WHO	General Access Area		Security Area			
	Public Badge **is not** required	**Non Public** Badge **is** required	**Property Protection Area** Badge **is** required	**Limited Area** Badge & PIN required		**Vault-Type Room** Badge & PIN required
	No Classified Processing				Secure Space	
Q-cleared person with badge	✓	✓	✓	✓	✓	✓ Access List or Escort
L-cleared person with badge	✓	✓	✓	✓	✓	✓ Access List or Escort
Uncleared citizen with badge	✓	✓	✓	✓ Escort Required	✓ 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	No Classified Processing				Secure Space	
Sandia owned laptops with full operating systems	✓	✓	✓	✓	✓	NO, Unless Authorized
ANY Mobile devices	✓	✓	✓	✓	NO	NO
Simple electronic devices	✓	✓	✓	✓	✓	✓
Controlled Articles (that are not mobile devices)	✓	✓	✓	✓ CARP Required	✓ CARP Required	✓ CARP Required
Medical Devices	✓	✓	✓	✓	✓	✓ Must notify
Prohibited Articles (weapons, drugs, alcohol)	NO	NO	NO	NO	NO	NO

Mobile Device Restriction in 'Secure Space'

You are responsible for understanding the capabilities of any device you plan to introduce into Sandia-controlled premises. Any device (whether Sandia, government or personally owned) that meets the definition of Mobile Device is not permitted in Secure Space. **Any introduction of such a device is immediately reportable to SIMP.**

Other devices

Sandia owned laptops operating full versions of Sandia's common operating environment (COE) are exempt from mobile device restrictions. **Controlled Articles** that do not meet the definition of mobile device must be registered through CARP. **Medical devices that are not mobile devices are not impacted by mobile device restrictions.**

SEC050: Initial Security Briefing

Sandia National Laboratories (All Sites)

Revised February 2021

Security + YOU
Think. Assess. Protect.

This **Initial Security Briefing** provides a concise overview of security responsibilities, and is intended for all individuals accessing Sandia National Laboratories (SNL)

Mission and Program Areas of Sandia National Laboratories

Our unique responsibilities in the nuclear weapons (NW) program create a foundation from which we leverage capabilities, enabling us to solve complex national security problems. As a multimission national laboratory and federally funded research and development center (FFRDC), Sandia accomplishes tasks that are integral to the mission and operation of our sponsoring agencies by:

- Anticipating and resolving emerging national security challenges
- Innovating and discovering new technologies to strengthen the nation's technological superiority
- Creating value through products and services that solve important national security challenges
- Informing the national debate where technology policy is critical to preserving security and freedom throughout our world

Major program areas include defense, nonproliferation, climate, infrastructure, homeland security, counter-terrorism, cybersecurity, and nuclear weapons.

Safeguards and Security Program Responsibilities

The Safeguards and Security Program is responsible for access control, physical protections, information protection, protective force, education and awareness, security incident management, classification, classified matter protection and control, operations security, and international security operations.

Secure Space and Mobile Devices

Mobile devices are prohibited from entering any Secure Space.

A **Secure Space** is any location at SNL where classified processing can be expected to occur. Secure Space is exclusively located within a Limited or more restrictive area, and is delineated at its boundaries by red, white and blue signs.

A **Mobile Device** is defined as any portable *computing* device that: has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g. wirelessly transmit or receive information); possesses local, non-removable data storage; is powered-on for extended periods of time with a self contained power source. Examples include cell phones, tablets, smart watches, fitness trackers and other electronic devices.

Controlled and Prohibited Articles

Controlled Articles are items that are controlled because of their potential to record or transmit information without authorization. Examples include recording equipment, electronic equipment with a data exchange port capable of being connected to automated information system equipment or radio frequency transmitting equipment (including Bluetooth and cellular devices). These articles are required to be registered through the Controlled Articles Registration Process (CARP) prior to introduction into Limited or more restrictive areas. Government-owned computers procured through SNL's JIT purchasing system are exempt from CARP.

Prohibited Articles are items that are not allowed anywhere on Sandia-controlled premises. Prohibited articles include items that are illegal, or likely to produce injury or damage to persons or property. Examples include dangerous instruments or materials; alcohol or other intoxicants; illegal drugs and paraphernalia; firearms, weapons, explosives or incendiary devices.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-13333 O v6

Sandia National Laboratories

Protection of Unclassified Controlled Information (UCI)

- Access to **Unclassified Controlled Information (UCI),** which includes **Official Use Only (OUO)** and **Unclassified Controlled Nuclear Information (UCNI)** may be given to a person who needs it to perform his/her duties (need to know) and must be properly marked, stored, and protected. Access to UCI does not require a clearance. For further guidance contact ***Security Connection.***
- **Personally Identifiable Information (PII)** should always be protected and limited to official business. For further guidance, contact ***Security Connection.***

Protection of Classified

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

Access to **classified matter** is restricted to persons with a both a valid ***access authorization*** (aka security clearance) and a "***need to know***". All classified matter is subject to specific requirements for identification, use, protection, dissemination and disposal. Classified markings must be clearly affixed to each piece of material or page indicating category and level of sensitivity. When transmitting, use **secure** forms of telecommunication (classified fax machine and other electronic transmissions).

When working with classified information, only use computers on **approved classified networks** (e.g., Sandia Classified Network [SCN]) or an approved stand-alone system. For guidance on classified computing, contact your ***Cyber Security Representative or 3CSi (505-284-3274).*** Follow appropriate marking and protection requirements at all times, even on classified systems.(e.g., mark 'system high' until reviewed by an authorized **Derivative Classifier [DC],** then update the marking as necessary).

Releasing Information Outside SNL

Get a formal review. If you intend to release information to an uncontrolled, widespread, unknown, or public audience, the information must go through the formal **Review and Approval (R&A)** process. This includes information intended for release to Congress. For further guidance, contact ***Security Connection.***

Security Notice

- Misuse or theft of SNL or Government equipment (e.g., computers, vehicles) could be considered **"waste, fraud, and abuse"** and may be a punishable offense.
- All individuals are **subject to search** of their persons, hand-carried items, and vehicles upon entering or leaving Sandia controlled premises.
- Do not park in unauthorized areas (e.g., reserved, handicap, security).
- Follow all posted speed limits (if not posted, the speed limit is **15 mph**).
- Use of **tobacco products** is not allowed on Sandia-controlled premises.
- Comply with all gate entry protocols (e.g., staffed, automated, vehicle, military).

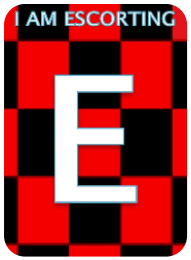
Sandia-Controlled Site Control Access

Access to Sandia National Laboratories (SNL) is controlled by DOE authorized badges. The most common are cleared DOE PIV (aka **HSPD-12**) credentials and cleared/uncleared Local Site Specific Only (**LSSO**) badges. Badges identify the holder's clearance status, which in turn identifies the types of information and areas the individual may access.

Sandia Members of the Workforce and visitors **MUST NOT VOUCH** others into pedestrian access control points (turnstiles, gates, doors, etc.).

Everyone **MUST swipe or present his/her badge** at each access control point when entering buildings, rooms and other security areas.

Sandia Controlled Escorting Procedures



- Persons under **escort** must always remain with their escort in Limited or more restricted areas. **Escorts must be appropriately cleared and badged U.S. citizens** who are familiar with Sandia safety and security-related laboratory procedures that apply to the areas being accessed.
- While escorting, escorts and uncleared individuals must display the red and black **"U" and "E"** cards along with their authorized badges (pictured).
- **Uncleared** foreign nationals require a **Foreign National Request Security Plan (FNRSP)** which identifies who is authorized to escort the foreign national and the areas approved for access. These individuals can be readily identified by bright red LSSO badges. For further guidance, consult your ***manager or Deployed Security Professional.***

Badge Procedures/Best Practices

- Your badge is **government property**; return it when your employment is terminated, clearance status changes, or it is no longer needed.
- Badge must be worn conspicuously, photo side out, above the waist and front of your body.
- Remove or obscure badge from visual access when not on SNL/DOE premises.
- **Do not use your badge as means of identification** for unofficial purposes,
- Protect your badge against **loss, theft, misuse or alteration**.
- Report **lost or stolen badges** to ***Security Connection***

REPORTING
CONCERNS
INCIDENTS
EMERGENCIES

Security Concerns, Incidents and Questions, call Security Connection. Available 24/7/365
321 from any Sandia landline phone, or **505-845-1321** from any other phone
Emergencies, alarms and life-threatening situations, call 911 from any Sandia landline phone
In SNL/NM, **505-844-0911** | In SNL/CA, **925-294-2222**
Report non-emergencies, call 311 from a Sandia phone or **505-844-0311** or **505-845-0311**