIL, mark and protect it as

**CUI//OPSEC.**

For assistance, contact [opsec@sandia.gov](mailto:opsec@sandia.gov) or visit [opsec.sandia.gov](http://opsec.sandia.gov).

## CONTROL INFORMATION ACCESS

**Key Terms: Classified Information Protection**

All members of the workforce are responsible for protecting *classified information*. This means safeguarding classified information against inadvertent or unauthorized release to those without a **valid access authorization** and a **need to know**:

**Access Authorization**

Also known as a '**clearance**', an access authorization denotes an individual's **eligibility** to access a **particular type** of information or material classified by the federal government.

**Need to Know**

A determination made by an **authorized holder** of classified and/or sensitive information that a prospective recipient **requires** access to the information in order to perform or assist in a **lawful and authorized governmental function**.

Classified information must either be under the direct control of an authorized holder responsible for its protection, or stored appropriately.



## CONTROL INFORMATION ACCESS

### Classified Information

To ensure that DOE and Sandia information is properly protected, it is essential that classified matter be appropriately managed at all times, from identification or creation through disposition.

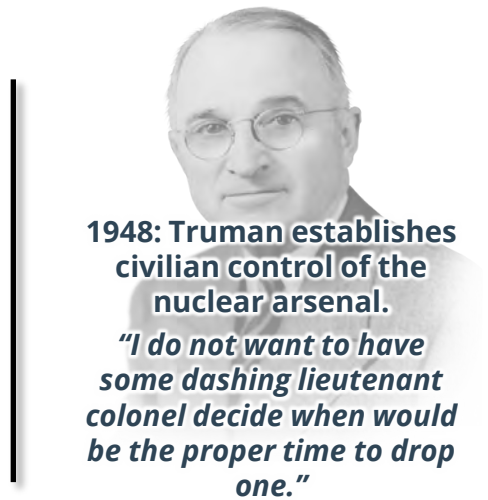
The large amount of information and material in use at the Laboratories, and the fact that this content moves from organization to organization and from site to site, requires uniform processes for marking and controlling it.

See **Getting Started With Classified** in **RESOURCE DOCUMENTS**.

**Classified Information** is information that is classified by statute or executive order.

**Classification levels** identify the degree of damage that could be done to national security due to unauthorized disclosure of this information.

**Classification categories** are type of information as defined in statutes or Executive Orders.



Classification Level	DOE Classification Categories and Clearance Levels				Degree of Damage
	Restricted Data (RD)	Formerly Restricted Data (FRD)	Trans-classified Foreign Nuclear Information (TFNI)	National Security Information (NSI)	
Top Secret (TS)	Q Only	Q Only	Q Only	Q Only	Exceptionally Grave
Secret (S)	Q Only	Q and L	Q and L	Q and L	Serious
Confidential (C)	Q and L	Q and L	Q and L	Q and L	Damage

Access to classified information is:  
**compartmented** to prevent harm to national security, if lost.  
**restricted** to persons with a security clearance and a **need to know**.

**CONTROL INFORMATION ACCESS****Classified Information Resources**

Sandia's policy is to ensure that only authorized personnel determine whether documents and material are unclassified or classified. When working with classified information, we don't expect you to know it all. Here are some resources available to help.

**Derivative Classifier (DC)** – an individual authorized to confirm that an unmarked document or material is unclassified or determine that it is classified as allowed by his or her description of authority.

**Use Sandia's 'Jupiter' application to find your DC.**

**Derivative Declassifier (DD)** – an individual authorized to declassify or downgrade documents or material that an employee believes no longer requires protection, in specified areas, as allowed by his or her description of authority. DDs are located in the Classification Office.

**Classified Administrative Specialist (CAS)** – an individual trained to mark, store, duplicate, destroy, and move (e.g. mail, ship, fax, hand carry, receive) classified matter.

**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** – helps with classification topics not handled by your DC, DD, or CAS. They are also there to help resolve any disagreements about a DC determination.

**CONTROL INFORMATION ACCESS****The Classification Challenge Process**

If you think a DC determination is incorrect, you have the responsibility to challenge the determination. For assistance with challenges, contact the Classification Office: **NM: 505 844-5574 / [classificationdept@sandia.gov](mailto:classificationdept@sandia.gov) CA: [CAClassDept@sandia.gov](mailto:CAClassDept@sandia.gov).**

You are encouraged to resolve challenges locally in discussions with your DC and the Classification Officer. If it cannot be resolved, you have the right to submit a formal 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, DOE OC at any time. Request additional information from [outreach@hq.doe.gov](mailto:outreach@hq.doe.gov).

**Under no circumstances will you be subject to retribution for making such a challenge. See Laboratory Policy SS002, *Identifying Classified Information*, Section 4 for Challenge procedures.**

## CONTROL INFORMATION ACCESS

**Protection and Control of Classified Information**

Throughout every lifecycle stage of documents and material, Safeguards and Security has established robust policies to help you protect and control **Classified Information**.

See the **Getting Started With Classified Handout** in the **RESOURCE DOCUMENTS**.

**IDENTIFY**

All documents in **Potentially Classified Subject Areas** must be reviewed for classification by a cognizant **Derivative Classifier (DC)**:

- Before being finalized
- Before being released outside of a working group
  - Before being permanently filed, and:
- No later than 180 days after the creation of the document or last revision.

**Get a DC Review**

- ✓ A newly generated document or material in a classified subject area that potentially contains classified information
- ✓ An existing, unmarked document or material an employee believes may contain classified information
- ✓ An existing, marked document or material an employee believes may contain information classified at a higher level or more restrictive category
- ✓ Extracts: A newly generated document that consists of a complete section (e.g., chapter, attachment, appendix)
- ✓ Printed output from a classified information system
- ✓ Document or material generated in a classified subject area and intended for public release (e.g., for a publicly available webpage, for news organizations), including documents provided to or testimony given to Congress

**MARK**

Ensure all classified matter is marked with the proper and complete classification markings.

If the classified matter has not yet been reviewed by a DC, mark and protect at the **highest potential classification** level the item is believed to contain until it is reviewed by a DC.

For more information, take **SEC301: Classified Matter Training**, and **SEC303: Classified Marking Training**.

## CONTROL INFORMATION ACCESS

# Protection and Control of Classified Information

Throughout every lifecycle stage of documents and material, Safeguards and Security has established robust policies to help you protect and control **Classified Information**.

See the **Getting Started With Classified Handout** in the **RESOURCE DOCUMENTS**.

## PROTECT

Classified matter must be protected from release to those without the valid need-to-know or access authorization, and any additional access authorization if required.

When not in use (i.e. under your direct control), classified matter must be stored in a GSA Security Container or VTR approved for the highest level of classification the matter contains.

For assistance protecting classified matter, consult your **Classified Administrative Specialist (CAS)**.



GSA-Approved Storage Repositories  
(Safes/Vault Type Rooms [VTRs])



## DISSEMINATE

Classified matter may only be disseminated to those with a **valid need-to-know and access authorization**.

Protect classified matter from inadvertent or unauthorized release by ensuring classified work takes place only in a structure (not outside or in common areas), and if electronic, takes place on an **approved system and network** for the level and category it contains.

For assistance sending classified matter, work with your **CAS**.

## DISPOSE

Classified matter may only be destroyed using equipment and process approved by Classified Matter Protection and Control (CMPC), such as a classified shredder or through the use of a **red** destruction bag. Classified matter intended for destruction must be **protected** until it is destroyed. After destruction, residue must be **inspected to ensure no classified matter remains**.

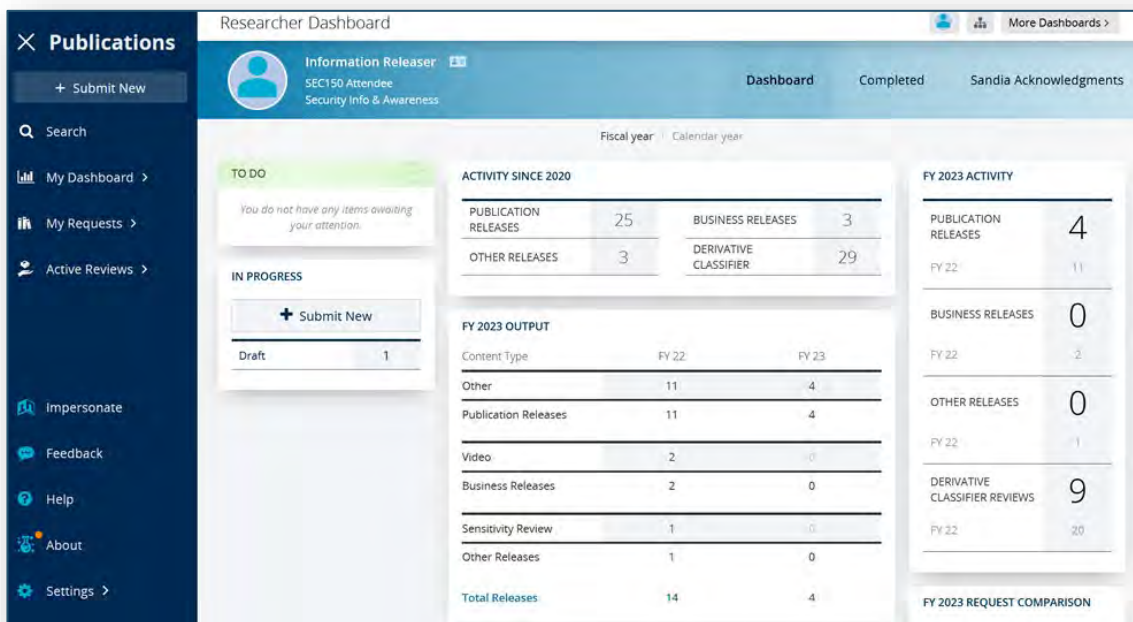
For assistance destroying classified matter, consult your **CAS**.

## CONTROL INFORMATION ACCESS

# Releasing Information outside of Sandia

If you will be sharing information outside SNL, use the **Information Release (IR)** online tool.

This process ensures that all documents released by Sandia are reviewed for classification and sensitivity prior to release in order to prevent unauthorized disclosure of classified or controlled information.



**Researcher Dashboard**

Information Releaser  
SEC150 Attendee  
Security Info & Awareness

Dashboard | Completed | Sandia Acknowledgments

Fiscal year | Calendar year

**TO DO**

You do not have any items awaiting your attention.

**IN PROGRESS**

+ Submit New

Draft	1
-------	---

**ACTIVITY SINCE 2020**

PUBLICATION RELEASES	25	BUSINESS RELEASES	3
OTHER RELEASES	3	DERIVATIVE CLASSIFIER	29

**FY 2023 OUTPUT**

Content Type	FY 22	FY 23
Other	11	4
Publication Releases	11	4
Video	2	0
Business Releases	2	0
Sensitivity Review	1	0
Other Releases	1	0
<b>Total Releases</b>	<b>14</b>	<b>4</b>

**FY 2023 ACTIVITY**

PUBLICATION RELEASES	4
FY 22	11
BUSINESS RELEASES	0
FY 22	2
OTHER RELEASES	0
FY 22	1
DERIVATIVE CLASSIFIER REVIEWS	9
FY 22	20

**FY 2023 REQUEST COMPARISON**

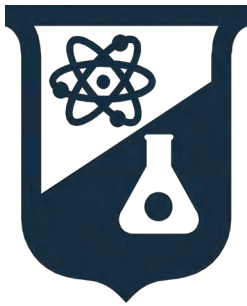
## CONTROL INFORMATION ACCESS

**Special Nuclear Material (SNM)**

Some Sandia sites may have **special nuclear material (SNM)**.

SNM is protected according to the material's **category** (quantity) and **level of attractiveness** (ease of turning it into a weapon) to an adversary trying to create a nuclear weapon.

Since it is an attractive adversary target, there are strict **requirements** as to where it can be used or stored and who has access to it.

**Special Nuclear Material (SNM)**

Fissile material that is especially useful in nuclear weapons.

SNM requires **specific protections**.

If you work with SNM, you will receive **additional training**.

## CONTROL INFORMATION ACCESS

**The DOE's 'No Comment' Policy**

DOE has a 'no comment' policy regarding classified information in the open literature or in response to public inquiry on classified subjects.



A **comment** is any activity that could potentially allow an unauthorized person to locate classified information or confirm the classified nature or its technical accuracy.

Commenting on classified information can result in **greater damage** to national security by **confirming details** such as its location, classified nature, or technical accuracy.

**Do not** comment on the classification status or technical accuracy of information.

If asked, state only: ***"We don't comment on items in open literature."***

**Report DOE classified information in open source to SIMP (Security Connection).**

For more information, see **DOE GEN-16** or take **CLA138** in TEDs.



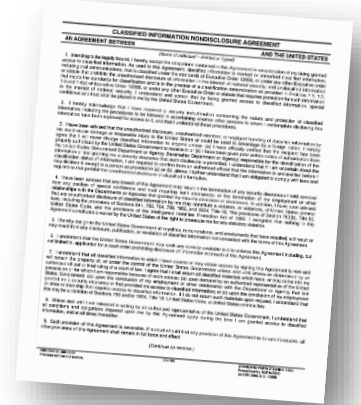
## CONTROL INFORMATION ACCESS

# Your Commitment to Protect: The SF 312

As a condition of access, a cleared individual must complete an SF 312 Classified Information Nondisclosure Agreement before accessing classified information or matter.

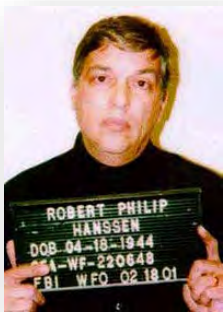
See **SF 312 Classified Nondisclosure Agreement Form** in **RESOURCE DOCUMENTS**.

The SF 312 is a legally enforceable nondisclosure agreement (NDA) between **you** and the **U.S. Government** wherein you agree to protect classified information from **unauthorized disclosure**.



## *Unauthorized Disclosure*

The transfer, via any means, of classified information or material to someone who is not authorized to receive such information.



**Failing to meet your responsibilities outlined in the SF 312 regarding classified could result in:**

- **Termination.**
- **Civil and criminal penalties** as outlined in the SF 312.

## SECURITY INCIDENTS

# The Security Incident Management Program (SIMP)

The **Security Incident Management Program (SIMP)** inquires into all potential security incidents at all sites.

**Incidents of Security Concern**, sometimes referred to as **Security Incidents**, are events that are of concern to the DOE Safeguards and Security Program that warrant a formal inquiry and subsequent reporting of the incident to DOE.

An **inquiry** must be conducted to establish the pertinent facts and circumstances surrounding the security incident. If you suspect you have caused an incident or witnessed one, **report immediately** to SIMP via **Security Connection** 505-845-1321.

### Events you MUST report:

**Unauthorized Network Based Transmission**  
(e.g. classified on the SRN)

**Improperly Secured Information System**  
(e.g. SCN not locked)

**Unauthorized Portable Electronic Devices**  
(e.g. around classified)

**Improper Storage/Protection of Classified**  
(e.g. safe left open)

### SIMP will:

- Collect facts
- Prevent additional release of information
- Report to DOE

**Do not provide details over the phone! Let the inquiry official drive the conversation.**

## SECURITY INCIDENTS

# Security Incident Reporting Requirements

If you suspect you have caused an incident or witnessed one, report immediately to Security Connection (24/7/365).

All potential incidents must be reported — an inquiry will determine whether an incident has actually occurred. If sensitive information was improperly protected it may be reported to DOE.

A very small number of reports to SIMP result in incidents.

Be nice and Report Twice. Let your security professional or manager know.



**If you See Something, Say Something!**

## SECURITY INCIDENTS

### Causes of Security Incidents

Human performance and effectiveness is a known factor with security incidents at Sandia. Most common contributors fall into one of the four categories below.

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

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

## SECURITY INCIDENTS

### Causes of Security Incidents

Understand where you are vulnerable to making mistakes, know your limitations and resources, and do what you can to reduce the risk of security incidents occurring.

Make sure your family knows these limitations!

**Self-check before entering a Limited Area**

**Secure your work area every time you walk away**

**Know your Security Professional**

**Call Security Connection with questions**

**Talk to your family about Sandia's security rules**

## COUNTERINTELLIGENCE

**The Threat is Real**

Sandia is one of America's premier national security laboratories.

Foreign intelligence services are keenly interested in gaining access to the intellectual property that our Laboratory produces and frequently attempts to do so. International terrorist organizations intent on causing a "terrorism of mass destruction" incident on U.S. soil also target Sandia.

To succeed, foreign intelligence officers as well as international terrorists would require the cooperation of an insider unworthy of the trust vested in them by Sandia.

**Office of Counterintelligence**

The mission of the **Office of Counterintelligence** is to protect and defend against hostile foreign intelligence activities and terrorism threats targeting Sandia National Laboratories.

**Sandia hosts visitors from all over the world.**

The Intelligence Community has assessed that a number of foreign countries, to include some traditional U.S. allies, continue their collection activities against the United States. These foreign collection efforts continue to be driven by military force modernization, economic competition, and commercial modernization using technologies with dual-use applications. Foreign individuals, businesses, government entities, and intelligence-affiliated personnel continue to employ collection techniques against U.S. targets both abroad and in the United States.

**Counterintelligence would like you to be familiar with some of the targets and targeting methods used by FIs.**

## COUNTERINTELLIGENCE

## Detecting and Deflecting Elicitation

You may be targeted by a trained elicitor using a number of common techniques:

**Assumed Knowledge:** *Pretend to have knowledge or associations in common with a person.*  
“According to the computer network guys I used to work with...”

**Can you top this?** *Tell an extreme story in hopes the person will want to top it.* “I heard Company M is developing an amazing new product that is capable..”

**Criticism:** *Criticize an individual or organization in which the person has an interest in hopes the person will disclose information during a defense.* “How did your company get that contract? Everybody knows Company B has better engineers for that type of work.”

**Deliberate False Statements / Denial of the Obvious:** *Say something wrong in the hopes that the person will correct your statement with true information.* “Everybody knows that process won’t work—it’s just a DARPA dream project that will never get off the ground.”

**Feigned Ignorance:** *Pretend to be ignorant of a topic in order to exploit the person’s tendency to educate.* “I’m new to this field and could use all the help I can get.” “How does this thing work?”

**Flattery:** *Use praise to coax a person into providing information.* “I bet you were the key person in designing this new product.”

**Good Listener:** *Exploit the instinct to complain or brag, by listening patiently and validating the person’s feelings (whether positive or negative).* If a person feels they have someone to confide in, he/she may share more information.

**The Leading Question:** *Ask a question to which the answer is “yes” or “no,” but which contains at least one presumption.* “Did you work with integrated systems testing before you left that company?”

**Volunteering Information / Quid Pro Quo:** *Give information in hopes that the person will reciprocate.* “Our company’s infrared sensors are only accurate 80% of the time at that distance. Are yours any better?”

**Ruse Interviews:** *Someone pretending to be a headhunter calls and asks about your experience, qualifications, and recent projects.*

**Oblique Reference:** *Discuss one topic that may provide insight into a different topic.* A question about the catering of a work party may actually be an attempt to understand the type of access outside vendors have to the facility.

**Quote Reported Facts:** *Reference real or false information so the person believes that bit of information is in the public domain.* “Will you comment on reports that your company is laying off employees?” “Did you read how analysts predict...”

You can politely discourage conversation topics and deflect possible elicitation by:

- Referring them to public sources (websites, press releases)
- Ignoring any question or statement you think is improper and changing the topic
  - Deflecting a question with one of your own
    - Responding with “Why do you ask?”
      - Giving a nondescript answer
      - Stating that you do not know
  - Stating that you would have to clear such discussions with your security office
    - Stating that you cannot discuss the matter

## COUNTERINTELLIGENCE

### **Are you a target?**

#### **Targeting Methods by FIs**

- Hacking of electronic media (e.g., computers, social networks)
- Eliciting during conferences/trade fairs
- Tasking foreign students at U.S. universities
- Debriefing foreign visitors to the U.S. routinely
- Targeting ethnic employees/scientists
- Use of Interpreters
- Sexspionage

#### **Targets for Foreign Services:**

##### **Clearance Holders**

##### **Anyone with access to:**

- SNL Facilities
- SNL Equipment, Electronic media
- SNL Personnel
- SNL Data



## COUNTERINTELLIGENCE

**Real Life Examples – The Spy Gallery**

Here are some examples of real-life threats that have occurred all over the country, including New Mexico. Read through them to understand and prevent making the same mistake.

**Sexpionage****Anya Kushchenko aka Anna Chapman**

- Online Realtor
- Russian Illegal
- Active 2009-2010
- Made contact with high-level government officials
- Deported back to Russia in 2010 as part of a prisoner exchange

**Sexpionage****Ben Bishop**

- Civilian Defense Contractor
- Romantically involved with a 27 y/o Chinese grad-student
- Active 2011-2013
- Provided classified information to her
- Sentenced in 2014 to 87 months in prison

**Sexpionage****Donald Keyser**

- US Department of State - Ambassador
- Romantically involved with a Taiwanese Intelligence Officer
- Active 2002-2004
- Sentenced in 2007 to one year and one day in prison for unauthorized possession of classified documents and lying to the FBI

**Insider****Roy Oakley**

- DOE – East Tennessee Technology Park
- Stole restricted nuclear materials
- Attempted to sell the materials to France
- Active at least 2006 – 2007
- Sentenced in 2009 to six years in prison for unlawful Disclosure of Restricted Data under the Atomic Energy Act

## COUNTERINTELLIGENCE

**Real Life Examples – The Spy Gallery**

Here are some examples of real-life threats that have occurred all over the country, including New Mexico. Read through them to understand and prevent making the same mistake.

**Insider****Jonathan & Diana Toebe**

- Husband: cleared Engineer Naval Nuclear Propulsion Program since 2012; Wife: Teacher
- Provided RD to undercover federal agent
- Pleaded guilty in 2022
  - Jonathan sentenced to over 19 years
  - Diana sentenced to over 21 years

**Insider****Henry Kyle Frese**

- Former employee of Defense Intelligence Agency (DIA)
- Top Secret clearance
- Active 2017 – 2019
- Sentenced in 2020 to 30 months for leaking classified information to journalists

**Insider****Ron Rockwell Hansen**

- Former employee of Defense Intelligence Agency (DIA)
- Top Secret clearance
- Active 2014 – 2018 for the People's Republic of China
- Sentenced in 2019 to 10 years for attempting to communicate, deliver or transmit information

**Insider****Pedro Mascheroni**

- Los Alamos National Laboratory employee
- Sent angry letters to legislators, scientific panels and private advocacy groups accusing DOE of mismanaging its nuclear weapons program and wasting billions of dollars on a giant laser
- Attempted to pass S-RD nuclear weapons info. to Venezuela
- Active 2007-2009
- Sentenced in 2015 to five years in prison

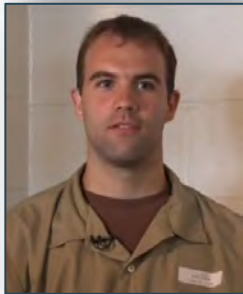
## COUNTERINTELLIGENCE

**Real Life Examples – The Spy Gallery**

Here are some examples of real-life threats that have occurred all over the country, including New Mexico. Read through them to understand and prevent making the same mistake.

**Insider****Peter Rafael Dzubinski Debbins**

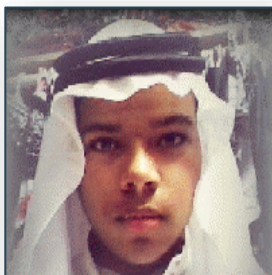
- Former Army Green Beret
- Active 1996-2011::Provided sensitive details about chemical and Special Forces units
- 2021: sentenced to 188 months for conspiring with Russian intelligence operatives to provide U.S. national defense information

**Insider****Glenn Duffie Shriver**

- US Civilian/Student studying in China
- Recruited and paid by the PRC to his "expertise"
- Department of State and CIA Applicant
- Active 2004-2010
- 2011: sentenced to four years in prison

**Insider****Alexander Fishenko**

- Dual citizen (U.S. and Russia); Russian Agent 1998 - 2012
- 2015: sentenced to 10 years in prison for acting as an agent of the Russian govt. in the U.S., conspiring to export and illegally exporting controlled microelectronics to Russia, conspiring to launder money and obstruction of justice

**Terrorism****John T. Booker Jr.**

- Civilian
- Facebook posts about committing jihad
- Attempted to detonate a vehicle bomb on the Ft. Riley military base
- February 2016: sentenced to 30 years in prison for one count of attempted use of a weapon of mass destruction and one count of attempted destruction of government property by fire or explosion.

## COUNTERINTELLIGENCE

### Real Life Examples – The Spy Gallery

Here are some examples of real-life threats that have occurred all over the country, including New Mexico. Read through them to understand and prevent making the same mistake.



#### Terrorism

##### Nidal Hasan

- United States Army – Major
- Inspired and in communication with Anwar al-Awlaki
- Dec. 2008 – Nov. 2009
- Nov. 5, 2009 killed 13 people, injured 32 at FT Hood, TX
- In 2013 sentenced to death



#### Terrorism

##### Tamerlan and Dzhokhar Tsarnaev

- April 2013 Boston Marathon Bombing; killed three and injured several hundred
- Not affiliated with any terrorist organization
- Tamerlan killed in April 2013 trying to evade police
- Dzhokhar sentenced in May 2015 to death



#### Cyber

##### Robin Sage

- Facebook profile setup as 25-years-old
- Cyber Threat Analyst
- U.S. Navy's Network Warfare Command
- Graduated from MIT
- 10 years of experience



#### Cyber

##### Charles Eccleston

- Department of Energy 1988-2001
- National Regulatory Commission 2008-2010
- January 2015 spear-phishing attack on DOE employees
- Believed to be targeting for China
- Sentenced in 2016 to 18 months in prison



#### Cyber

##### ORNL Spear phishing

- Oak Ridge National Laboratory ORNL (Tennessee)
- 530 employees received e-mail with malicious link
- Server was breached when 27 employees clicked the link









## COUNTERINTELLIGENCE

# Reporting Requirements

The mission of Sandia Counterintelligence (CI) is to protect you, your work, Sandia's reputation as a U.S. National Security Laboratory, and U.S. National Security from foreign intelligence and international terrorist threats. To do this, CI needs your help.

## Report the following to Security Connection:

-  Substantive contact with a foreign national
-  All unofficial/personal **foreign travel** plans (to *any* country)
-  During foreign travel: unplanned interactions, unusual or suspicious activity, or legal/customs incidents
-  Financial or property interests in a foreign country
-  Foreign honoraria, gifts, or expenses paid
-  Unsolicited or suspicious behavior/contact (including emails, calls, or face-to-face)

### **SUBSTANTIVE CONTACT:**

A personal or professional relationship with a foreign national that is enduring and involves substantial sharing of information (including personal, business, or research information) and/or formation of emotional bonds (not to include family members).

The phrase also applies to any associations that involve sharing SNL information.

### **BE NICE, REPORT TWICE!**

You are required to report to DOE using the SF-86 and to Sandia via the current CI Reporting mechanism. Contact [ci-help@sandia.gov](mailto:ci-help@sandia.gov) or visit the CI Webpage for specific guidance on reporting.

## COUNTERINTELLIGENCE

# Additional Resources

Counterintelligence provides valuable expertise to all Members of the Workforce. Contact the Office of Counterintelligence for:

- Education/Preparation
- Foreign visit host briefings/debriefings
- Foreign travel briefings/debriefings (both professional or personal)
- Monthly Newsletters
- Spy of the Month Articles
- CI Monthly Calendars



**For more information:**

**505-284-3878 | [ci-help@sandia.gov](mailto:ci-help@sandia.gov)**

## Resource Documents

**You're just about done.**

Now that you have downloaded and read through the booklet the following resource documents and document links have been provided for your reference. The hard copy information provided in this booklet is accurate for the date you signed the completion record, but we recommend you use the links below to download the most current handout.

[Understanding the Clearance Process](#)

[Reporting Requirements](#)

[Who and What Can Go Where](#)

[Critical Information Lists \(CILs\)](#)

[Getting Started with Classified](#)

[SF 312 Classified Information Nondisclosure Agreement](#)

To receive **credit** in the **Sandia Learning Management System** for the SEC150 Comprehensive Security Briefing and to acknowledge your understanding of your SF 312 Classified Information Nondisclosure Agreement responsibilities outlined in the SF 312, see instructions on the **final page of this booklet**.

On behalf of Sandia National Laboratories  
Safeguards & Security Awareness Program

# THANK YOU!



# Understanding the Clearance Process



## Personnel Security Program Purpose

The Department of Energy (DOE) Personnel Security Program establishes requirements that ensure DOE's missions are accomplished in a secure environment by men and women in whom both the Department and the American people may place their complete trust and confidence. **A security clearance is an administrative determination confirming that the individual is eligible for access to classified information.**

No individual will be provided access to **classified information** or **Special Nuclear Material (SNM)** unless they have been granted the appropriate security clearance and possesses a **need-to-know**. Access to, knowledge of, or possession of classified information or SNM will not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

## Security Clearances

Security clearances and access authorizations denote an individual's **eligibility for access** to a particular type of classified information or material, such as **National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), or SNM**. In determining such eligibility, DOE may consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. Generally, DOE issues **Q and L access authorizations**.

An individual's eligibility for a clearance is based on the completion of a background (re)investigation conducted for DOE by the Defense Counterintelligence Agency (DCSA), the Federal Bureau of Investigation (FBI), or other federal agency authorized to conduct background investigations. Upon completion of the investigation, DOE **adjudicates** the information for clearance eligibility.

## Adjudication

Based upon information acquired through background (re)investigations and information otherwise available to personnel security officials, the adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that they are an **acceptable security risk**. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.

Eligibility for a security clearance is predicated upon the individual meeting established personnel security guidelines through the careful weighing of a number of variables known as the whole-person concept, based on National Standards that include **Adjudicative Guidelines for Determining Eligibility for Access to Classified Information**. Where no information exists related to any of the areas of concern identified in the Guidelines, a favorable determination will be made. If however information does exist related to any areas of concern identified in the Guidelines, such information will be regarded as derogatory and create a question as to the individual's security clearance eligibility. Provided such a question can be favorably resolved, the appropriate security clearance will be granted or continued.

Available, reliable information about the person, past and present, favorable and unfavorable, is considered in reaching an eligibility determination. In evaluating the relevance of an individual's conduct, both disqualifying and mitigating conditions outlined in the Adjudicative Guidelines are assessed and include **considering the following factors**:

- the nature, extent, and seriousness of the conduct
- the circumstances surrounding the conduct, to include knowledgeable participation
- the frequency and recency of the conduct
- the individual's age and maturity at the time of the conduct
- the voluntariness of participation
- the presence or absence of rehabilitation and other permanent behavioral changes
- the motivation for the conduct
- the potential for pressure, coercion, exploitation, or duress
- the likelihood of continuation or recurrence

## Sources of Legal Authority & Guidance

Legal authority and guidance for the DOE Personnel Security Program can be found in **Title 10, Code of Federal Regulations, Part 710 (10 CFR 710)** and **Executive Order (E.O.) 12968**. In all matters related to its internal personnel security activities, DOE retains **absolute authority**.

## Due Process

If it is determined that an individual is not eligible for a security clearance, Administrative Review procedures as set forth in **10 CFR 710** are initiated to ensure that they are afforded full due process in a manner consistent with traditional American concepts of justice and fairness.



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.

SAND2022-11100 O 08.15.2022 v1.0



# DOE and SNL REPORTING REQUIREMENTS OF SECURITY INTEREST



Revised: 14 February 2023

## 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 or circumstance, unless otherwise indicated.
- To begin the reporting process, contact Security Connection at 321 from a Sandia landline, 505-845-1321 from any phone, or [security@sandia.gov](mailto:security@sandia.gov). When applicable, follow additional guidance specified below.

## Members of the Workforce (MOWs)

All MOWs are required to report the events/circumstances specified below, when applicable. However, the **red highlighted** items are applicable only to clearance holders and clearance applicants. (See the [related FAQs](#) for additional information.)

### GENERAL REQUIREMENTS

1. **Become aware of any of the following about a DOE clearance holder or applicant:**
  - a) Unwillingness to comply with rules and/or regulations, or to cooperate with security requirements
  - b) Unexplained affluence or excessive indebtedness
  - c) Alcohol abuse
  - d) Illegal use or misuse of drugs or drug activity
  - e) Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified matter or other materials specifically prohibited by law from disclosure
  - f) Criminal conduct
  - g) Any activity that raises doubts about another individual's continued eligibility for access to classified matter.
  - h) Misuse of U.S. government property or information systems.  
**Note:** *Individuals who report circumstances about others may be asked to provide additional corroborative information.*
2. **Attempted elicitation (to include by media sources), exploitation, blackmail, coercion, or enticement to obtain classified matter or other information, or material specifically prohibited by law from disclosure.**

### LIFE CIRCUMSTANCES

3. **Marry or cohabit.**  
**Note:** *A cohabitant is a person who shares bonds of affection, obligation, or other commitment, as opposed to a person who resides for reasons of convenience (e.g., a roommate). A cohabitant does not include individuals such as a husband, wife, and children. Also see "Foreign Interaction" regarding cohabitation with a foreign national.*
4. **Action to legally change one's name.**

### CITIZENSHIP

5. **Change in citizenship (i.e., U.S. or foreign) or acquisition of another country citizenship(s).**

### MENTAL HEALTH

6. **Hospitalization for mental-health reasons.**

### LAW ENFORCEMENT

7. **Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, state, or other law-enforcement authorities for violations of law within or outside the U.S.**  
**Exception:** *Traffic violations for which a fine of less than \$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.*

### DRUG USE

8. **The use of any Federally illegal drug (to include the abuse or misuse of any legal drug).**
9. **Any drug-related treatment.**
10. **Positive (i.e., unfavorable) drug test regardless of source (e.g., court-ordered, military, employment).**

### ALCOHOL USE

11. **Any alcohol-related treatment.**

### FINANCIAL MATTERS

12. **Bankruptcy.**
13. **Wage garnishment (e.g., due for debts, divorce, child support).**
14. **Delinquency more than 120 days on any debt.**
15. **Unusual infusions of assets greater than \$10,000 (e.g., inheritance, winnings, or similar financial gain).**

### WORKPLACE CIRCUMSTANCES

16. **Incidents of Security Concern (IOSCs).**
17. **Waste, fraud, and abuse.**
18. **Property theft.**
19. **Use, possession, transfer, sale, or trafficking of illegal drugs.**
20. **Counterfeit/suspect items.**

## FOREIGN TRAVEL

21. All unofficial/personal foreign travel plans (to any country).  
⇒ To be reported via [DOE F 272.2, Personnel Security Information Report](#), no less than 30 calendar days before travel. (See the [CI website](#) for more information about foreign travel.)
  - If reporting in advance is not possible due to an emergency or unplanned crossings to Canada or Mexico, reporting must be made immediately upon return. Emergency travel also requires verbal notification to management.
  - Keeping a record of all personal foreign travel is recommended as a reference for future clearance (re)investigations.
22. Any of the following, to be reported via [DOE F 272.2](#) upon return from unofficial/personal foreign travel to any country:
  - a) Unplanned interactions with foreign governments, companies, or citizens, and the reasons for the interaction(s), excluding routine travel/tourism-related contacts.
  - b) Unusual or suspicious occurrences during travel, including any of a possible security or counterintelligence significance.
  - c) Foreign legal or customs incidents.
23. Travel to a sensitive country. Also, deviations from sensitive-country travel itineraries.  
**Note:** A list of sensitive countries is available at the [Counterintelligence \(CI\) website](#).
24. Travel to any country where discussions with sensitive-country foreign nationals regarding sensitive subjects are anticipated or have already occurred.  
**Note:** This includes chance meetings where sensitive-country foreign nationals are in attendance.
25. Travel to any country where sensitive subjects will be discussed.

## FOREIGN INTERACTIONS

26. Cohabitation with any foreign national for more than 30 days, regardless of the nature of the relationship.

27. Contact with any known or suspected foreign intelligence entity.
28. Substantive contact\* with any foreign national.  
\*“Substantive contact” refers to a personal or professional relationship that is enduring and involves substantial sharing of information (including personal, business, or research information) and/or the formation of emotional bonds (not to include family members). The phrase also applies to any associations that involve sharing SNL information.
29. Contact with foreign nationals who make requests that could be attempts at exploitation or elicitation.
30. An immediate family member assuming residence in a sensitive country and/or when that circumstance changes (i.e., return to the U.S. or move to any other country).  
**Note:** A list of sensitive countries is available at the [Counterintelligence \(CI\) website](#).
31. Participation in research or talent recruitment programs that are sponsored or managed by China, Iran, North Korea, or Russia.
32. Participation in (e.g., attending, presenting) a virtual event (conference, workshop, seminar, roundtable, etc.) hosted by a foreign entity, either fee or no-fee based. See the [Virtual Event Participation Form](#) at the Counterintelligence website.
33. Participation in other activities (including employment, academic or professional appointments, grant programs, and contracts) sponsored by China, Iran, North Korea, or Russia.

## FOREIGN ACTIVITIES

34. Direct involvement in a foreign business.
35. Opening of a foreign bank account.
36. Purchase of a foreign property (whether located in a foreign country or not).
37. Application for or receipt of foreign citizenship.
38. Application for, possession, or use of a foreign passport or identity card for travel.
39. Voting in a foreign election.
40. Adoption of a non-U.S. citizen child.

## SCI- and SAP-Briefed Personnel

Additional reporting requirements may apply.

- SCI holders are directed to access the [FIE-REX homepage](#) ⇒ “Report It” (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. Determination that a security clearance is no longer required.
- D. Termination of employment under unfavorable circumstances, regardless of the reason for the termination.
- E. Individual’s death.
- F. Failure or refusal to cooperate with authorized an appropriate personnel-security-related requests.

Sandia National Laboratories is a multi-mission 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. SAND2023-112680





# Who and What Can Go Where?



It is **your responsibility** to understand and comply with requirements associated with access to Sandia-controlled premises. Tech areas are geographic designations that do not directly correlate to Security Areas. **Security areas** (e.g., General Access Area [GAA], Property Protection Area [PPA], Limited Areas [LA], Vault-Type Room [VTR]) are physically defined space identified by posted signs and some form of access control, which may contain special nuclear material, classified matter, or property, and which include restrictions on **who and what** may be introduced into these areas. Access to Sandia's security areas requires a **DOE security badge** (except in Public GAAs), and unescorted access to Limited or more restrictive areas requires a **clearance**. Before a **uncleared foreign national** can access DOE sites, information, cyber networks, or technologies (physically or remotely), a **Foreign National Request Security Plan (FNR SP)** that identifies access needs, specific locations being accessed, and identification of authorized hosts, cohosts and escorts must be submitted and approved. For more information, contact the **Foreign Interactions Office** at [fionm@sandia.gov](mailto:fionm@sandia.gov).

WHO	General Access Area (GAA)		Property Protection Area (PPA)	Limited Area (LA)	Vault-Type Room (VTR)
	Public	Non-Public			
DOE Badged, cleared individual	✓	✓	✓	✓	Access list or escort required
DOE Badged, uncleared individual	✓	✓	✓	Escort required	Escort required
Unbadged individual (incl. children)	✓	Only as approved for certain events			NO
Uncleared foreign national	FNR SP may be required	Approved FNR SP REQUIRED prior to access	Approved FNR SP REQUIRED prior to access	Approved FNR SP REQUIRED prior to access. Must be escorted at all times by approved host or escort.	NO

In Sandia's security areas, some items may be restricted from introduction or use. Certain locations within Security Areas may also be marked as **Secure Space**, which is an additional categorization of space *within* a limited or more restrictive area:

WHAT	GAA	PPA	LA	VTR	SECURE SPACE
Sandia-issued laptops	✓	✓	✓	Authorization required prior to introduction	
Sandia-issued controlled articles	✓	✓	Authorization required prior to introduction	Authorization required prior to introduction	
Personally owned controlled articles (except mobile devices and simple items)	✓	✓	NO	NO	
Prohibited articles	NO	NO	NO	NO	
Sandia-managed mobile devices Sandia devices are allowed in a Limited Area outside of Secure Space, including offices	✓	✓	Bluetooth/WiFi disabled	NO	
Personally owned mobile devices Personal devices are only allowed in Limited Area <i>common areas</i> outside of Secure Space	✓	✓	COMMON AREAS ONLY Bluetooth/WiFi disabled	NO	
Medical Portable Electronic Devices	✓	✓	Evaluation & approval required prior to introduction.		

**Controlled Articles** are articles, such as portable electronic devices, both government and personally-owned, which are capable of **recording** information or **transmitting** data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment). Controlled articles may **not** be introduced into a Limited Area and/or Vault-Type Room (VTR) without prior authorization:

**Sandia-issued controlled articles** not already authorized in policy must be registered and approved via the **Controlled Articles Registration Process (CARP)** before being introduced into a Limited Area or VTR. Sandia-issued controlled articles may not be stored in a limited or more restrictive area while awaiting approval.

**Personally owned controlled articles** are **prohibited** from entering a limited or more restrictive unless specifically identified in policy. Personal controlled articles are not eligible for registration and approval via CARP. The only personally owned controlled articles currently authorized in policy are **one-way (non-Bluetooth) vehicle entry key fobs, calculators, one-way pagers, and simple garage door openers**. AM/FM/XM radios, MP3 players, and CD/DVD players are allowed as long as they are **not capable of recording information or transmitting data**.

**Prohibited Articles** are items administratively restricted from being introduced onto Sandia-controlled premises. Prohibited articles (e.g., firearms, dangerous weapons, pepper spray, knives over than 2.5 inches, illegal drugs) are **not allowed** on any Sandia-controlled premises (including parking lots).

**Mobile Devices** include any portable computing device that has a **small, easily carried form factor**; possesses onboard sensors that allow the device to **capture audio or video information**; **does not utilize a desktop operating system** safeguarded by an NNSA Cyber Security Program; is designed to **operate wirelessly**; possesses local, non-removable **data storage**; and is powered-on for extended periods of time with a **self-contained power source**.

Authorized individuals are permitted to bring their mobile devices (e.g., smart phones/tablets) into areas up to and including limited areas with Bluetooth and WiFi disabled, but must not introduce said devices into any location designated/marked as Secure Space. Mobile devices in a limited area **must not be left unattended outside of approved storage**.

**Sandia-managed mobile devices** are permitted anywhere in a limited area not designated/marked as Secure Space, including locations where classified discussions may or may not occur (e.g., offices, touchdown spaces). However, they must be removed and placed in approved storage prior to holding classified conversations.

**Personally owned mobile devices** are only permitted in limited area **common areas** not designated/marked as Secure Space. Common areas include outdoors, break rooms, hallways, and approved storage locations.

**Sandia visitors** are **not allowed to bring their mobile devices into limited areas**. Only Sandia Members of the Workforce and individuals associated with DOE/SFO, Communications & Transport, and Executive Protocol are permitted to bring mobile devices into limited areas.

**Medical Portable Electronic Devices (MedPEDs)** are not permitted within a limited or more restrictive area until approved following an evaluation for **technical security vulnerabilities**. Approved devices may be brought into limited areas only in accordance with mitigations or guidance as provided (e.g., 'Airplane Mode') following the evaluation. Until a MedPED is approved, it is **not authorized** to enter a limited area. Users of MedPEDs and Sandia sponsors should request a **technical review at least 30 days** before access to a limited area is needed.

For more information on obtaining a technical review, contact the **MedPED Team** at [medped@sandia.gov](mailto:medped@sandia.gov) or visit [medped.sandia.gov](http://medped.sandia.gov).



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. SAND2022-10713 O 06.20.2023 v12.0



# Critical Information Lists (CILs)



All Members of the Workforce (MOWs) are responsible for **practicing good OPSEC** (aka operations security) by protecting critical information from inadvertent or intentional release outside of the security boundary, where it can be **exploited by an adversary** intent on harming Sandia, our allies, or our mission.

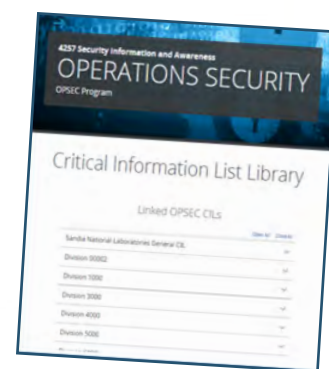
Critical information at Sandia is **specific facts** about friendly intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences of accomplishment of friendly objectives.

At Sandia, critical information must be identified at the programmatic or operational level. The OPSEC program oversees the identification of the critical information and assists MOWs in analysis of factors including risk, consequence of loss, and adversary (e.g., insiders, foreign intelligence entities, violent extremists, etc) intent and capability.

## Using a **Critical Information List (CIL)**

Once identified, critical information is compiled into a **Critical Information List (CIL)**. All approved CILs are published in the [Critical Information List Library](#). You are required to maintain an understanding of all CIL(s) that apply to your work.

A CIL provides any MOW with a concise listing of critical information topics that must be protected against inadvertent or intentional release. A CIL will often include topics that you do not believe are sensitive - if identified on a CIL, that information is **valuable to an adversary** and must be protected. A CIL may also include additional countermeasures against release, such as procedures to prevent sensitive information from being released via aerial imaging during outdoor activities



Review the most current CILs relevant to the work you do by visiting the [Critical Information List Library](#) on the OPSEC homepage on the Sandia Restricted Network (SRN). Without SRN access, request a copy of any appropriate CIL(s) from your manager.

## Protecting critical information as **Controlled Unclassified Information (CUI)**

All MOWs are responsible for identifying and protecting **Controlled Unclassified Information (CUI)**. Government-owned unclassified information that is addressed in a CIL is controlled as CUI according to the Operations Security category, and is marked **CUI//OPSEC**.

When reviewing your information for CUI, any information identified on a CIL for your work is CUI, and **must be protected**. As critical information is CUI, it must be removed prior to publishing or releasing information where it can be exploited by an adversary.

If you encounter information that you believe to be useful to an adversary (e.g., critical information) that is not addressed in a CIL relevant to your work, contact Sandia's OPSEC Program to begin development of a new CIL or to update an existing CIL.



For more information, contact Sandia's OPSEC Program at [opsec@sandia.gov](mailto:opsec@sandia.gov), or visit the OPSEC Program homepage at [opsec.sandia.gov](http://opsec.sandia.gov) on the SRN.



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.

SAND2023-017290 03.29.2023 v1.0





# Getting Started with Classified



## Classification Program Purpose

The purpose of the Classification Program is to *identify* information **classified** under the **Atomic Energy Act or Executive Order (E.O.) 13526**, so it can be **protected against unauthorized dissemination**. **Identifying Classified Information Policy (SS002) and Classified Matter Protection and Control [CMPC] Policy (SS003)** contain much of what you will need to know when working with classified information at SNL.

## Classification Terms

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

**Classified matter** – Any combination of documents and material containing classified information.

**Levels, categories, caveats, and degree of damage** define what protections are needed. As risk increases, so do protection measures required for access to the information and the degree of expected damage due to unauthorized disclosure.

Classification Level	DOE Classification Category and Clearance Level for access				Degree of damage
	Restricted Data (RD)	Formerly Restricted Data (FRD)	Trans-classified Foreign Nuclear Information (TFNI)	National Security Information (NSI)	
Top Secret (TS)	Q only	Q only	Q only	Q only	Exceptionally Grave
Secret (S)	Q only	Q and L	Q and L	Q and L	Serious
Confidential (C)	Q and L	Q and L	Q and L	Q and L	Damage

## Categories of Classified Information

**Restricted Data (RD)** – 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)** – 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)** – 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.

## Working with Classified Information

When working with classified or potentially 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. Work with your **Cyber Security Representative** to identify secure forms of communication.

Information processed on a classified computing system must be marked and protected at the highest potential level, category, and caveat for the information you believe it contains. If unsure, mark as a **"working paper"** at the highest overall potential classification level, category and caveat that the system is approved for (**"System High"**) until it is reviewed by an authorized Derivative Classifier, after which the markings can 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.

**Classification Bulletin GEN-16, REVISION 2, "No Comment" Policy on Classified Information in the Open Literature** addresses concerns regarding documents marked as classified in the open literature. Visit [www.energy.gov](http://www.energy.gov) and search for the Classification Bulletin cited above for more information.

If you see unattended **classified matter**, **SECURE IT** and **REPORT IT** to **SIMP** by calling **505-845-1321**



## Classification Resources

### Derivative Classifier (DC)

An individual **authorized** to confirm an unmarked document or material is unclassified or determine it is classified as allowed by his or her letter of authority.

**Only trained DCs** determine whether documents and 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 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.

### Derivative Declassifier (DD)

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.**

#### Declassification review must occur when 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 RD/FRD/TFNI.
- ◆ 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 that is a permanent historical record that is 25 years old or older.

**You can find a DC or DD using Jupiter ([jupiter.sandia.gov](http://jupiter.sandia.gov)), or by calling 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 determinations. Provide input to classification guidance released by DOE OC. Reviews information intended for public release. You must use the formal Information Review (IR) process if you intend to release information to an uncontrolled, widespread, unknown, or public audience. This includes information intended for release to Congress.

### Classification Challenges

If you think a DC determination is **incorrect**, you have the **responsibility** to challenge the determination. For assistance with challenges, contact the Classification Office:

**NM: (505) 844-5574 / [classificationdept@sandia.gov](mailto:classificationdept@sandia.gov) | CA: [CAClassDept@sandia.gov](mailto:CAClassDept@sandia.gov).**

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



Sandia National Laboratories is a multitechnology 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.

SAND2023-12676 O 02.2023 v2



---

# CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

---

AN AGREEMENT BETWEEN

AND THE UNITED STATES

*(Name of Individual - Printed or typed)*

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, \*952 and 1924, title 18, United States Code; \*the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

*(Continue on reverse.)*

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, \*952 and 1924 of title 18, United States Code, and \*section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001, section 2001.80(d)(2)) so that I may read them at this time, if I so choose.

\* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
-----------	------	---

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS		ACCEPTANCE	
<b>THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.</b>		<b>THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.</b>	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

**SECURITY DEBRIEFING ACKNOWLEDGEMENT**

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

**NOTICE:** The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

# SEC150, *Comprehensive Security Briefing* Completion Record *and* SF 312, *Classified Information Nondisclosure Agreement* Acknowledgment

The Safeguards and Security Awareness program wants you to understand that you must:

**THINK** about the information you access at home or onsite  
**ASSESS** the damage it can cause you, Sandia, or our reputation, and  
**PROTECT** the information every email, meeting, hour of every day.

## By signing below, you:

**Confirm** that you have received, read, and understand your Department of Energy (DOE) security roles and responsibilities for access to classified information or matter or special nuclear material as provided in this booklet; and

**Confirm** that you have received, read, and understand your Sandia-specific security roles and responsibilities as they pertain to Sandia access, information, and activities, as provided in this booklet.

## Additionally, by signing below you:

**Confirm** that you reviewed the obligations outlined for all clearance holders in the SF 312: *Classified Information Nondisclosure Agreement* on the preceding page;

**Acknowledge** that you **must** formally execute the SF 312 prior to being granted initial access to classified matter, information or area (including making a classified visit or holding a cleared badge);

**Acknowledge** that (with regard to your Sandia-sponsored clearance) until you execute the SF 312 you may not:

- Visit any other sites where classified is stored or handled
- Knowingly put yourself in any situation where you have the potential to access classified information or matter
- Knowingly put yourself in any situation where your DOE clearance could be used

Print Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Provide this completion record to [securityed@sandia.gov](mailto:securityed@sandia.gov) to receive credit in the Sandia Training system (TEDS). Note that this pdf booklet meets minimum DOE requirements but that **Sandia MOWs are still required to complete the instructor led-comprehensive security briefing.**

Questions? Contact Security Connection: 505-845-1321 | [security@sandia.gov](mailto:security@sandia.gov)