

SECI50

Comprehensive Security Briefing



Sandia
National
Laboratories

PRESENTED BY

Safeguards & Security
Awareness Program

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.

SAND2020-4482 O

Introduction

Welcome to Sandia National Laboratories (SNL). You are receiving this booklet because your clearance has been granted.

The Safeguards and Security Awareness Program has designed this booklet to provide information required by DOE Order (O) 470.4B, Safeguards and Security Program. As a cleared member of the workforce (MOW) (employee, contractor, or consultant) you may be given unescorted access to security areas and the potential access to classified information, matter or special nuclear material (SNM) and it is essential that you are aware of your SNL site-specific security responsibilities and requirements to understand the important role you play in Protecting What Is Ours.

If you are working at the New Mexico or California site, you are still required to attend a live Comprehensive Security briefing. Contact Security Connection for briefing enrollment questions.

HERE ARE THE TOPICS THAT ARE COVERED IN THIS BOOKLET.

Working At This Laboratory

Control Site Access

Control Security Area Access

Control Information Access

Security Incidents

The Threat Is Real

Resource Documents

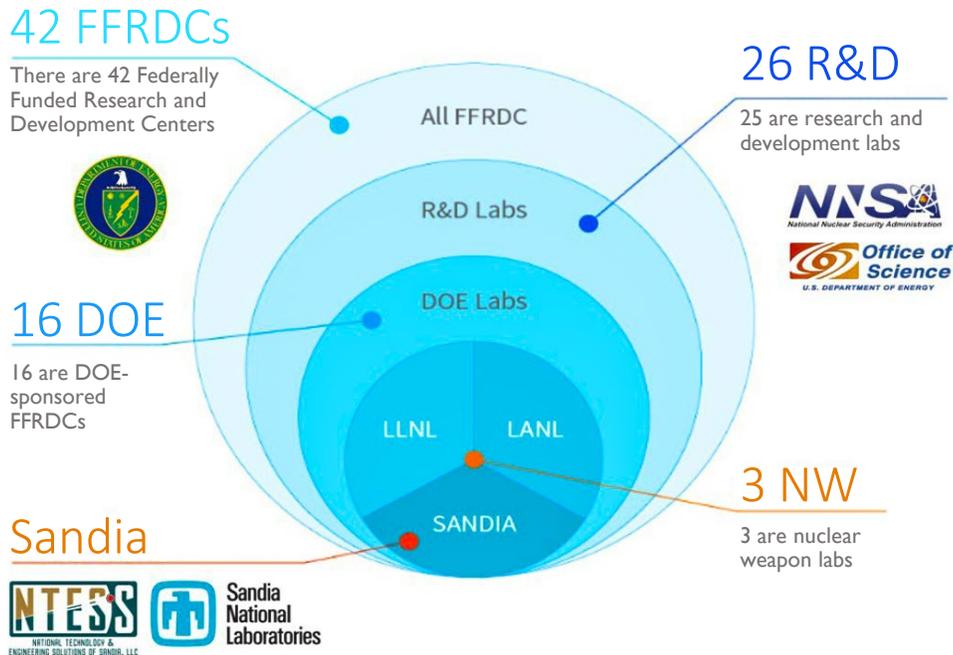
Completion Record

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.

All of us at Sandia National Laboratories look forward to working with you and we hope you are as excited as we are about what we do. **Let's get started.**

Working At This Laboratory

We are all expected to provide **“Exceptional Service In the National Interest.”** In this section, we will cover Sandia’s history, Operations Security, and Need To Know.



Sandia was established early in the Cold War as an FFRDC to help meet the government’s nuclear weapons needs. Sandia’s delivery on its nuclear weapons mission garnered the attention of other agencies and our sponsor, who took note and asked Sandia to expand its program portfolio. Today, the trust inherent to an FFRDC continues to serve as a basis for Sandia’s public service, portfolio, and ongoing success.

The American people have entrusted us to protect very important information, including nuclear, chemical, and biological material; classified matter; and other controlled information.

WE ARE A NATIONAL SECURITY LABORATORY

Part of the world’s most advanced research network.

Crucial to America’s success since 1949.

Pioneering amazing development based on our vast network of technology, brain power, and resources.

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

WE ARE RESPONSIBLE FOR

- | | |
|-------------------|----------------|
| Clean rooms | Sandia foam |
| Hybrid technology | Pulsed power |
| Bio fuels | Nanotechnology |

Our people and our information are at risk everyday.



Working At This Laboratory

Use Operations Security (OPSEC)

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;
make security a part of everything you do.



You leave for work and can't recall if you closed the garage...so you go back and check. Yet we have had 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.



At home, you know the risks and the consequences. Be as diligent at work as you are at home!

Information Must Be Protected

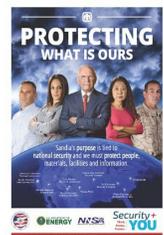
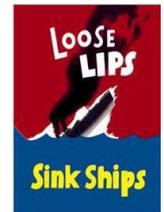
This applies to both classified and unclassified.

Seemingly insignificant bits of information can be combined to build a bigger picture.

YOU MUST HAVE A NEED TO KNOW (NTK)

Need to Know (NTK): The need for the information to do your work.

- You must have a NTK to view any classified or unclassified controlled information (UCI).
- Just because you have a clearance does not mean you have the right to see someone else's information.
- You may have a different need to know than your manager or even your office mate.



This need-to-know mindset will help you protect what is ours.



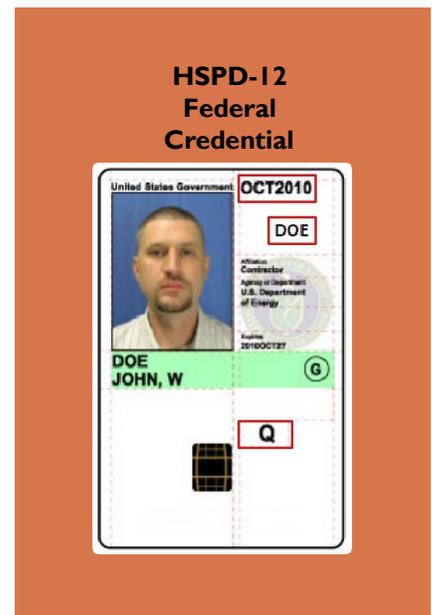
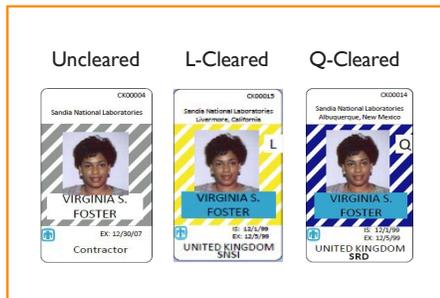
Control Site Access

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 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.

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. Know the limits of what can or cannot be discussed. 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

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 waist
- Over outerwear

RENEW THE BADGE IF:

- Physical appearance significantly changes
- Name legally changes
- Clearance status/level changes
- Badge authorization expires
- Badge becomes faded or damaged

RETURN BADGE:

- When site access is no longer required/authorized (e.g., termination, leave for 90 consecutive calendar days or more)
- As directed by SNL authorities (e.g., SNL Manager, Pro Force, Personnel Security)

DON'T:

- Wear off-site unless at a DOE-affiliated location
- Use as identification for unofficial purposes
- Allow it to be altered/photocopied



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

Report lost or stolen badges immediately to Security Connection.

Control Site Access

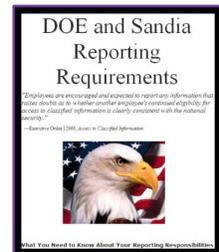
The Department of Energy (DOE) Personnel Security Program establishes requirements that ensure DOE's missions are accomplished in a secure environment by men and women in whom both the Department and the American people may place their complete trust and confidence. All individuals' initial and continued eligibility for security clearances are determined against the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (National Guidelines).

The following could impact your DOE clearance and result in termination.

Careless handling of, failure to protect, or unauthorized disclosure of classified	Allegiance/Foreign preference
Criminal behavior	Falsification/Dishonesty
Alcohol use	Mental illness/condition
Illegal use of a controlled substance	Financial irresponsibility
Gross misconduct	Sabotage/Espionage/Treason

YOUR REPORTING REQUIREMENTS

- Review the pamphlet (see pg. 27)
- Timely reporting is required. Don't be afraid to report
- You can't be coerced or blackmailed if you don't try to hide anything



WASTE, FRAUD, OR ABUSE

Report suspected incidents to Ethics Advisory and Investigative Services.

Ordering 10 replacement parts for a piece of equipment that will never be used, in order to spend year-end funds.	Waste
Submitting an expense report that contains false information.	Fraud
Using a Sandia computer, printer, and telephone for personal business or outside employment.	Abuse



Control Security Area Access

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.

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 I security locked door(s) and protection provided by intrusion alarm system.

General Access Areas

Security Areas

PUBLIC	NON-PUBLIC	PROPERTY PROTECTION AREA (PPA)	LIMITED AREA (LA)	VAULT TYPE ROOM (VTR)
Badge <i>is not</i> required Clearance <i>not</i> required	Badge <i>is</i> required Clearance <i>not</i> required	Badge <i>is</i> required, no PIN Clearance <i>not</i> required	Badge & PIN <i>is</i> required Clearance <i>is</i> required, or must be escorted	Badge & PIN <i>is</i> required Clearance <i>is</i> required
No classified processing	No classified processing	No classified processing	Classified processing/handling	On Access list, or must be escorted Classified processing/handling

INCREASING CONTROL



Control Security Area Access

Escorted Access is required in Limited Areas or above for individuals who do not have the proper **need-to-know** or access authorization (clearance) for that security area.

An **Escort** is an authorized individual having the responsibility to oversee and control people in a security area who do not have the proper need-to-know or access authorizations for the security area.

Escorts must:

- ✓ Be a U.S. citizen.
- ✓ Have a DOE security badge (HSPD-12 or SNL LSSO) with the proper clearance level for the areas being accessed.
- ✓ Be familiar with safety and security procedures for the areas being accessed.

**IT'S ABOUT INFORMATION PROTECTION.
UNTIL A CLEARANCE IS GRANTED, WE CAN'T VALIDATE TRUST.**

**CARE
CUSTODY
CONTROL**

Escorts must:

- ✓ Take measures in advance to prevent compromise of sensitive (classified or unclassified) information.
- ✓ Ensure uncleared personnel have official business or is a Sandia employee or contractor.
- ✓ Escort ratio is 1:8 uncleared individuals. Ratios may only be reduced for security/safety reasons.
- ✓ Observe all requirements of spaces visited.
- ✓ Upon transfer of escorting duty, ensure the new escort accepts responsibility.

DO NOT ESCORT IF YOU'RE NOT COMFORTABLE DOING SO.



When escorting, the escort must wear an "E" card, and the uncleared individual must wear a "U" card.

Call Security Connection if you need help getting these cards.



Control Security Area Access

At all SNL sites additional rules apply to foreign nationals (FNs), including the areas they may visit.

A FN is any person who is not a U.S. citizen, which includes lawful permanent residents/green card holders.

Uncleared foreign nationals require a Foreign National Request (FNR) Security Plan (SP) **before** they are granted access to Sandia Labs or its information.

A **FNRSP** is specific to each FN who requires any of the following:

- Access to any SNL controlled premises (after-hours access may be requested)
- Access (cyber) to SNL's computing or information technology (IT) resources
- Access to SNL/DOE information that is not publicly available
- Access to a DOE/SNL facility or officially sponsored attendance at a DOE/SNL event offsite to discuss a sensitive subject or Export Controlled Information

Uncleared FNs must:

- ✓ Have an approved Foreign National Request (FNR) Security Plan (SP)
- ✓ Access only the areas listed on the FNR SP
- ✓ Know who the hosts and escorts are on the FNR SP



Escorting, Tailgating, Vouching, and System Overlapping

ESCORTING

Action taken by an authorized individual to oversee and control people within a security area who do not have the proper need to know or access authorization for that area.

TAILGATING

Action taken by an individual to avoid established security protocols (e.g., badge swipe) by following another individual into a security area without that individual's knowledge. This term is not synonymous with piggybacking.

VOUCHING

Visually verifying the access authorization of another person for the purpose of granting them entry into a security area. The person being vouched is described as piggybacking

Note: Per Laboratory Process SS008.I, Site Access, **vouching is only allowed at vehicle gates**, not at pedestrian access-control points (gates, turnstiles, doors etc.) or facilities equipped with automated access controls.

- SS008.I conveys detailed instructions that must be performed when vouching at vehicle gates.

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

You can help Sandia protect what is ours by understanding that each security area has different requirements for what you can or cannot bring in.

Controlled articles: items not allowed within limited or more restricted areas without **prior authorization**. These are “gadgets” that can record, transmit, or have a data port, and therefore are capable of compromising information.

One type of controlled articles are Portable Electronic Devices (PEDs). Anyone visiting or working on Sandia premises must adhere to IT004, *Manage Controlled Electronic Devices and Media Policy*, such as knowing and understanding the features of any device before bringing it on to Sandia-controlled premises, and ensuring you follow the rules for the specific security area you will be entering (e.g., turning off Bluetooth and WiFi). Review the policy and/or PEDs.Sandia.gov to review the rules and restrictions before bringing any device onto Sandia premises (Sandia Restricted Network [SRN] access required). If you do not have SRN access, call Security Connection.



EXAMPLES OF CONTROLLED ARTICLES

Cell phones
Digital picture frames

Recording equipment
iPods/iPads

Cameras
Wearable electronics

Prohibited articles: items prohibited at all Sandia-controlled premises because they can produce substantial injury to persons, damage property, or are prohibited by law.

EXAMPLES OF PROHIBITED ARTICLES

Explosives
Alcohol
Firearms

Controlled substances (e.g., illegal drugs, paraphernalia)
Hazardous radiological, chemical, or biological materials

If you escort or host visitors or uncleared persons, be sure to ask if they are carrying any controlled or prohibited articles before entering security areas. PEDs are not allowed in Vault Type Rooms (VTRs, formerly known as Closed Areas), Special Access Program Facilities (SAPFs), and Sensitive Compartmented Information Facilities (SCIFs).

You are responsible for consequences if they bring a controlled or prohibited article into a Limited or more restricted security area.

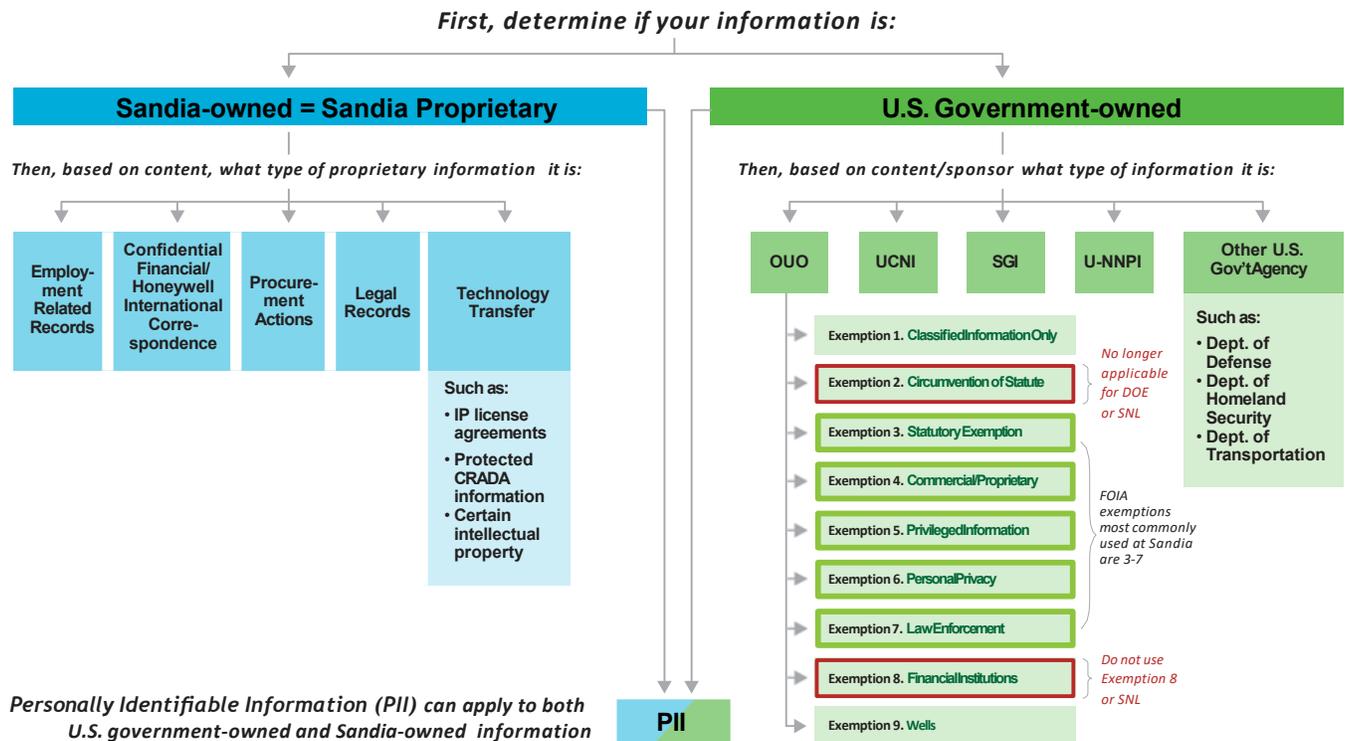
Call Security Connection for questions on what is or isn't allowed, or to report failure to comply.



Control Information Access

All Members of the Workforce are responsible for controlling information access. This is done by first knowing how to identify the information so you can properly protect, use, disseminate, and dispose of it. In this section we will cover Identifying, Protecting and Controlling Unclassified Controlled Information (UCI).

UCI: Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security, Sandia National Laboratories, or our business partners.



Note: Exemption 2 is obsolete for DOE & SNL. If you find a document that is marked Exemption 2, you don't need to remark it, but if you extract any of the information from that document you will need to mark your information with a new exemption that applies.

Make a conscious determination of the sensitivity of the information throughout its life cycle. Safeguard all information created or collected in support of official business in a manner consistent with the sensitivity of the information.

You are responsible for determining what type of information you generate.

Control Information Access

Members of the Workforce must comply with applicable contracts, laws, and regulations to manage and protect Official Use Only (OUO) information so that Sandia may use these resources with integrity to better serve the nation.

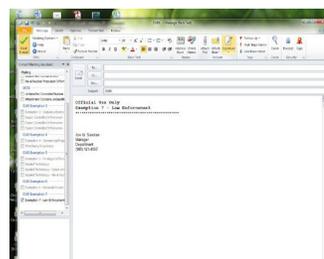
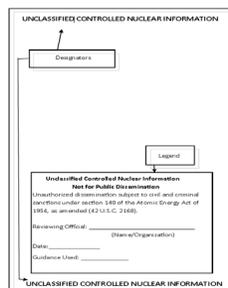
OUO is U.S. Government-owned unclassified controlled information that may be exempt from public release under the **Freedom of Information Act (FOIA)** and has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities. Your Derivative Classifier should have classification guides that include OUO topics relevant to your organization's work. Members of the Workforce should identify which subjects, programs, processes, documents, emails, presentations, faxes, or any other format within your organization or programs have the potential to include OUO information. All OUO information falls under at least one of eight FOIA exemptions (exemptions 2 through 9). Here are some examples of FOIA exemptions:

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

Email: Email containing UCI must also be protected and properly marked. Some types of UCI require use of an approved encryption method such as Entrust or FIPS 140-2 methods.

Sandia has an internal UCI email marking assistant tool to help properly mark emails sent internally as well as emails sent outside the Sandia.gov domain. Contact Corporate Computing Help Desk (CCHD) for assistance (505) 845-2433.

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



Control Information Access

You are responsible for Identifying UCI to help protect, control and prevent unauthorized access to that information. Here are some important responsibilities.

Marking	Storing	Communicating
<p>DOCUMENTS/MATTER</p> <p>Use proper markings to correctly store and protect information</p>	<p>IN A GAA</p> <p>Keep information in an individual locked office, suite, or receptacle</p>	<p>DOCUMENTS/MATTER</p> <p>Use proper markings to correctly store and protect information</p>
<p>EMAIL MESSAGES</p> <p>Mark and encrypt according to the information's protection requirements</p>	<p>IN A PPA</p> <p>Keep information in an individual locked office, suite, or receptacle</p>	<p>EMAIL MESSAGES</p> <p>Mark and encrypt according to the information's protection requirements</p>
<p>FAXES</p> <p>Use cover sheets to alert the recipient that the information needs to be protected</p>	<p>IN A LIMITED AREA</p> <p>Lock up OUO Ex 6. Turn over to display a blank sheet if UCNI</p>	<p>FAXES</p> <p>Use coversheets to alert the recipient that the information needs to be protected</p>
<p>Use the right UCI marking to ensure the integrity of that marking is not degraded</p>		<p>Keep UCI out of sight from individuals who do not have a NTK</p>

Any Member of the Workforce who purposefully circumvents OUO protections risks administrative penalties ranging from reprimand to loss of employment.

CIRCUMVENTIONS INCLUDE:

- Intentional release of OUO information to a person who does not have Need To Know (NTK).
- Intentional or negligent release of an OUO marked document to a person who has no NTK.
- Intentionally not marking a document known to contain OUO information.
- Intentionally marking a document as OUO that does not contain OUO information.

Errors in identifying OUO information is not a Security Incident Management Program (SIMP) reportable incident unless those errors result in the loss of Export Controlled Information (ECI).

Sandia offers **OUO101** to help you with identifying, marking, protecting, disseminating, disposing of all Unclassified Controlled Information.



Control Information Access

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.

CLASSIFIED INFORMATION

Information that is classified by a statute or executive order.

CLASSIFIED MATTER

Any combination of documents and material containing classified information.

CLASSIFICATION LEVELS

These identify the degree of damage that could be done to national security due to unauthorized disclosure of this information. Classification categories are types of information as defined in statutes or Executive Orders.

Access to classified information is:

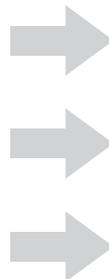
- compartmented to prevent harm to national security, if lost.
- restricted to persons with a security clearance and a **“need-to-know.”**



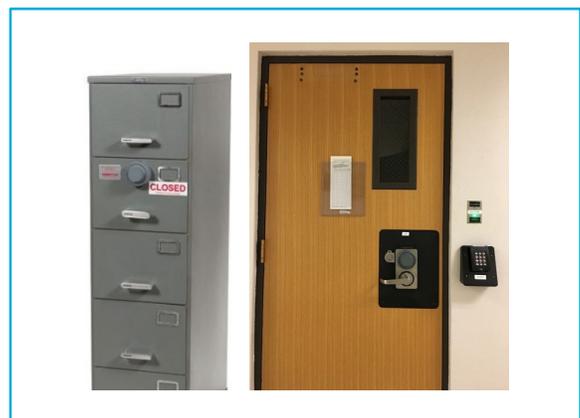
1948: Truman establishes civilian control of the nuclear arsenal. *“I do not want to have some dashing lieutenant colonel decide when would be the proper time to drop one.”*

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

CLASSIFIED



GSA-APPROVED STORAGE REPOSITORIES (SAFES/VTRS)



Control Information Access

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 determine that a document, equipment, or material is unclassified or classified based on classification guidance or source documents, as allowed by his or her description of authority.

DERIVATIVE DECLASSIFIER (DD)

An individual authorized to declassify or downgrade Sandia-originated document, equipment or material in specified areas as allowed by his or her description of authority. DDs are located in the Classification Office.

CLASSIFIED ADMINISTRATIVE SPECIALIST (CAS)

An individual trained to mark, store, duplicate, destroy, and move (e.g., mail, ship, fax, hand carry, receive) classified matter.

CLASSIFICATION OFFICE

Your local Classification Office is available to help with classification topics not handled by your DC, DD, or CAS. They are also there to help resolve any disagreements about a DC determination.

DOE OFFICE OF CLASSIFICATION

If a challenge cannot be resolved locally, the Classification officer will submit a challenge in writing to the DOE Director, Office of Classification. Anyone has the right at any time to submit a challenge directly to the Director, Office of Classification. Under no circumstances is the challenger subject to retribution or repercussions for making a classification challenge.

Outreach@hq.doe.gov.

Use Sandia's "Jupiter" website to find your DC or DD.

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 that an employee believes may contain classified information

An existing, marked document or material that 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)

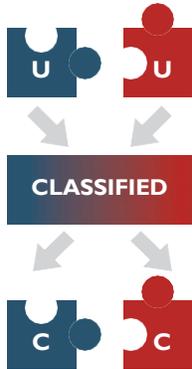
Printed output from a classified information system

Document or material generated in a classified subject area and intended for public release (e.g., for a publicly available web page, for news organizations), including documents provided to or testimony given to Congress



Control Information Access

It is everyone's responsibility to prevent loss of classified information, by understanding the risks of association and compilation and the consequences of mishandling classified information.

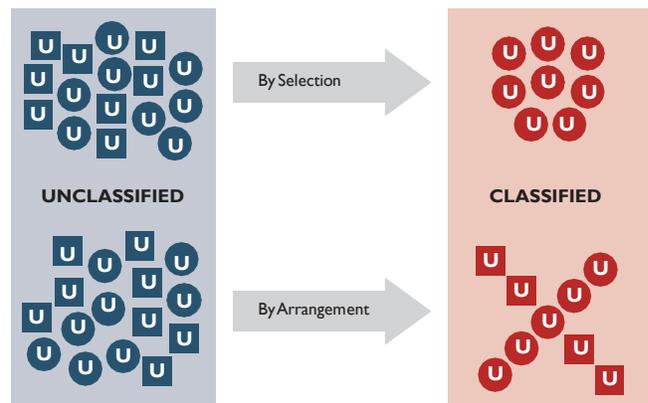


ASSOCIATION

Combining **different** “unclassified” elements can create a “**classified**” statement. When separated, the information stays classified.

COMPILATION

Combining **similar** “unclassified” elements, by selection or arrangement can create a “**classified**” document.



Understand DOE's “No Comment” Policy

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.

When in doubt, don't bring any attention to it.

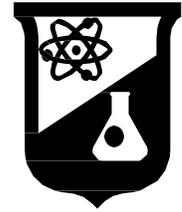


Control Information Access

Sandia sites may have Special Nuclear Material (SNM), which is fissile material that is especially useful in nuclear weapons. 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 SNM is an attractive target, there are strict requirements as to where it can be used or stored and who has access to it.

If you work with SNM, you'll receive additional training, because SNM requires specific protections.



Your Commitment to Protect

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

Here are some things to know about the SF-312:

- DOE holds on to the SF-312 form for 50 years.
- It is a contract between you and the U.S. Government.
- You agree to protect classified information from **unauthorized disclosure**.

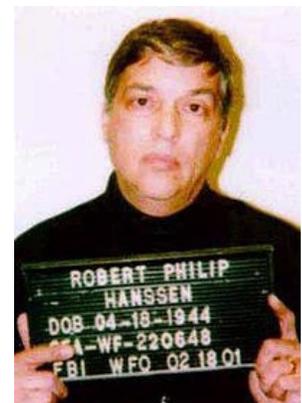


UNAUTHORIZED DISCLOSURE

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 regarding classified could result in:

- Termination.
- Civil and criminal penalties as outlined in the SF-312, *Classified Information Nondisclosure Agreement*.



Security Incidents

Sandia supports a culture of timely reporting, which helps mitigate ongoing threats and lessens the potential for compromise of sensitive (classified and unclassified) information. The **Security Incident Management Program (SIMP)** inquires into all potential security incidents at all sites.

Timely reporting of security incidents is an important aspect of identifying security risks and preventing, limiting, or mitigating the consequences of unintentional release of Sandia and DOE information.

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.

Some things you would report

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

Unauthorized Portable Electronic Devices (e.g., w/Bluetooth, or around classified)

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

Improper Storage/Protection of Classified (e.g., safe left open, password in desk)

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

SIMP will:

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

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

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.

TASK DEMANDS	INDIVIDUAL CAPABILITIES
Time pressure	Unfamiliarity w/task /first time evolution
High workload	Lack of knowledge
Simultaneous, multiplerequests	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
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

RECOGNIZE WHEN YOU'RE AT RISK AND TAKE A MOMENT.

Reduce Your Risk

Self-check before entering a Limited Area

Secure your work area every time you walk away

Talk to your family about Sandia’s security rules

Know your Security Professional

Call Security Connection with questions

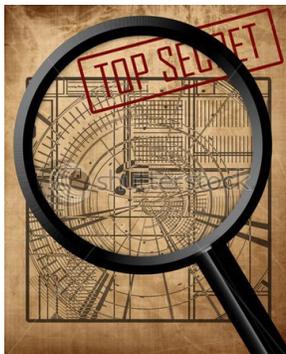


The Threat is Real

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.



Sandia's Office of Counterintelligence relies on the trust and cooperation of alert Members of the Workforce (MOW) to counter these threats to U.S. national security, to the reputation of Sandia National Laboratories, and to the livelihood of each and every MOW.



THE COUNTERINTELLIGENCE PROGRAM IS DESIGNED TO:

- Counter the efforts of enemy spies
- Counter threats posed by terrorists/Homegrown Violent Extremists (HVEs)
- Conduct investigations and analysis
- Maintain U.S. Intelligence Community liaison
- Protect you

FOREIGN VISITORS TO SANDIA SITES

come from all over the world, including but not limited to:

Armenia	Pakistan
Bangladesh	Russia (Former Soviet Union)
Egypt	People's Republic of China
France	Republic of Korea (S. Korea)
India	Saudi Arabia
Iraq	Turkey
Israel	Taiwan
Japan	Ukraine
Kenya	Uzbekistan
Kyrgyzstan	Venezuela

TARGETS FOR FOREIGN SERVICES

Clearance Holders

Anyone with access to:

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



The Threat is Real

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 targeting methods used 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



Real-Life Examples

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.



CYBER **SPEAR-PHISHING**

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



INSIDER **GLENN DUFFIE SHRIVER**

- US civilian/student studying in China
- Recruited and paid by the PRC for his "expertise"
- Department of State and CIA Applicant
- Active 2004-2010
- Sentenced in 2011 to four years in prison

The Threat is Real

Real-Life Examples



SEXSPIONAGE/HONEY TRAP

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



INSIDER

ROY OAKLEY

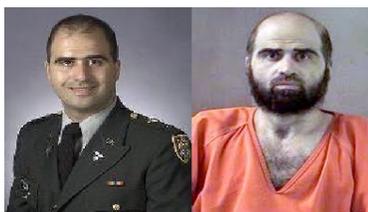
- DOE – East Tennessee Technology Park
- Stole restricted nuclear materials
- Attempted to sell the materials to France
- Active at least 2006 – 2007
- Sentenced in 2009 to six years in prison for unlawful Disclosure of Restricted Data under the Atomic Energy Act



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 information to Venezuela
- Active 2007-2009
- Sentenced in 2015 to five years in prison



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



ROBIN SAGE

- A fictional person created to show how social media can be deceiving
- Social media profiles were created under this alias with photo borrowed from another website and job title “Cyber Threat Analyst”
- In less than a month, ‘she’ amassed nearly 300 social-network connections, receiving offers to consult with companies like Google and Lockheed Martin



The Threat is Real

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:

- Foreign travel to sensitive countries
- Current substantive interactions with a foreign national
- Financial or property interests in a foreign country
- Foreign honoraria, gifts, expenses paid
- Unsolicited/suspicious contact (emails/calls/face-to-face)
- Unusual/suspicious behavior

Substantive Interaction

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

Counterintelligence Resources

- Monthly newsletters
- Spy of the Month articles
- CI monthly calendars
- Periodic tidbits
- Education/preparation
- Provide foreign visit host briefings/debriefings
- Provide foreign travel briefings/debriefings (professional or personal)



For more information:

505-284-3878 | CI-HELP@SANDIA.GOV



Resource Documents

You're just about done.

Now that you have downloaded and read through the booklet the following documents should be reviewed and used as resource material to help you understand the importance of your roles and responsibilities.

For credit, see [instructions on the Completion Record](#).

DOE & Sandia Reporting Requirements

Understanding The Clearance Process

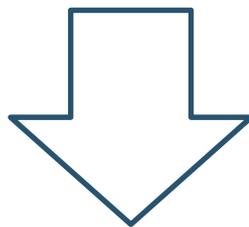
Who & What Can Go Where

SNL Critical Information List

Getting Started With Classified

SF-312 Classified Information Nondisclosure Agreement (do not sign)

[Completion Record \(last page\)](#)



Other Reporting Requirements

Incidents of Security Concern; i.e., Security Incidents	Report immediately, but do not provide details over the phone . NM: Security Connection (321) CA: Security Connection (321) or SIMP (925-294-2600) TTR: Central Alarm Station (702-295-8285) Note: Contractors must also report incidents to their Facility Security Officers.
Waste, Fraud, & Abuse (WFA)	Report incidents of WFA and criminal matters to Ethics Advisory & Investigative Services (505-845-9900) and other appropriate authorities (e.g., manager, security officials). Alternatively, for WFA incidents, you may email the Office of Inspector General directly, or call 800-541-1625.
Counterfeit/Suspect Items	Upon discovery of suspect or counterfeit items, report the circumstance or submit questions to sgasci@sandia.gov , or via counterfeit.sandia.gov .
Theft of Property	Immediately report any theft of Sandia or U.S. Government property to Property Management (loststolen@sandia.gov). Note: All property that is considered stolen, lost, or missing must be reported regardless of value and regardless of whether it is considered controlled or uncontrolled property.
Wrongdoing	Report incidents of wrongdoing to Ethics: 505-845-9900. Note: <ul style="list-style-type: none"> • Incidents of wrongdoing are not limited to items listed elsewhere herein. • You may also report directly to the Office of Inspector General information about wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, other recipients of DOE financial assistance, or their employees.
Drug Use	Report the following to Ethics at 505-845-9900: <ul style="list-style-type: none"> • Positive drug test results (regardless of source [e.g., court system and military testing]) • Incidents of illegal drugs in the workplace. This includes trafficking in, selling, transferring, possessing, or using illegal drugs. Note: <ul style="list-style-type: none"> • Illegal drugs are prohibited on Sandia-controlled premises and KAFB property. • The use of illegal drugs—or legal drugs in a manner that deviates from medical direction—is a serious offense and could result in termination of your clearance and your employment, as well as arrest.

Fold here

DOE and Sandia Reporting Requirements

What You Need to Know About Your Reporting Responsibilities



Revised: January 28, 2019

"Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

— Executive Order 12968, Access to Classified Information

Managers

Managers are responsible for immediately reporting to Personnel Security (NM: 505-845-9355, CA: 925-294-1358) when an employee's clearance is no longer required, employment is terminated, individual is on extended leave of 90 calendar days or more, or access authorization is not required for 90 calendar days or more. Ensure DOE F 5631.29, *Security Termination Statement*, and badges are immediately delivered to the Clearance Office.

Remote Sites Personnel

Report to SNL/NM, unless otherwise indicated.

SCI- and SAP-Briefed Personnel

Contact the appropriate Special Security Officer or Program Security Officer for guidance regarding program-specific reporting requirements.



Sandia National Laboratories

SAND2009-0424P



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

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 that an individual is eligible for access to classified information. An access authorization is an administrative determination that an individual is eligible for access to particular types or categories of classified information or material. Unless otherwise indicated, the term "security clearance" encompasses access authorizations throughout this briefing.

No individual will be provided access to classified information or Special Nuclear Material (SNM) unless that individual has 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 Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), National Security Information (NSI), or Special Nuclear Material. In determining such eligibility, DOE may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. Generally, DOE issues Top Secret, Secret, and Confidential security clearances, and Q and L access authorizations.

An individual's eligibility is based on the completion of a personnel security investigation conducted for DOE by the Office of Personnel Management (OPM), the Federal Bureau of Investigation (FBI), or other federal agency authorized to conduct background investigations.

ADJUDICATION

Security clearance determinations are based on information acquired through the investigation conducted on the applicant or employee or otherwise available to personnel security officials.

All individuals' initial and continued eligibility for security clearances are adjudged against the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (National Guidelines). Where the Cognizant Personnel Security Office (CPSO) has no information related to any of the areas of concern identified in the Guidelines, either from the report of investigation or from other sources, a favorable determination must be made. Where the CPSO has information related to any areas of concern identified in the Guidelines, either from the report of investigation or from other sources, such information will be regarded as derogatory and create a question as to the individual's security clearance eligibility. If questions as to the individual's security clearance eligibility can be favorably resolved in accordance with the processes and considerations set forth in the Guidelines, the appropriate security clearance must be granted or continued.

The adjudication process is the careful weighing of a number of variables, known as the whole person concept, utilizing the National Guidelines. In evaluating the relevance of an individual's conduct, the CPSO will assess the disqualifying and mitigating conditions outlined in the National Guidelines, which take the following factors into account:

- 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

DUE PROCESS: When applicants and employees are determined to not meet the standards for access to classified information, the CPSO initiates the Administrative Review procedures to deny or revoke a security clearance, as set forth in 10 CFR 710. These procedures are established to ensure that an individual is afforded full due process in a manner consistent with traditional American concepts of justice and fairness.

References: Executive Order 12968, Access to Classified Information (dated 8-7-95); Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Adjudicative Guidelines (dated 12-29-04); Title 10, Code of Federal Regulations, part 710 (10 CFR 710), Criteria and procedures for Determining Eligibility for Access to Classified Material or Special Nuclear Material; DOE Order 472.2, Personnel Security (dated 7-21-11); DOE O 475.1, Counterintelligence Program (dated 12-10-04)

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



Who and What Can Go Where?

SS008 - Control Access to Information and Facilities Policy

At Sandia, Tech Area or Technical Area is used to designate certain geographical areas at our sites. Security Area refers to a physically defined space (identified by posted signs and some form of access control). **Controlled Articles** are devices that have the potential to record and/or transmit information with or without authorization. The Controlled Article Registration Process (CARP) application is used for registering controlled articles that will enter a Limited Area (or higher). **Prohibited Articles** are items that not allowed anywhere on Sandia controlled premises that are likely to produce injury or damage to persons or property. Report unauthorized articles on Sandia controlled premises to Security Connection.

WHO	General Access Area		Security Area		VAULT TYPE ROOM (VTR) Badge & PIN is required
	PUBLIC Badge is not required	NON-PUBLIC Badge is required	PROPERTY PROTECTION AREA (PPA) Badge is required	LIMITED AREA (LA) Badge & PIN is required	
Q-cleared individual (SNL LSSO badge or DOE HSPD-12 credential)	✓	✓	✓	✓	✓ Access list or escort required
L-cleared individual (SNL LSSO badge or DOE HSPD-12 credential)	✓	✓	✓	✓	✓ Access list or escort required
Uncleared individual (SNL LSSO badge)	✓	✓	✓	✓ Escort required	✓ Escort required
Children / Friends	✓	Only as approved for certain events			NO
Uncleared foreign national	✓	A Foreign National Request Security Plan (FNR SP) may be required before working with an uncleared foreign national. FNR SPs list areas they may access. For additional guidance contact the Foreign Interactions Office (505-844-8263).			

WHAT					
AM/FM radio	✓	✓	✓	✓	✓
Electronic medical device capable of recording or transmitting data	✓	✓	✓	✓	✓ Reporting required
Sandia-owned PEDs (includes blackberries, iPads, and iPhones)	✓	✓	✓	✓	*NO
Sandia-owned camera	✓	✓	✓	✓ Register with CARP	✓ Register with CARP
Non Sandia-owned Portable Electronic Devices (PEDs) (includes personal, business, & other government agency)	✓ **	✓ **	✓ **	Rules and restrictions apply	*NO
Personal weapons/Alcohol	Prohibited Article				
Marijuana (medical, extracts such as CBD, etc.)	Prohibited Article				
Someone else's prescription medication	Prohibited Article If your drug test indicates the presence of a prescription medication, and you cannot produce a valid prescription in your name, you will be subject to disciplinary action (e.g., termination of employment).				

* Laptops and other electronic devices may be allowed in VTRs under certain circumstances. Contact the VTR owner for more information.

** Some areas of a GAA or PPA may not approved for PEDs. Always be aware of local signage before leaving your device anywhere.

Sensitive Compartmented Information (SCI) and Special Access Program (SAP) facilities have their own rules and restrictions. Contact the POC for that facility for more information.

Comply with all posted local (such as facility-specific) restrictions and control measures for controlled devices and media.



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-15422 O | 01/2020 v5



CALL SECURITY CONNECTION AT 505-845-1321



Sandia National Laboratories Critical Information List (CIL)

Sandia National Laboratories critical information applies to all sites.

The site (or organizational) OPSEC Coordinators can disseminate site-specific critical information. If the release of critical information can cause harm to Sandia National Laboratories’ programs, activities, personnel, customers, or assets, then it must be protected from inadvertent and unauthorized disclosure, even if it is not on this or any other CIL. Sites and organizations (divisions, centers, departments, sub-contractors, and/or programs) should use this list as a baseline for developing and maintaining their own CIL.

Critical Information: Specific facts about friendly (e.g., U.S., SNL) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

PROGRAMS AND ACTIVITIES:

New or established programs that present a target to adversaries, including but not limited to classified, sensitive, and unclassified programs, and those programs that fall into applicable governmental sensitive technology lists.

The table below is the CIL and used for SNL programs and activities.

CRITICAL INFORMATION LIST (CIL)		
Applications of new technology	Diagrams, blueprints, and schematics	Program/project and personnel relationships
Capabilities and limitations	Emergency response and procedures	Purchasing/procurement, vendors, shipping, and receiving requests
Communication methods, user name/ passwords	Facilities and infrastructure	Scope and type of work conducted
Critical job details, roles, and responsibilities	Financial, budget, accounting, and contract information	Shipment details for sensitive materials
Current and future operations	Network information	Travel and conference details, travel requests and reports
Dates, times, locations, and events (tests, exercises, etc.)	Plans, publications, and procedures	Work schedules and staffing changes/ reports, milestones

Disclaimer: Critical Information listed here may not be all inclusive. Programs and activities should review their CIL on a recurring basis. For assistance contact the OPSEC Program Office.

IMPORTANT NOTICE: A printed copy of this document may not be the document currently in effect. Contact the OPSEC Program Office at OPSEC@sandia.gov or 505.844.OPSEC(6773).



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. SAND2018-11284 M | 2018 10 01



CALL SECURITY CONNECTION AT 505-845-1321



Getting Started with Classified

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

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

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

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

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

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

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

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

Protecting and Controlling Classified Information and Matter (SS003, Classified Matter Protection and Control)

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

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

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



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-7610 O | 07.2019 v6



CALL SECURITY CONNECTION AT 505-845-1321



Getting Started with Classified

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.

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 (either a formal, or a programmatic review) for:

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

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

DDs are located in the Classification Office.

Declassification review must occur when document or material is:

- Prepared for declassification in full.
- Prepared as redacted versions.
- Requested under statute or Executive Order (i.e., declassification for public release).
- Referred to DOE by other government agencies that are marked or identified as potentially containing RD/FRD/TFNI or DOE NSI equities.

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

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

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

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

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

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

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

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



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.



CALL SECURITY CONNECTION AT 505-845-1321



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
----------------	-------------------

THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.

SIGNATURE	DATE
-----------	------

NAME AND ADDRESS (Type or print)

THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.

SIGNATURE	DATE
-----------	------

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.

Completion Record

SEC150 Comprehensive Security Briefing Completion Record

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.

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.

Acknowledge that you cannot access classified information or matter or special nuclear material at any site until you have been granted a clearance and executed an SF-312 Classified Information Nondisclosure Agreement.

**Members of the Workforce who, on a regular basis, will be physically accessing Sandia New Mexico (SNL/NM) or California (SNL/CA) must attend a live briefing. You can enroll via the Sandia Restricted Network (SRN) using the TEDS Training System. Otherwise, email SecurityEd@sandia.gov to request a schedule of available briefings.*

***Live Briefings are currently suspended at Sandia National Laboratories sites. You will receive guidance if you will be required to attend one at a later date.**

Print full name: _____

Signature: _____

Date: _____

The Safeguards and Security Awareness program wants you to understand that it is important for you to:

THINK about the information you access at our sites,
ASSESS the damage it can cause you and Sandia, and
PROTECT the information every hour of every day.

Provide this completion record to securityed@sandia.gov to receive credit in the Sandia TEDS Training system. You will then receive instructions for execution of the SF-312 Classified Information Nondisclosure Agreement and steps to obtain your cleared site specific badge.



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-12518 TR



CALL SECURITY CONNECTION AT 505-845-1321

