Sandia National Laboratories

S&S-PLN-120, NON-POSSESSING SUBCONTRACTOR SECURITY REQUIREMENTS PLAN

SUBCONTRACTOR CERTIFICATION

Revision Date: October 2018

This plan summarizes the security responsibilities for *(insert company name and address below)***:**

Company Name:

_____

Company Address:

Street: _____

City: _____ State: _____

Zip Code: _____

The provisions of the subcontract(s) with Sandia National Laboratories (SNL) do not authorize the above-named company to receive, store, transmit, or originate classified information within the subcontractor's facility(ies) or place of business. However, performance of work will require personnel to hold DOE personnel security clearances for access to classified information and/or special nuclear material (SNM) at SNL and/or other approved DOE facilities. The purpose of our Non-Possessing Subcontractor Security Requirements Plan (SRP) is to flow down SNL and DOE security requirements to our subcontractor and lower tier subcontractor population. The SRP should serve as a reference when questions about security arise. I understand that the above-named company is responsible for ensuring that all personnel involved in SNL subcontracts, including company managers, employees, and direct consultants, as well as any lower-tier subcontractors whose employees require DOE personnel security clearances, comply with all applicable SNL and DOE security requirements.

Facility Security Officer Certification:

As the designated Facility Security Officer, I accept responsibility for ensuring company compliance with applicable SNL and DOE security policy, including the specific requirements in the SRP.

Facility Security Officer Name	**Facility Security Officer Signature**
Facility Security Officer Telephone Number	**Date**

Key Management Personnel Certification:

As the Key Management Personnel representative, I certify that the Facility Security Officer has been given the authority, resources, and other management support needed to ensure company compliance with all applicable SNL and DOE security requirements. When a new Facility Security Officer is appointed, the company agrees to immediately notify the SNL Contract Security Management Program to execute a new SRP.

Key Management Personnel Name	**Key Management Personnel Signature**
Key Management Personnel Telephone Number	**Date**

S&S-PLN-120 — NON-POSSESSING SUBCONTRACTOR SECURITY REQUIREMENTS PLAN

Responsible Program Representative: Delvin Wood (4226)

Issue Date: 08 April 2013

Revision Date: 02 October 2018

IMPORTANT NOTICE – A printed copy of this document may not be the document currently in effect. The official version is in the S&S Controlled Document Library, located on the Sandia restricted network (SRN).

CONTENTS

1.0 INTRODUCTION 4
1.1. Overview 4
1.2. Ownership and Oversight 2
2.0 PROGRAM MANAGEMENT OPERATIONS 3
2.1. Protection Program Management 3
2.1.1. *Program Management and Administration 3*
2.2. S&S Planning & Procedures Management Control 3
2.2.1. *Self-Assessment Program 3*
2.2.2. *Issue Resolution 4*
2.2.3. *Incident Reporting and Management 5*
2.3. Program-Wide Support 6
2.3.1. *Foreign Ownership, Control or Influence (FOCI) 6*
2.3.2. *Facility Approval and Registration of Activities 7*
2.3.2.1. Key Management Personnel 8
2.3.2.2. Personnel Security Clearances 9
2.3.2.3. Facility Data and Approval Record 9
2.3.2.4. Contract Security Classification Specification 9
2.3.2.5. DOE Facility Clearance Suspensions 10
2.3.2.6. DOE Facility Clearance Terminations 11
2.3.3. *Facility Clearance Reporting Requirements 11*
2.3.3.1. Reporting Significant Changes 11
2.3.3.2. Reporting Anticipated Changes 12
2.3.3.3. Reporting Other Changes 13
2.3.4. *Security Management in Contracting 13*
3.0 PERSONNEL SECURITY 15
3.1. Validating Persons of Interest 15
3.2. DOE Security Badges 15
3.2.1. *Badge Types 15*

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No SAND2021-11672 O.

3.2.2. *Badge Request Process* *16*
3.2.3. *Picking Up Badges* *17*
3.2.4. *Returning Badges* *17*
3.3. DOE Personnel Security Clearances 18
3.3.1. *Clearance Action Requests* *19*
3.3.2. *Clearance Action Applicant Tasks* *20*
3.3.3. *Clearance Action FSO Responsibilities* *20*
3.3.4. *U.S. Citizenship* *21*
3.3.5. *Subcontractor Personnel Reviews* *21*
3.3.6. *Clearance Termination* *23*
3.3.7. *Clearance Withdraw* *24*
3.3.8. *Clearance Suspensions, Revocations and Denials* *24*
3.3.9. *Impact to Clearance During a Leave of Absence (LOA) of 90 Calendar Days or More* *24*
3.3.10. *Clearance Reinvestigations* *25*
3.4. Classified Visits 25
3.4.1. *SNL Outgoing Classified Visits* *25*
3.4.2. *SNL Incoming Classified Visits* *25*
3.5. Unclassified Visits and Assignments by Foreign Nationals 26
3.5.1. *Onsite SNL Work* *26*
3.5.2. *Off-Site SNL Work* *26*
4.0 ALCOHOL, DRUGS AND TOBACCO AT SNL 27
4.1. Substance Testing Types and Requirements 27
4.2. Medical Marijuana 28
4.3. Use of Legal and Valid Prescription Medications 28
4.4. Alcohol Testing 29
4.5. Subcontractor Personnel Responsibilities 29
4.6. FSO Responsibilities 29
4.7. Consequences 30
5.0 SAFEGUARDS AND SECURITY AWARENESS 30
5.1. Security Briefings 30
5.1.1. *Initial Security Briefing (SEC050)* *30*
5.1.2. *Comprehensive Security Briefing (SEC150)* *31*
5.1.3. *Annual Security Refresher Briefing (SEC100)* *32*
5.1.4. *Security Termination Briefing (SEC225)* *32*
5.2. Classified Information Nondisclosure Agreement 32
5.3. DOE/SNL – Individual Reporting Requirements 33
5.3.1. *Other Reporting Requirements* *33*
5.3.2. *Reporting Counterintelligence Interests* *33*
6.0 SAFEGUARDS & SECURITY TRAINING PROGRAM 34
7.0 INFORMATION SECURITY 35

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No SAND2021-11672 O.

7.1. Classified Information 35
7.2. Classification Office 36
7.3. Classified Matter Protection and Control 37
7.4. Unclassified Information 37
7.4.1. *Personally Identifiable Information (PII)* 38
7.4.2. *Official Use Only Information* 38
7.5. Operations Security 39
8.0 PHYSICAL SECURITY 39
8.1. Security Areas 39
8.2. Automated Access Control 41
8.3. Vehicles in Limited Areas 41
8.3.1. *Personal Vehicles* 41
8.3.2. *Subcontractor Vehicles (Construction/Maintenance and Service/Delivery)* 42
8.4. Controlled Articles 42
8.4.1. *SNL-Owned Electronic Devices* 42
8.4.2. *SNL-Owned Computer Media* 42
8.5. Prohibited Articles 43
8.6. Personally Owned Portable Electronic Devices (PEDS) 43
9.0 INTELLIGENCE WORK 44
9.1. Physical Security 44
9.1.1. *Security Areas* 44
9.1.2. *Controlled Articles/Portable Electronic Devices* 44
9.2. Information Security 44
9.2.1. *Classification Guidance* 44
9.3. Personnel Security Program 45
9.3.1. *General Requirements for DOE Personnel Security Clearances* 45
9.3.2. *DOE Personnel Security Clearance Types and Access* 45
9.3.3. *DOE Security Badges* 45
9.3.4. *Polygraph Designated Positions* 45
9.3.5. *Personnel Security Clearance Suspension, Revocation and Denial* 45
9.4. Safeguards & Security Awareness 46
9.4.1. *Reporting Requirements* 46
9.5. Cyber Security 46
10.0 REFERENCES 46
10.1. External Source (Requirements) Documents 46
10.2. Related Documents 46
11.0 RELATED TOOLS & RESOURCES 47
ACRONYMS A-1
DEFINITIONS B-1
CHANGE HISTORY CH-1

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No SAND2021-11672 O.

1.0 INTRODUCTION

1.1. OVERVIEW

Sandia National Laboratories (SNL) is a multi-mission laboratory operated by National Technology and Engineering Solutions of Sandia LLC (NTESS), a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's (DOE) National Nuclear Security Administration (NNSA) under contract DE-NA0003525. SNL has major research and development responsibilities in nuclear deterrence, global security, defense, energy technologies and economic competitiveness. SNL main facilities are located in Albuquerque, New Mexico (SNL/NM) and Livermore, California (SNL/CA).

SNL is responsible for complying with, and flowing down, the DOE Contractor Requirements Documents incorporated into its contracts with subcontractors at any tier and extent necessary to ensure compliance with DOE Directives. This plan reflects the security requirements that are being flowed down to all tier non-possessing subcontractor companies, hereinafter referred to as company, subcontractor, lower-tier subcontractor or facility, performing work under subcontract to SNL.

In accordance with the DOE Acquisition Regulation (DEAR) Clause, Section 952.204-73(e), a subcontractor that will not possess or handle classified matter or nuclear material at the subcontractor's place of business, but will require DOE personnel security clearances for the subcontractor's personnel to perform work at other cleared facilities, must be processed for a DOE Facility Clearance (FCL) and be designated as a "non-possessing" facility. Per DOE requirement, this Security Requirements Plan (SRP) must be executed to cover the non-possessing subcontractor's security responsibilities. Non-possessing companies are not approved to possess, discuss, or computer process classified information at their physical locations. Subcontractor personnel are prohibited from working on classified subject areas from home, or other locations that have not been approved by SNL or a federal government entity for classified work. No classified work, or access to security areas where classified work is performed, shall begin until the subcontractor company has received notification of approval from SNL Contract Security Management (CSM).

The purpose of this SRP is to define requirements and procedures the subcontractor and its personnel must abide by for all U.S. Government support service subcontracts to obtain DOE personnel security clearances. When subcontract terms specify that performance of work under a SNL subcontract require personnel to hold DOE personnel security clearances for access to classified information, special nuclear material (SNM), or unescorted access to SNL security

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND No SAND2021-11672 O.

areas at approved DOE facilities, subcontractor personnel must comply with the requirements of the DOE facility (e.g., SNL) at which they are performing the work.

It is the responsibility of subcontractor personnel to be aware of, and comply with, all applicable SNL rules and requirements (e.g. SNL's security policy, ES&H policy, ES&H manual, and other site-specific requirements). Subcontractor personnel with Sandia Restricted Network (SRN) authorization have access to SNL's policies and procedures. Subcontractor personnel without SRN authorization may obtain SNL's policies and procedures from their SNL manager or Sandia Delegated Representative (SDR). The company is responsible for ensuring that all of its personnel including company managers, employees, direct consultants, and any lower-tier subcontractors whose employees require DOE personnel security clearances are provided appropriate training to satisfy all applicable security requirements of the SNL facility, to include requirements within this plan.

If subcontractors violate DOE policy and/or security requirements, that subcontractor must contact their respective SNL management representative, Subcontracting Professional (SP), SDR and CSM immediately to report the violation.

In addition to the requirements in this plan, any subcontractor, low-tier subcontractor, or sub-agreement involving approved safeguarding of Restricted Data or other classified information, must also comply with DOE regulations in 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*. Any provisions included in the special terms and conditions of an award must also be treated as requirements for compliance.

The company and Facility Security Officer (FSO) are obligated to adhere to the requirements and procedures within this plan upon signatures of an authorized company representative and the FSO. Questions about the requirements relayed in this plan may be directed to SNL CSM via email at farateam@sandia.gov.

1.2. OWNERSHIP AND OVERSIGHT

This plan applies to all non-possessing subcontractors and any lower-tier subcontractors performing work under a SNL subcontract. The SNL CSM Team manages this plan, and with assistance from the Safeguards and Security (S&S) Program subject matter experts (SMEs), maintains, reviews, and updates the plan as necessary.

2.0 PROGRAM MANAGEMENT OPERATIONS

2.1. PROTECTION PROGRAM MANAGEMENT

2.1.1. *Program Management and Administration*

The overall day-to-day security responsibility for the subcontractor facility rests with the appointed company FSO. The company shall appoint an FSO in writing[1]. The FSO must be a U.S. citizen, an employee of the company, and must obtain and maintain a DOE personnel security clearance commensurate with the FCL. The FSO is assigned the responsibility of administering the requirements of the S&S Program at their facility. The FSO will supervise and direct security measures necessary for implementing and administering the requirements of the S&S Program within his or her facility. The FSO is instrumental in making sure that personnel are aware of security procedures and practices, regardless of whether they have access to classified information or other DOE security interests.

The FSO ensures personnel are aware of, and comply with, SNL security procedures and requirements outlined in this plan as well as the standards set forth in the attached references.

2.2. S&S PLANNING & PROCEDURES MANAGEMENT CONTROL

2.2.1. *Self-Assessment Program*

Surveys, self-assessments, and review programs are conducted to ensure that S&S systems and processes at contractor facilities are operating in compliance with SNL and DOE/NNSA policies and requirements for the protection of security assets and interests. These programs provide the means for timely identification, as well as the correction of deficiencies and noncompliant conditions to prevent adverse events. These programs also validate the effectiveness of corrective actions implemented to address identified deficiencies.

Contractor companies holding FCLs are required to review their security programs, by conducting continuous self-assessments to monitor and evaluate organizational activities for compliance with security requirements. To ensure that the company is following security requirements, CSM will conduct a periodic security review to ensure plan compliance. A schedule will be developed and conducted by CSM to ensure that no changes have occurred to information previously submitted by the company. CSM will communicate the results of the review with the FSO, SDR and applicable S&S SMEs.

---

[1] If a facility is under Defense Security Service (DSS) cognizance, the DSS Industrial Security Representative will facilitate the appropriate training requirements. Companies who hold an active U.S. Department of Defense (DoD) facility clearance are not required to complete additional training; however, the appointment or documentation of the appointed FSO may be required.

Sandia Contractor Review and Evaluation (SCORE) is a SNL corporate tool for evaluating subcontractor performance. CSM may utilize SCORE to evaluate subcontractor implementation and compliance of SNL security requirements based on the periodic security review.

2.2.2. *Issue Resolution*

Subcontractors that are out of compliance with any conditions or requirements are given a short time frame to comply. Failure to comply within the required timeframe may result in termination of the company's FCL, which may impact the company's ability to meet the subcontract Statement of Work. All actions taken to resolve matters will be coordinated with the SDR and SP.

The table below describes the issue and escalation process if the subcontractor is out of compliance with any conditions or requirements. This includes the company being non-responsive to requests for information. The purpose of this process is to ensure company compliance with requirements, and to ensure that issues are tracked to resolution so that problems do not adversely impact the mission. Full compliance is expected within the maximum time specified and starts at the initial notice. The time specified in the request may vary based on the complexity, risk and/or severity of the request, as determined by SNL. If the expected time for resolution exceeds, or is not received by, the requested date, an escalation process will be initiated for each request. The escalation process below describes how SNL will raise each issue of concern to a higher level of management for resolution, particularly when resolution cannot be reached at the subcontractor level.

Notification	Notification/ Distribution To:	Consequences
Initial	FSO	Correspondence outlining requirements and importance of compliance and reporting of issue via SCORE process. Advised that if action is not taken within the maximum time allowed, the 2nd notice (as described below) will result in notification to the SDR and SP.
2nd	FSO, SDR and/or SP	Correspondence outlining requirements and importance of compliance; request to SDR and SP to address matter with FSO; second notice via SCORE; advised that if action is not taken within the maximum time allowed, the 3rd notice (as described below) will result in notification to the Contractor Senior Management Official (CSMO), SDR and SP for action and possible suspension or termination of the DOE FCL.
3rd	FSO, CSMO, SDR and/or SP	Correspondence outlining requirements and importance of compliance; request to CSMO, SDR and SP to address matter with FSO; reporting in SCORE; advised that if action is not taken within the maximum time allowed, the 4th notice (as described below) will result in suspension or termination of the DOE FCL.
Final	FSO, CSMO, SDR and/or SP	Notification, at the discretion of the SP and/or S&S, to suspend or terminate the DOE FCL.

2.2.3. *Incident Reporting and Management*

Incidents of Security Concern (IOSC), also referred to as security incidents, are events that are of concern to the DOE S&S Program, that warrant a formal inquiry by the SNL Security Incident Management Program (SIMP) and subsequent reporting of the incident to DOE.

Security incidents include a range of possible actions, inactions, or events that:

- Pose a threat to national security interests and/or DOE assets.
- Create potentially serious or dangerous security situations.
- Have a significant effect on the S&S Program's capability to protect DOE S&S interests.
- Indicate the failure to adhere to security procedures.
- Illustrate the system is not functioning as designed, by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

Subcontractors and any lower-tier subcontractors should strive to avoid and prevent security events, incidents, and adverse impacts to national security. It is required to immediately report the following:

- Security incidents (see: DOE and Sandia Reporting Requirements)
    - For SNL/NM, contact the Security Incident Reporting Pager at 505-283-SIMP (7467).
    - For SNL/CA, contact the CA Inquiry Official (IO) at 925-294-2600.
    - For SNL/ NM or SNL/CA, contact SNL Security Connection at 321 from a SNL phone, or 505-845-1321 from a non-SNL phone.
- Incidents involving intelligence information or occurring inside a Sensitive Compartmented Information Facility (SCIF)
    - Contact the SNL Field Intelligence Element (FIE) hotline at 505-284-4724.
    - For SNL/ NM or SNL/CA, contact SNL Security Connection at 321 from a SNL phone, or 505-845-1321 from a non-SNL phone.
- Real or suspected foreign intelligence-gathering efforts
    - This event should be reported to both the SNL Security Incident Reporting Pager for SNL/NM, or the CA IO for SNL/CA, and the SNL Office of Counterintelligence.
        - For SNL/NM, contact the Security Incident Reporting Pager at 505-283-SIMP (7467).
        - For SNL/CA, contact the CA IO at 925-294-2600.
        - SNL Office of Counterintelligence 505-284-3878.

Note: Foreign intelligence-gathering efforts may include elicitation, eavesdropping, bag operations, electronic interception, etc., and may be encountered within the United States or when on foreign travel.

The SNL IO will lead and organize the inquiry to gather specific information about the IOSC. The FSO and subcontractor personnel are responsible for:

- Preserving and protecting evidence related to an incident at the appropriate classification level and category.
- Cooperating with the IO to include providing requested documents, materials, or information relevant to the inquiry.

If an incident occurs at any of the SNL Remote Sites (Kauai Test Facility, Tonopah Test Range, Weapons Evaluation Test Lab or Washington, D.C., Office), contact the SNL/NM SIMP Office and the SNL Remote Site FSO to report. Do not discuss details of the incident via telephone, alphanumeric pager, email, or voice-mail. A SIMP IO will contact the reporting individual to obtain additional information.

If necessary, instructions for onsite sanitization will be provided to the FSO or the site manager with notification back to SIMP upon completion. In some circumstances computers and or hard drives may have to be sent to SNL/NM for appropriate actions. Dependent on the severity of the event, SNL/IO's may be required to travel to the respective site to facilitate the inquiry.

2.3. PROGRAM-WIDE SUPPORT

2.3.1. *Foreign Ownership, Control or Influence (FOCI)*

The purpose of the Foreign Ownership, Control or Influence (FOCI) Program is for CSM and DOE to evaluate the foreign involvement of a subcontractor company being considered for award of a SNL subcontract that requires personnel security clearances. A FOCI determination is required for any subcontractor company when personnel of the business structure require DOE/NNSA personnel security clearances to perform on the subcontract. The objective of the FOCI Program is to obtain information that indicates whether the proposed subcontractor or contractor companies are owned, controlled, or influenced by a foreign person/entity, and whether the potential for an undue risk to the common defense and national security may exist as a result.

A company is deemed to be operating under FOCI when a foreign interest has the power to direct or decide matters affecting the management, or operations, of the company in a manner that may result in unauthorized access to classified information, or in a manner that may adversely affect the performance of classified subcontracts. The foreign interest power may be, direct or indirect, and/or may potentially be exercised or exercisable. SNL will generally not sponsor subcontractors under FOCI to the extent mitigation is required. Exceptions may be made if the company has a unique capability (e.g., equipment, facilities, patents, skills). Exceptions are determined by SNL, in coordination with DOE. Mitigation under Defense Security Service (DSS) is not always transferable.

A favorable FOCI determination along with a granted FCL and an approved Contract Security Classification Specification (CSCS) form allows a non-possessing subcontractor company to request personnel security clearances for their employees. A FOCI determination is not required for individuals who are not affiliated/associated (through employment, ownership, or other representation) with any company, university, or other form of business. An individual must be

processed for a FCL when:

- They are doing business as a company formally registered with an Employer Identification Number.
- One or more employees require personnel security clearances.
- Classified matter will be retained at his/her physical place of business.

DOE has an electronic system for submission of FOCI information to CSM and DOE. FSOs must use this system for the submission of FOCI packages, including changes to update their FOCI information. CSM assists the FSO with completing a FOCI packet to allow for DOE to review and make a FOCI determination. The FOCI website may be accessed at https://foci.anl.gov/doesub/. CSM will invite the FSO to create an account to utilize the electronic system.

FSO FOCI Responsibilities

- The FSO will submit FOCI packages online through the FOCI website. In all FOCI activities, the company shall provide complete information to enable DOE to ascertain the attendant risk, including, but not limited to, accurate and complete submission of the Standard Form (SF) 328, *Certificate Pertaining to Foreign Interests*, and information provided during periodic security reviews and review activities. The FSO must ensure that all changes that might affect the FOCI determination are reported to CSM before they occur.
- The FSO must submit a separate FOCI package for each tier parent located in the United States, Puerto Rico, or a U.S. possession or territory. The parent must have a FCL at the same, or higher, level as the subsidiary. However, DOE will determine the necessity for the parent to be cleared or excluded from access to classified information.
- The FSO must maintain all records pertaining to FOCI, including records such as original signatures on the SF 328, and make such records available upon request to SNL and/or DOE.
- The FSO must adhere to periodic security review and certification information when requested.
- The FSO must complete a new FOCI package when changes have occurred, or when directed to do so by CSM.

Note: If a facility is under DSS cognizance, the DSS Industrial Security Representative will facilitate the FOCI process. Companies who hold an active U.S. Department of Defense (DoD) facility clearance through the DSS are not required to complete a separate FOCI package for DOE.

2.3.2. *Facility Approval and Registration of Activities*

Subcontract companies must have a legitimate need for a FCL in connection with a U.S. government subcontract. Once a procurement need (subcontract) has been established by a SP for work requiring personnel security clearances, the SNL CSM Program is responsible for facilitating DOE's review and approval of a subcontractor's eligibility for a FCL. CSM oversees the FCL process from initial issuance through termination based on procurement need, and monitors the subcontractors continued eligibility.

CSM ensures that all tiered subcontractors and tiered parent organizations authorized to obtain personnel security clearances for SNL have been granted and maintain the appropriate DOE FCL.

A FCL is an administrative determination that a facility (including an appropriately sponsored subcontractor) is eligible to access, receive, produce, use, and/or store classified matter; this includes nuclear materials, other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, and/or DOE property of significant monetary value. This plan applies to all non-possessing subcontractors and any lower-tier subcontractors performing work under an SNL subcontract. Non-possessing companies are not approved to possess, discuss, or computer process classified information at their physical locations. Once DOE has made the determination that a subcontractor facility is eligible for access, the facility is required to maintain that eligibility throughout the lifetime of their FCL.

Facility Security Clearance Components:

1. Subcontract requiring personnel clearances
2. Favorable FOCI determination
3. FSO designation and training
4. Key Management Personnel (KMP) security clearances (executives, FSO etc.)
5. Security Requirements Plan
6. Ongoing Assessments

The DOE FCL shall not be used for advertising or promotional purposes. Any personnel security clearances and badges associated with the FCL shall be used for operational efficiency consistent with contractual obligations.

2.3.2.1. Key Management Personnel

All company officials who occupy positions which have the authority to affect the organization's policies or practices in security activities conducted under the subcontract, as determined by the DOE cognizant security office, must be designated as KMP. At a minimum, KMP must include the senior management official responsible for all aspects of subcontract performance and the designated FSO. In order for a company to be granted a DOE FCL, specified KMP must be granted DOE personnel security clearances. At the discretion of DOE/NNSA, an interim FCL can be granted after a favorable FOCI determination and personnel security clearance requests are in process for KMP.

KMP requiring personnel clearances are determined on a case-by-case basis by DOE/NNSA. KMP must obtain and retain their DOE personnel security clearance at the level of the DOE FCL or formally be excluded from classified access. DOE/NNSA will determine KMP not required to obtain a personnel security clearance and be excluded from access to classified information to be disclosed to the company.

Note: If a subcontractor is under DSS cognizance, the DSS Industrial Security Representative will determine those KMP that must be cleared. Those KMP will obtain DoD clearances and are

not required to obtain DOE clearances unless there is a DOE contractual need requiring the designated KMP to possess a DOE clearance.

2.3.2.2. Personnel Security Clearances

All subcontractor and lower-tier subcontractor personnel performing classified work under a SNL subcontract must be granted a DOE personnel security clearance. Subcontractor personnel security clearances must be requested and granted under their employer's FCL. Tier subcontractors must possess a separate FCL under which personnel security clearances are requested and granted.

2.3.2.3. Facility Data and Approval Record

The purpose of the DOE F 470.2, *Facility Data and Approval Record (FDAR)*, is to document the approval or termination of the facility clearance, company information and approved classified access levels. DOE registers the facility approval by entering the Facility Data and Approval Record (FDAR) into the DOE S&S Information Management System (SSIMS). The FOCI determination and issuance of the FDAR ensure that the subcontractor is eligible for DOE personnel security clearances.

SNL will provide the FDAR to the FSO when the facility is approved and throughout the lifecycle of the FCL to include any changes. It is the FSO's responsibility to retain the FDAR and ensure that any changes or inaccuracies are reported to CSM for update/correction.

Although the DOE F 470.2 is the official DOE record, SNL has amended the form to conform to SNL site specific standards. The SNL FDAR e-form is likewise utilized as a representation for DOE F 470. 2. Either version can be provided to the FSO or company representative upon request.

2.3.2.4. Contract Security Classification Specification

DOE F 470.1, *Contract Security Classification Specification (CSCS)*, is used to register security activities (i.e., subcontracts) while also disclosing security and classification guidance for the information to be disclosed.

SNL is responsible for incorporating appropriate security requirements clauses in the SNL Request for Quotation (RFQ) or other solicitation, and for providing subcontractor personnel with the security guidance needed during the performance of the subcontract. The CSCS form is, by reference (see Clause 610FO, "Security Requirements"), part of the subcontract and is binding. The subcontractor company is required to adhere to the security specifications outlined in the CSCS and this plan.

Subcontractors who further subcontract are responsible for flowing down the security clauses and requirements in a contractually binding manner. In addition, the lower-tier subcontractor must be issued a contract requiring personnel clearances, then a CSCS form must be submitted specifically reflecting the lower-tier subcontract and will need to be approved by CSM prior to personnel clearances being issued.

The SDR is responsible for submitting a CSCS to register the authorized subcontract requiring DOE personnel security clearances. Upon review and approval by SMEs (e.g. Classification Analyst, Derivative Classifier etc.), CSM registers the security activity by entering the CSCS into SSIMS. Registration of the classified subcontract in SSIMS ensures that subcontractor personnel working on a subcontract are eligible to be processed for DOE personnel security clearances.

Although the DOE F 470.1 is the official DOE record, SNL has amended the form to conform to SNL site specific standards. The SNL CSCS e-form is likewise utilized as a representation for DOE F 470.1. Either version can be provided to the FSO or company representative upon request.

2.3.2.5. DOE Facility Clearance Suspensions

A DOE FCL will be suspended if:

- The subcontractor is out of compliance with any conditions or requirements of maintaining a FCL.
- The subcontractor is determined to be under FOCI, and it has not been mitigated. Subcontract performance on activities involving proscribed information must not continue until all applicable FOCI requirements are met.
- Findings or other deficiencies in a survey, self-assessment, periodic security review, inquiry, inspection or evaluation indicate suspension of a FCL is necessary by SNL/DOE/NNSA. SNL will determine whether the DOE FCL must be suspended pending validated corrective actions.
- Any action occurs that negates the company's favorable FOCI determination.
- The subcontractor is out of compliance with FOCI mitigation plans.
- The subcontractor fails to comply with personnel security requests.
- The subcontractor fails to flow down security requirements to their lower-tier subcontractors.
- The subcontractor fails to comply with the requirements within this plan.
- Actions, such as a merger or buyout, affect the ownership status of the subcontractor company.

When a decision is made to suspend the FCL of a company, the following actions will be taken:

- CSM will notify the FSO or company representative in writing that its FCL has been suspended. Such notification will state the reason for the suspension and will inform the company that the award of new subcontracts to the facility will not be permitted, and no new DOE personnel security clearance actions may be granted until the facility has been restored to a fully valid status. The notification will further state that termination of the FCL may occur if the issues causing the suspension are not rectified within the time frame and manner specified by SNL.
- All affected DOE elements and, if applicable, affected Other Government Agencies will be notified by CSM of the suspension action.

During the suspension, no new contracts may be awarded to the company, and no new personnel security clearances (other than KMP) may be requested. Work may continue on existing contracts the company holds by those who already possess personnel clearances. Uncleared work is not affected and new uncleared badges may be requested for new personnel. When the conditions that resulted in the suspension have been resolved in a manner acceptable by SNL, the FCL may be reinstated. The reinstatement must be based on the necessity to complete or continue work associated with the original FCL. If the conditions cannot be resolved, the FCL may be terminated.

2.3.2.6. DOE Facility Clearance Terminations

When all subcontracts have expired, terminated, and/or a FCL is no longer necessary, CSM will take action to terminate the FCL and CSCS. If the subcontractor has other security activities outside of SNL, CSM will terminate the CSCS and transfer the FCL to another DOE Designated Responsible Office.

Upon termination of a CSCS, CSM will distribute a Security Activity Closeout Certification to the FSO for completion. The FSO is asked to review the certificate and concur that all personnel clearances have been terminated, and associated badges/credentials have been returned, or transferred to other SNL subcontracts. The FSO is required to submit the completed certificate to CSM and retain a copy for their records.

2.3.3. *Facility Clearance Reporting Requirements*

FSOs are required to report certain events that have an impact on the status of their facility clearance. Subcontractor facilities holding an FCL must submit written reports of changed conditions and anticipated changes affecting the FCL.

Note: If a facility is under DSS cognizance, all changes must be reported through e-FCL. As a courtesy, SNL requests that all changes also be reported to CSM via email at farateam@sandia.gov to ensure conformity.

2.3.3.1. Reporting Significant Changes

When changes to the extent and nature of FOCI affect the information in a contractor's most recent FOCI submission(s), the FSO must immediately provide written notification and supporting documentation relevant to the changes to CSM (or the respective DOE Cognizant Security Office [CSO]) through e-FOCI.

A detailed list of significant changes that require reporting are outlined in the Contractor Requirements Document section of DOE O 470.4B, Admin Chg 2, *Safeguards & Security Program* and SF-328, *Certificate Pertaining to Foreign Interests*. Significant changes that may warrant processing of the subcontractor/parent for a new FOCI determination include, but are not limited to:

- All circumstances that would change any answer on the SF 328 from "No" to "Yes" (this must be reported by submitting a changed condition SF 328).
- A previously reported threshold or factor that was favorably adjudicated by the DOE CSO has increased to a level requiring a determination by the Office of Environment, Health, Safety and Security or, for NNSA, the Office of Defense Nuclear Security.
- A previously reported foreign ownership threshold or factor that was favorably adjudicated has increased to the extent that any FOCI mitigation method is required.
- Any changes in ownership or control, including stock transfers that affect control of the company. Notice of changes include, but are not limited to, ownership or control events that are required to be reported to the Securities and Exchange Commission (SEC), the Federal Trade Commission, or the Department of Justice (DOJ).

2.3.3.2. Reporting Anticipated Changes

Anticipated changes and actions are events that arise when the subcontractor or any of its tier parents enter into formal negotiations toward agreement, a written memorandum of understanding, or when written application for financing is made in the case of financing agreements. The FSO must immediately provide written notification of anticipated actions to CSM via email farateam@sandia.gov. Failure to provide written notification of anticipated actions may result in suspension or termination of the FCL. Anticipated actions include, but are not limited to:

- An action to terminate business, operations of the subcontractor, or any of its parents for any reason. Reasons for the previously stated actions may include, but are not limited to, entering into any transaction of merger, consolidation, or amalgamation with another company; conveying, selling, leasing, transferring, or disposing of all, if not a substantial portion of, business or assets; and/or making any material change that could have an adverse effect on the subcontractor organization's ability to perform its contractual obligations for SNL or other subcontractors of SNL.

  Note: The FSO is required to notify CSM when their company enters into negotiations for a proposed merger, acquisition, takeover, or restructure within the company's chain of ownership. Failure to notify CSM prior to a merger, acquisition, takeover, or restructure will result in the suspension or termination of the FCL.

- Legal actions taken to initiate bankruptcy proceedings involving the subcontractor organization or any of its tier parents.
- Imminent adjudication of, or reorganization resulting from, bankruptcy actions involving the subcontractor organization or any of its tier parents.
- The subcontractor or its tier parents entering into negotiations with non-U.S. citizens that may reasonably be expected to require amendment of the SF-328, Certificate Pertaining to Foreign Interest, including, but not limited to, negotiations for the sale of securities to a non-U.S. citizen(s).

2.3.3.3. Reporting Other Changes

The FSO must immediately provide written notification to CSM via email at farateam@sandia.gov, and e-FOCI of the changes listed below. Failure to do so may result in suspension or termination of the FCL.

Other reportable changes include, but are not limited to:

- Any change of operating name, address of the company, or any of its cleared locations.
- Any changes to information previously submitted for KMP, including, if appropriate, the names of the individuals the incoming KMP are replacing.
    - A new complete listing of KMP must be submitted any time a KMP change is made and/or when requested in writing by SNL or DOE/NNSA.
- Any pre-subcontract negotiation or award not placed through a government contracting authority that involves or may involve: (1) the release or disclosure of U.S. classified information to a foreign interest or (2) access to classified information furnished by a foreign interest.

When requested by SNL or DOE/NNSA, the subcontractor shall provide a current list of all classified subcontracts as well as classified lower-tier subcontracts issued to other subcontractors. Also, when requested by the DOE/NNSA, selected subcontractors shall provide security costs charged to the government for a specified period of time. The data points will be used by the DOE in developing the annual Report to Congress on overall National Industrial Security Program Costs.

2.3.4. Security Management in Contracting

In accordance with the DEAR Clause, Section 952.204-2(1), FCLs are required for all tier subcontractors requiring DOE personnel security clearances. The prime subcontractor is responsible for ensuring that the SDR is aware of the need for further lower-tier subcontracting, and will identify the lower-tier subcontractors that require a FCL and DOE personnel security clearance. The SDR will generate a CSCS for these lower-tier subcontractors on behalf of the prime subcontractor. SNL will also sponsor the lower-tier subcontractors for a FCL at the same or lower level than the prime subcontractor's FCL. The prime subcontractor must be granted a FCL at the same or higher level than its tier subcontractors.

Before a prime subcontractor requires lower-tier subcontractor personnel to obtain DOE personnel clearances, release or disclose classified information to a lower-tier subcontractor, or cause classified information to be generated by a lower-tier subcontractor, the following actions are required:

1) **Determine the security requirements of the lower-tier subcontract.**
    a. The requirements of DEAR 952.204-2, Security (March 2011), DEAR 952.204-70, *Classification/Declassification (July 2009)*, and SNL Clause 610-FO, *Security Requirements*, must be incorporated into the solicitation/subcontract. A "security requirements clause" (reference 610-FO) and a CSCS shall be incorporated in the RFQ or other solicitation to ensure that the prospective subcontractor is aware of the security

requirements of the subcontract and can plan accordingly. Regardless of the performer of the work, subcontractors with the above clauses incorporated into their subcontract are responsible for compliance with all applicable security requirements. Affected subcontractors are responsible for flowing down the clauses and all applicable security requirements to lower-tier subcontracts at any tier to the extent necessary to ensure compliance with security requirements.

b. The subcontractor must obtain and maintain an appropriate FCL.
c. If the prime subcontract contains requirements for the release or disclosure of certain information even though it may not be classified, such as sensitive but unclassified information, the requirements shall be incorporated in the solicitation and the subcontract.

2) Determine facility clearance status of prospective lower-tier subcontractors.

a. If a prospective lower-tier subcontractor does not have the appropriate FCL, the prime subcontractor shall notify the SDR of the subcontract to request submission of a CSCS. The prime subcontractor shall allow sufficient lead time in connection with the award of the subcontract to enable an uncleared bidder to be processed for the necessary FCL.

3) Determine the classification guidance of the lower-tier subcontract.

a. The SDR will extract classification guidance from the prime subcontractor's CSCS when preparing guidance that pertains to a lower-tier subcontract CSCS.
   Note: The classification specification shall not contain any classified information.
b. When preparing classification guidance for a subcontract, the SDR shall ensure the CSCS is incorporated in each classified subcontract.

4) The CSCS and SRP shall be included in the subcontract awarded to the successful bidder.

a. A revised CSCS shall be issued, as necessary, during the lifetime of the subcontract, when the security requirements and/or classification guidance changes. It is the subcontractor's responsibility, at any tier, to understand and apply all aspects of the security guidance through proper communication and direction to ensure personnel compliance with this requirement.

Notify CSM at 505-844-5759 or at farateam@sandia.gov when any of the following occur with a lower-tier subcontractor company:

- Personnel security clearances are no longer needed.
- Lower-tier subcontracts have expired.
- Lower-tier subcontracts have terminated and/or a FCL is no longer necessary.

3.0 PERSONNEL SECURITY

3.1. VALIDATING PERSONS OF INTEREST

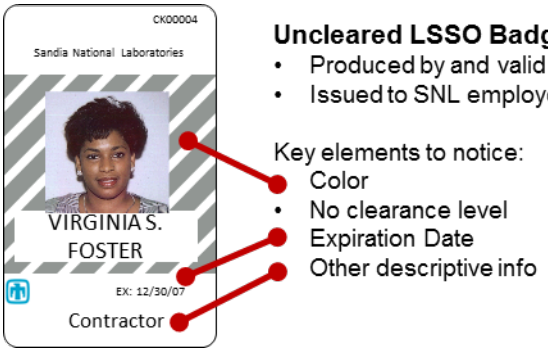
The SNL Validation Office assists SNL employees/sponsors in conducting due diligence reviews of their subcontractor personnel. The SNL Validation Office also assist with consultants and visitors to understand the people with whom they do business. Prior to granting site or SRN/Sandia Classified Network (SCN) cyber access to subcontractor personnel, a public records and commercially available data source check is conducted through the LexisNexis Accurint for Government System. Any significant criminal information discovered will be verified through the National Crime Information Center system. Failed validations occur when the Validation Office does not validate a specific individual to the level requested. In such cases, the SNL employee/sponsor will be notified, a failed validation entry is made in Enterprise Person, and a security hold is placed on the individual's badge and/or badge authorization. A passing validation allows the individual to be further processed for access to SNL site and cyber resources. Granting or denying physical site access is at the discretion of SNL.

3.2. DOE SECURITY BADGES

DOE security badges are issued to subcontractor personnel as evidence of access authorization (i.e., personnel security clearance) and/or a means of gaining physical access/admittance to SNL-controlled premises.

3.2.1. *Badge Types*

SNL-issued Local Site Specific Only (LSSO) badges and DOE Personal Identification Verification (PIV) credentials (i.e., Homeland Security Presidential Directive 12 [HSPD-12] federal credential) are considered DOE security badges.



Uncleared LSSO Badge

- Produced by and valid throughout SNL
- Issued to SNL employees, visitors, contractors and consultants

Key elements to notice:

- Color
- No clearance level
- Expiration Date
- Other descriptive info

Uncleared Foreign National Visitor Badge

- Produced by and valid only at the SNL site listed on the badge
- Issued to SNL visitors

Key elements to notice:

- Color
- No clearance level
- Issue and Expiration Date
- Other descriptive info

Cleared LSSO Badge

- Produced by and valid throughout SNL
- Issued to SNL employees, visitors, contractors and consultants

Key elements to notice:

- Clearance Level
- Color
- Expiration Date
- Other descriptive info

DOE PIV Credential

- Common government-wide design
- Used by other agencies, but not valid at SNL to denote clearance level

Key elements to notice:

- Agency affiliation *(Must reflect "DOE" to be valid for use at SNL)*
- Clearance level

No relationship between the printed expiration date on the credential and a cleared badge authorization

3.2.2. *Badge Request Process*

The Sandia Total Access Request Tool (START) is the means by which badging requests are initiated for U.S. citizen subcontractor personnel. START will require cyber access to the SRN. FSO's without SRN access may be sponsored for it if their SNL representative wishes to do so. It is the responsibility of the applicable SNL manager, or team lead, to originate badge requests for subcontractor personnel under their supervision/responsibility.

Upon approval of the START request by a SNL manager, an uncleared badge authorization is created. This allows subcontractor personnel to obtain a SNL-issued, uncleared LSSO badge. The LSSO badge is valid and functional only through the expiration date printed on it. The date of expiration is determined when the START request is submitted. For uncleared subcontractor personnel, only an uncleared LSSO badge is issued.

The badging process for subcontractor personnel on a cleared subcontract begins in the same manner as an uncleared subcontract. In addition to the creation of an uncleared badge authorization, a request for a DOE security clearance is also made by the SNL manager. While awaiting a clearance determination from DOE, subcontractor personnel may be issued uncleared LSSO badges. Upon being granted a clearance, a separate cleared badge authorization is created by the SNL Clearance Office. Once the cleared badge is ready for pick-up, the approving SNL manager, office administrative assistant (OAA), FSO and SDR will be notified via email. The now cleared subcontractor must return their uncleared LSSO badge (if issued) to the SNL Badge Office in exchange for a cleared LSSO badge. The cleared LSSO badge is valid and functional only through the cleared badge authorization expiration date printed on it. Most cleared subcontractor personnel are issued a DOE PIV credential and will retain the cleared LSSO badge for about one week or until the credential is available. In effect, the credential becomes the subcontractor's permanent cleared security badge.

Issuance of a DOE PIV credential to subcontractor personnel is dependent on several factors, including whether or not they require continuous physical access to SNL security areas or General Access Areas (GAA), or other DOE facilities, in connection with their work for SNL. If this is not the case—for example, where the individual works remotely, requires site access on infrequent or rare occasions, or would likely never require physical access to SNL facilities—only a cleared LSSO badge is warranted and would be issued as necessary.

Prior to a requesting renewal of a cleared badge in START, the contract Period of Performance must be extended by Procurement, the CSCS must be revised by the SDR and approved by CSM, and the subcontractor's EP record must be updated. The SDR, the subcontractor's SNL manager, OAA, and the FSO will be notified to inform subcontractor personnel that their cleared badge has been renewed and physical site access may continue.

3.2.3. *Picking Up Badges*

Subcontractor personnel who elect to use a state-issued driver's license or ID card as proof of identity when picking up a DOE security badge for access to SNL-controlled premises, must present a driver's license or ID card that is compliant with the Real ID Act. Failure to comply with the Real ID Act will result in denial of access, unless an alternative ID document is available. Although state-issued driver's licenses and ID cards are the most common means used to establish identity, they are not the only available means. Alternative ID documents containing a photograph listed on the Department of Homeland Security Form I-9, *Employment Eligibility Verification,* may also be used as proof of identity (U.S. passport/card, U.S. military ID, etc.).

3.2.4. *Returning Badges*

Given that badges can be used to gain unauthorized access to SNL and other DOE-related facilities, SNL has implemented effective badge-recovery procedures to prevent the compromise of National Security. Badges may be returned in person to the SNL Badge Office (preferred method) or by mail. If mailed, DOE PIV credentials must be sent via certified/signature required delivery (e.g., USPS, FedEX, UPS). SNL LSSO badges may be sent by standard US Mail.

The FSO is responsible for ensuring that all DOE security badges that are no longer required (e.g., subcontract has ended and no extension has been granted, personnel terminate employment) are promptly returned to the SNL Badge Office, regardless of the expiration date. Similarly, it is the responsibility of the FSO to ensure that any unexpired SNL LSSO badges no longer required (e.g., badge expiration date extends beyond last day of work on the subcontract), are promptly returned to the SNL Badge Office.

In cases where the FSO is unable to retrieve a badge, the FSO is responsible for completing and submitting an SF 2730-LSB, *Reporting Lost, Stolen, Forgotten or Unrecovered Badge* form within 24 hours of discovery. DOE policy directs that any unrecovered DOE security badge is to be considered stolen government property and reported to SIMP as an IOSC. The FSO is ultimately responsible for ensuring that badges or other credentials distributed by SNL or DOE, granting physical access to DOE/NNSA-owned or leased facilities by the company's personnel, are returned upon:

- Termination of subcontract.
- Expiration of subcontract.
- Employment termination of an individual performing work under subcontract.
- Demand by SNL or DOE/NNSA to return the badge.

3.3. DOE Personnel Security Clearances

Personnel security clearances denote an individual's eligibility for access to a particular level and category of classified information or material. The classification levels are designated as Top Secret (TS), Secret (S), and Confidential (C). Classification categories are designated as Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI). DOE Q and L personnel security clearances are used at SNL. DOE Top Secret, Secret, and Confidential clearances are not issued. The chart below shows the classification levels and categories of classified matter that can be accessed based on personnel security clearance type.

Classification Level	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	Undue

Increasing Risk

While SNL sponsors and initiates the clearance process for subcontractor personnel, DOE will make the determination of whether an individual is eligible to access classified information and will grant or deny the clearance request. If subcontractor personnel are hired and placed in a position prior to receiving a clearance, the uncleared individual may not be afforded access to classified information, matter, or SNM, until their clearance has been granted. DOE personnel security clearances will only be processed for U.S. citizens who are at least 18 years of age.

A company must have a registered, active facility clearance before their personnel can be submitted for DOE "L" or "Q" personnel security clearances for the performance of their work under an authorized SNL subcontract. Prior to the submission of a clearance request to DOE, both SNL management and Clearance Office review and approval of the clearance request is required. Consequently, no classified work may begin under the performance of a subcontract until the company has been registered and approved by DOE. Although SNL has an established facility clearance, the FSO must ensure that tier subcontract companies with established subcontracts have been properly registered.

Personnel security clearances **may not** be requested to:

- Avoid the use of access controls or physical barriers.
- Alleviate individual or management responsibilities for properly protecting classified information, SNM, or controlling dissemination of classified information on a need-to-know basis.
- Determine an individual's fitness for employment.
- Establish a pool of personnel with pre-existing security clearances.
- Accommodate an individual's personal convenience, expedience, gain, or advantage.
- Anticipate unspecified classified work.

Personnel security clearances:

- May not be used as a determining factor for hiring, entering into a consultant agreement, or awarding a subcontract.
- Must be requested only when required, so as to avoid the unnecessary expenditure of resources and the unwarranted invasion of an individual's privacy.
- Must only be requested and maintained at the minimum number necessary to ensure operational efficiency.

3.3.1. *Clearance Action Requests*

START is the means by which clearance actions are initiated for U.S. citizen subcontractor personnel. It is the responsibility of the applicable SNL manager or team lead to originate clearance actions (e.g., initial request, reinstate, extend, upgrade, downgrade, reciprocity, etc.) for subcontractor personnel under their supervision/responsibility.

While awaiting a clearance decision, subcontractor personnel will be authorized for an uncleared badge and the SDR, the applicant's SNL manager, the OAA and (if applicable) the subcontracting company's FSO will be notified to inform their employee that an uncleared badge may be obtained at the SNL Badge Office. Additionally, subcontractor personnel will be notified directly by email of any tasks and associated deadlines necessary to complete the clearance request. The SNL manager, OAA, and (if applicable) FSO will be copied on all such messages.

3.3.2. *Clearance Action Applicant Tasks*

The SNL/NM Clearance Office and SNL/CA Visitor Control Office will provide instruction to subcontractor personnel on how to complete:

- SF-86, *Questionnaire for National Security Positions* (QNSP) (via e-QIP submission).
- The drug test requirement within 60 calendar days of the individual's SF-86, *Questionnaire for National Security Positions signature*.
- Electronic fingerprints via an approved capture method (e.g., at a GSA shared HSPD-12 enrollment center).
- DOE F 5631.18, *Security Acknowledgement*.

Note: In accordance with DOE policy, applicants for security clearances who are determined to have illegally used a controlled substance within 12 months of their Questionnaire for National Security Positions (SF 86) signature date, through self-admission, or a confirming drug test, will have their application process terminated from further consideration for a security clearance. They can demonstrate abstinence from illegal use of controlled substances for at least twelve months after their background investigation has been opened, and have appeal rights, depending on the circumstances of the discovery.

3.3.3. *Clearance Action FSO Responsibilities*

The FSO must ensure and advise personnel that they must properly complete security forms, and all related material may, as required, be reviewed for adequacy and completeness prior to submission to DOE. The FSO must also ensure that such information will not be used for any other purpose within the company. The FSO should recommend maintaining copies of their completed security forms to personnel for their personal records. Deficient security clearance requests will not be processed. The FSO must ensure that the request is corrected and resubmitted to the SNL/NM Clearance Office or SNL/CA Visitor Control Office in a timely manner.

The FSO must assist in the timely processing of security clearances by ensuring:

- The availability of the applicants and personnel for the performance of personal interviews by the investigative agency or DOE personnel security staff.
- Other personnel are made available, as needed, to provide background information during the performance of all personnel security background investigations.
- Compliance with procedures established by DOE/NNSA in providing its employee(s) with any forms directed by DOE/NNSA.
- Personnel cooperate with the officials responsible for granting access to DOE/NNSA owned or leased facilities, to include providing those officials with additional information in a timely fashion, upon request.

All records and information pertaining to DOE security clearance matters, including copies of personnel security forms and information collected from the conduct of contractor reviews, must be protected against unauthorized disclosure in accordance with the Privacy Act of 1974 (5 U.S.C 552a). Information for DOE personnel security clearance processing must not be used for

any purpose other than that for which it is intended and must not be provided to unauthorized parties.

3.3.4. *U.S. Citizenship*

Subcontractor personnel selected for positions requiring a DOE security clearance must provide evidence of U.S. citizenship. The FSO must verify such evidence, verbally or otherwise, as acceptable to the SNL party submitting the clearance request via START when requesting that the individual be processed for a security clearance. Acceptable forms of evidence of U.S. citizenship are listed below.

For subcontractor personnel born in the U.S., one of the following is required:

- Original or certified U.S. birth certificate.
- Current or expired U.S. passport.

For subcontractor personnel claiming citizenship by naturalization:

- A certificate of naturalization (Form N-550 or N-570) showing their name is required.

For subcontractor personnel claiming citizenship acquired by birth abroad to a U.S. citizen, one of the following (showing the individual's name) is required:

- A Certificate of Citizenship Form N-560 or N-561.
- A Report of Birth Abroad of a Citizen of the U.S. of America (State Department Form FS 240).
- A Certificate of Birth (Form FS 545 or DS 1350).
- Current U.S. passport.
- Record of Military Processing—Armed Forces of the U.S. (DD Form 1966), provided it reflects that the individual is a U.S. citizen.

3.3.5. *Subcontractor Personnel Reviews*

In accordance with DEAR clause 952.204-2, *Security Requirements*, subcontract and lower-tier subcontract companies are required to conduct a thorough review of an uncleared applicant or employee's background. They are also required to test for illegal use of controlled substances. Both the background review and controlled substance testing should be completed prior to selecting the individual for a position requiring a DOE personnel security clearance. Reviews help the company make a determination as to whether it is appropriate to select an uncleared applicant or employee, to a position requiring a DOE personnel security clearance. The review must be completed by the company prior to submitting a personnel security clearance request to the SNL/NM Clearance Office or SNL/CA Visitor Control Office.

Subcontractor personnel reviews must include:

- Verification of an uncleared applicant's or employee's, educational background, including any high school diploma obtained within the past five years, and degrees or diplomas granted by an institution of higher learning.
- Verification from the uncleared applicant or employee of no illegal drug use in the past 12 months. *Use of controlled substance includes; injecting, snorting, inhaling, swallowing, experimenting with or otherwise consuming any drug or controlled substance.*
- Contact with listed employers for the last three years and listed personal references.
- Local law enforcement checks, when such checks are not prohibited by regulation, state or local law, and when the uncleared applicant or uncleared employee resides in the jurisdiction where the subcontractor is located.
- A credit check and other checks as appropriate.

In collecting and using this information, the company must comply with all applicable laws, regulations, and Executive Orders, including those:

- Governing the processing and privacy of an individual's information, such as the Fair Credit Reporting Act, Americans with Disabilities Act (ADA), and Health Insurance Portability and Accountability Act.
- Prohibiting discrimination in employment, such as under the ADA, Title VII and the Age Discrimination in Employment Act, including pre- and post-offer of employment disability related questioning.

Subcontractor reviews are not required for personnel:

- In possession of a DOE security clearance.
- In possession of a clearance from another federal agency.
- Whose DOE security clearance may be reapproved without a federal background investigation.

Subcontract and lower-tier subcontract companies are required to maintain a record of the review and information concerning each uncleared applicant or employee who is selected for a position requiring a DOE personnel security clearance, and to furnish such information to SNL Personnel Security upon request.

Subcontractor personnel review records should contain:

- The date(s) each review was conducted.
- Each entity that provided information concerning the individual.
- A certification that the review was conducted in accordance with all applicable laws, regulations, and Executive Orders, including those governing the processing and privacy of an individual's information collected during the review.
- A certification that all information collected during the review was reviewed and evaluated in accordance with the contractor's personnel policies.

- The results of the test for illegal use of controlled substances.

3.3.6. *Clearance Termination*

An individual's responsibility to protect classified and sensitive information continues long after he or she has terminated employment, is separated from SNL, or no longer requires a security clearance.

Reasons for clearance termination include:

- Subcontract and/or employment is terminated.
- Clearance is no longer required.
- Cleared person is on an approved leave of absence and will not require access to classified matter or SNM for 90 consecutive calendar days.
- Access to classified matter or SNM is no longer required.

To simplify the clearance termination process, the SEC225 Security Termination Briefing is combined with DOE F 5631.29, Security Termination Statement. Contractor personnel must complete the steps below to terminate their clearance.

Review and sign DOE F 5631.29, *Security Termination Statement, and Security Termination Briefing* (SEC225), with their SNL manager or FSO.

Sign the Security Termination Statement. The SNL manager, FSO or SDR must sign as the "Debriefing Official".

Every effort should be made to obtain subcontractor personnel signatures. If obtaining all signatures is not possible on the completed DOE F 5631.29, an explanation is required. In the "Remarks" section of the form, provide an explanation of the circumstances surrounding the termination and why the signature could not be obtained. The FSO who signs as the Debriefing Official must also ensure that the "reason for security termination" indicated on the DOE F 5631.29 is both accurate and specific, especially when conditions of termination are unfavorable. Under unfavorable circumstances, SNL Ethics Advisory & Investigative Services must be informed by calling 505-845-9900.

The signed DOE F 5631.29 is Official Use Only (OUO) when completed and must be returned to the appropriate SNL Clearance Office within 2 working days of termination. Failure to ensure that a DOE F 5631.29 is provided to SNL within 2 working days of the date of security termination, will be considered an issue of non-compliance.

- Submit the form via fax to SNL/NM at 505-844-9739 or to SNL/CA at 925-294-1330, as an encrypted email to clearance-nm@sandia.gov or clearance-ca@sandia.gov, or hand carry. Do not use interoffice mail.
- Subcontractors may retain the Security Termination Briefing (SEC225) for their records.

3.3.7. *Clearance Withdraw*

If a clearance is in process and is no longer required, send a notification to clearance-nm@sandia.gov or clearance-ca@sandia.gov with the subcontractor personnel name, circumstances surrounding the withdrawal, and intent to withdraw the clearance.

3.3.8. *Clearance Suspensions, Revocations and Denials*

While only DOE/NNSA can render a formal personnel security clearance determination, SNL and/or the FSO are authorized to take actions that affect a subcontractor's access, such as restricting access to DOE classified information or SNM when a security clearance is terminated, suspended or withdrawn. However, this requirement does not preclude an FSO from having personnel execute a DOE F 5631.29, *Security Termination Statement and Security Termination Briefing,* prior to the individual's departure.

Upon receipt of notification of a subcontractor's security clearance suspension, the FSO and SNL manager must ensure that the individual is precluded from access to classified information and SNM. If the Statement of Work in the subcontract allows suspension of subcontractor personnel security clearances, it does not preclude the company from assigning or transferring an individual to duties that do not require a security clearance. It is at the discretion of SNL whether subcontractor personnel can work in an uncleared capacity until such time that a final clearance determination is made by DOE. Upon denial, or revocation of subcontractor personnel security clearances, the SNL FSO will render a determination if the subcontractor can remain in an uncleared capacity.

3.3.9. *Impact to Clearance During a Leave of Absence (LOA) of 90 Calendar Days or More*

DOE requires that when an individual's circumstances temporarily eliminate the need for access to classified matter (e.g., continuous unescorted area access to a limited area) for 90 calendar days or more (i.e., during a leave of absence), the individual's security clearance must be administratively terminated (for process see 3.3.6 above). An administrative termination of this nature is not an adverse action and does not prevent or hinder a subsequent request to reinstate the clearance.

DOE will consider waiving its requirement to administratively terminate a clearance if the details of a particular case indicate that such a waiver would be in DOE's interest. Consequently, SNL management may choose to initiate a request to waive the DOE requirement and thereby allow an active clearance to be temporarily maintained for subcontractor personnel on an approved leave of absence (LOA) that by design or circumstance extends to 90 calendar days or more. A subcontractor personnel LOA must first be established in accordance with company Human Resources policy, and the responsible SNL manager must agree to initiate the waiver request. Process details are available on the Security Toolcart. If the waiver request is granted by DOE, the clearance may remain active up to a maximum of 180 calendar days from the LOA start date. Waiver extensions are not permitted. If an LOA remains in effect for more than 180 calendar

days, the clearance will be administratively terminated. Thereafter, standard clearance reinstatement requirements apply (i.e., a clearance request must be initiated via START).

3.3.10. *Clearance Reinvestigations*

Reinvestigations are required, and are intended to ensure that individuals with security clearances are routinely re-evaluated to determine their continued need and eligibility to possess their clearances. Reinvestigations for both "L" and "Q" security clearances occur on a 5-year cycle. The SNL Clearance Office will provide instructions to subcontractor personnel who are due for clearance reinvestigation. Subcontractor personnel must comply with reinvestigation requests and adhere to deadlines in order to recertify their security clearance status. The FSO will be copied on all related notifications to individuals subject to reinvestigation and must ensure cleared personnel cooperate fully with all requirements concerning clearance reinvestigations.

3.4. CLASSIFIED VISITS

Classified information and matter must be protected by ensuring that only persons with the appropriate security clearances, need-to-know, and programmatic authorizations are afforded access during visits where the release or exchange of such information is involved.

3.4.1. *SNL Outgoing Classified Visits*

An outgoing classified visit at SNL is an event requiring physical access to non-DOE controlled premises (e.g., a DoD facility or other government agency location) for official business of classified nature. Subcontractor personnel are responsible for coordinating with their SNL manager or OAA to initiate their request through the SNL Outgoing Classified Visits System. SNL management approval is required for outgoing classified visits. The SNL Badge Office processes visit requests and notifies the host facility of the visit. The duration of a visit request may not exceed 1 year. For travel to DOE/NNSA facilities, only a DOE PIV credential is required. Utilization of a DOE PIV credential at other DOE/NNSA facilities should be in support of the Statement of Work listed in the authorized SNL subcontract.

3.4.2. *SNL Incoming Classified Visits*

Incoming classified visits at SNL apply to visitors from other government agencies who hold active personnel security clearances and require unescorted access to SNL controlled premises for purposes in which official business of classified nature will take place. Subcontractor personnel are not authorized to request or host an incoming classified visit at SNL. The contractor's SNL manager may host a visitor on behalf of subcontractor personnel. The contractor's OAA may initiate an incoming visit request on behalf of subcontractor personnel through the SNL Incoming Visits System.

Any person on an active subcontract with SNL, regardless of the frequency of their physical access to SNL, is considered subcontractor personnel and should never be passed as a visitor. During subcontract negotiation, visit requests may be allowed; however, once the subcontract has been placed, the company's employees cannot be passed as visitors at SNL.

3.5. UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS

As a national security laboratory, SNL actively supports DOE's role as a leader in science and technology. To maintain that leadership, DOE encourages international collaborations and, thus, allows access by foreign national visitors/assignees to its unclassified information, programs, and technologies. Consequently, foreign nationals are allowed access to SNL sites. However, SNL must ensure that foreign national access does not pose a risk to national security. Along with other measures, SNL protects information, assets, etc., by monitoring and controlling interactions with foreign nationals.

3.5.1. *Onsite SNL Work*

All foreign national subcontractor personnel are required to have an approved Foreign National Request Security Plan (FNRSP) from the SNL Foreign Interactions Office (FIO) prior to working onsite at SNL. The SNL manager or SDR is responsible for submitting an FNRSP for subcontractor personnel. Subcontractor personnel are required to present valid lawful status documents before a DOE badge is created and issued. The individual who hosts foreign national subcontractor personnel at SNL must be a U.S. citizen and an employee of NNSA or SNL. Subcontractor personnel are not authorized to host or co-host uncleared foreign nationals at SNL. Subcontractor personnel may escort uncleared foreign nationals at SNL if they:

- Are identified as an authorized escort on a FNRSP.
- Complete EC100 – Export Control Awareness Training.
- Possess a DOE-approved standard badge.
- Possess a clearance that is appropriate for the area in which escorting will occur.
- Are a U.S. citizen.

3.5.2. *Off-Site SNL Work*

When all work is conducted entirely offsite, and the research from a subcontract is considered fundamental research and will be published in open literature intended for public release, approval for foreign national subcontractor personnel to work offsite on a SNL project is not required. Any work or research being conducted on information that is not publicly available is considered to be "onsite" work and must have an approved FNRSP in place before the work can be performed.

Practice due diligence when sharing information with foreign nationals. Among other restrictions, subcontractors are not to share export-controlled information without Export Control Authorization. For additional guidance, refer to the Export Control Clause found in the NTESS Contract Information General Provisions (Section II Terms and Conditions).

4.0 ALCOHOL, DRUGS AND TOBACCO AT SNL

Subcontractor Personnel Reviews require subcontract and lower-tier subcontract companies to test uncleared applicants or employees for illegal use of controlled substances, prior to selecting the individual for a position requiring a DOE personnel security clearance.

Applicants for a DOE personnel security clearance must be tested to demonstrate the absence of illegal use of controlled substances. The SNL Drug Screening Clinic will facilitate drug testing of subcontractor personnel who are applicants for DOE personnel security clearances.

All positions requiring a DOE personnel security clearance are deemed testing designated positions (TDP). Subcontractor personnel applying for, or possessing, DOE personnel security clearances are subject to applicant, random and reasonable suspicion testing for illegal use of controlled substances. DOE will not process candidates for a DOE personnel security clearance unless their tests confirm the absence from their system of any illegal use of controlled substances. In addition, DOE will not process clearance requests until 12 months have passed from the day of drug use. SNL will not tolerate the illegal use of controlled substances (including abuse of legal prescription medications) or abuse of alcohol at a SNL worksite, or in the performance of company business.

SNL:

- Prohibits the use, sale, purchase, manufacture, transfer or possession of alcohol on SNL controlled property. In addition, being under the influence of alcohol on SNL controlled property or in the performance of SNL business is prohibited.
- May restrict work of subcontractor personnel in safety and/or security sensitive positions (SSSP) if they are taking medications that cause impairment and/or alter judgment.

4.1. SUBSTANCE TESTING TYPES AND REQUIREMENTS

Testing Type	Requirement
Pre-TDP	Subcontractor personnel who are obtaining or reinstating their DOE Q- or L-security clearance must have a drug test prior to submitting their SF-86, *Questionnaire for National Security Positions* (via e-QIP submission). SNL Drug Screening Clinic will facilitate drug testing of subcontractor personnel.
TDP	Subcontractor personnel in a TDP shall receive a pre-program screening and will be selected for unannounced testing on a random basis for urinalysis at a minimum rate of 30% of the total number of Members of the Workforce in the TDP positions annually.

Testing Type	Requirement
Medical Monitoring /Surveillance	Subcontractor personnel who participate in Commercial Driver License (CDL), Crane and Hoist (CAH), or Human Reliability programs (HRP) are subject to **frequent, unannounced testing** per each program regulated testing rates.
Reasonable Suspicion	SNL may require subcontractor personnel to be tested for the use of drugs, controlled substances, and/or alcohol **if reasonable suspicion exists**.
Post-Occurrence	**Following an occurrence** as defined in DOE O 232.2A, Chg. 1, *Occurrence Reporting and Processing of Operations Information,* for which subcontractor personnel have been identified as having caused or contributed to the conditions which caused the occurrence.
Post-Accident	**Following an applicable accident** (in accordance with 49 CFR 40 and 49 CFR Part 382) involving subcontractor personnel participating in CDL or CAH programs.

4.2. MEDICAL MARIJUANA

Although use of marijuana for medicinal purposes may be legal per state law in New Mexico, Nevada and California, federal statutes establishing the legal basis for an individual's eligibility for a security clearance take precedence and prohibit use of marijuana including medical marijuana by any applicant or holder of a DOE clearance in accordance with 10 CFR 710. If a drug test indicates use of marijuana, the test results in a verified positive drug test and consequences of a positive drug test for an illegal substance apply, regardless of whether the individual has registered with the State Department of Health or obtained a Registry Identification Card that exempts him/her from criminal and civil penalties for the medical use of cannabis. The term Medical Marijuana does not include any prescribed legal form of synthetic marijuana (e.g., Marinol or its equivalent).

4.3. USE OF LEGAL AND VALID PRESCRIPTION MEDICATIONS

Prescribed and over the counter drugs which have been legally obtained and are being used for the purpose for which they are prescribed, manufactured, or compounded are considered to be legal and valid medication. Subcontractor personnel who takes over the counter or prescribed medication are responsible for being aware of any effect the medication may have on their job performance. Subcontractor personnel must promptly inform Employee Health Services if they are taking medication likely to impair their ability to perform in a SSSP at SNL. SNL will work with subcontractor personnel to determine any medical restriction and whether any reasonable accommodations are necessary. Upon testing positive for a legal but impairment-causing prescription drug (e.g. Marinol – a prescribed and legal form of marijuana), a SNL Medical Review Officer (MRO) will interview subcontractor personnel, consult with their SNL line manager about their job duties, and determine whether a fitness-for-duty clinical evaluation is

necessary in order to determine whether the individual can safely perform his/her job with or without a medical restriction while taking the impairment-causing drug.

4.4. ALCOHOL TESTING

Alcohol testing is performed for those mandated programs that call for such testing such as post-accident/occurrence, rehabilitation testing, or if reasonable suspicion exists. Subcontractor personnel who render a breath alcohol test result of BAC 0.020% (.02 g/210L) or greater will be temporarily removed for a period of no less than 24 hours from any safety and/or security sensitive duties. Subcontractor personnel who test positive for alcohol abuse will be required to turn over their badge, will immediately lose SNL site access and will be removed from the performance of the SNL contract.

4.5. SUBCONTRACTOR PERSONNEL RESPONSIBILITIES

Subcontractor personnel must comply with the Member of the Workforce Drug Free Workplace Awareness Training every 2 years. Subcontractor personnel must also provide the MRO, true and accurate records and information relating to their substance use.

Subcontractor personnel who take over-the-counter or prescribed medication are responsible for being aware of any effect the medication may have on their job performance and must promptly inform Employee Health Services if they are taking medication likely to impair their ability to perform in a SSSP at SNL. SNL will work with the employee and their manager to determine whether any medical restrictions are necessary. Subcontractor personnel are responsible for adhering to any medical restrictions and identified accommodations implemented per Laboratory Policy EHS002.2, *Medical Restrictions Process*. When requested, subcontractor personnel must report for substance abuse testing within the timeframe allowed, and are expected to fully cooperate with instructions given by SNL Drug Testing Staff. Upon verbal notification, no excuses will be accepted for failure to report to the collection site before close of the business day. Subcontractor personnel who work at a non-SNL location will be given information on where to report to at the time of notification. Subcontractor personnel will have 24 hours from the time of notification to report to a collection site upon receipt of an overnight package containing instructions and the location of the nearest collection site.

4.6. FSO RESPONSIBILITIES

The FSO is responsible for complying with substance abuse testing reporting notifications. FSO's applying for, or in possession of, a DOE personnel security clearance are subject to substance abuse testing. The FSO is expected to assist SNL Drug Testing Staff with subcontractor personnel substance abuse testing reporting notifications if the SNL Drug Testing Staff is unable to contact the individual directly. The FSO is also responsible for instructing subcontractor personnel to comply with substance abuse testing upon verbal notification from SNL Drug Testing Staff.

4.7. CONSEQUENCES

A confirmed positive drug and/or alcohol test result, documented admittance of illegal drug use, refusal to provide a specimen, or failure to report for a substance abuse test per mandated program guidelines will result in the confiscation of badge, loss of SNL site access, and action up to and including removal from the performance of the SNL subcontract.

Subcontractor personnel may request a split specimen to be tested. However, they will bear the cost of the test. While awaiting the results of the split specimen test, subcontractor personnel may have their SNL issued badge deactivated by our MRO, which would restrict their access to SNL and Kirtland Air Force Base.

If subcontractor personnel fail to report per mandated program guidelines, notification will be provided to Personnel Security, Ethics Advisory and Investigative Services, who will contact the SP, FSO, and the individual's employer. Immediate confiscation of badge and loss of site access, removal of duties, and other action up to and including removal of the subcontractor from the performance of the SNL subcontract will be initiated by the Designated Employee Representative (DER).

If subcontractor personnel refuse to provide a specimen, or the test result is verified positive by the MRO, notification will be provided to Personnel Security and Ethics Advisory and Investigative Services, who will then contact the SP, FSO and the individual's employer. Immediate confiscation of badge and loss of site access, followed by removal of the subcontractor from the performance of the SNL subcontract, will be initiated by the DER.

5.0 SAFEGUARDS AND SECURITY AWARENESS

5.1. SECURITY BRIEFINGS

Security briefings inform individuals of their S&S responsibilities and promote continuing awareness of security practices. Subcontractor personnel assigned to perform work at SNL must complete the SNL Security Briefings identified on SNL's Security Toolcart as appropriate, or as assigned in SNL's Training and Employee Development System (TEDS) based on the criteria for briefings listed below. Subcontractor personnel who fail to complete the required security briefings as scheduled, may have their access to SNL suspended.

5.1.1. *Initial Security Briefing (SEC050)*

Subcontractor personnel who are issued a DOE badge must receive an initial briefing before they are given unescorted access to the SNL site. Subcontractor personnel transferring from one SNL site to another must review a site-specific initial briefing before assuming duties at the new site.

FSOs are advised to talk to new hires about the importance of security at SNL, and review the Initial Security Briefing. START is the official tracking system for this briefing requirement.

5.1.2. *Comprehensive Security Briefing (SEC150)*

Subcontractor personnel must receive a comprehensive security briefing upon receipt of a security clearance and before receiving initial access to classified information or matter, or SNM. This requirement is applicable to subcontractor personnel who have their security clearance sponsored by, or extended to, SNL. Subcontractor personnel will receive an email from TEDS requesting that they enroll in SEC150, a mandatory 4-hour in-class briefing within 180 days. Individuals unable to attend a live session may be authorized to receive an electronic booklet. See criteria below.

Subcontractor personnel with access to the SRN can enroll themselves in a live SEC150 session at the SNL/NM or SNL/CA site through TEDS. Those without SRN access should work with their SNL training coordinator to enroll or send enrollment requests to security@sandia.gov.

Subcontractor personnel unable to attend a live SEC150 session may be authorized by their SNL manager to receive a booklet to comply with the required training. The booklet includes a quiz that must be passed with no more than two missed questions. Subcontractor personnel must meet one or more of the following criteria to be eligible to receive a booklet:

- They have received a clearance grant notification and no live SEC150 briefings are scheduled in the near future, but a live briefing is still required.
- They will be working at a remote location, and attendance at a live briefing would result in significant cost (e.g., travel expenses).
- They will be immediately deployed to a location where live briefings are not available (e.g., overseas).

If the individual meets the above criteria, their SNL manager must send an authorization email to security@sandia.gov, to include all of the following:

- A valid email address and name for the individual.
- The specific criteria that warrant an exception.
- Documentation to support the exception (e.g., grant notification email).

The individual will receive an email from security@sandia.gov that will include:

- An authorization code will be issued for one-time use, which is required on the SEC150 completion record (as evidence of prior authorization).
- A link to the SEC150 Comprehensive Security Briefing and Quiz .pdf booklet.

When the quiz and completion record are received, the quiz will be graded. If no more than two questions are missed an "Equivalent" email is sent to the individual, the responsible manager, and the appropriate SNL Clearance Office to release the DOE badge and to have the individual sign the SF-312, *Classified Information Nondisclosure Agreement*.

5.1.3. *Annual Security Refresher Briefing (SEC100)*

Cleared subcontractor personnel and clearance applicants must receive annual (12-month intervals) security refresher briefings. This security briefing addresses current SNL security issues and reinforces information provided in SNL's Comprehensive Security Briefing.

Failure to complete the annual security refresher briefing will result in badge deactivation until the individual complies with the briefing requirement.

SEC100 is taken online after enrollment through TEDS. Subcontractor personnel receive email notifications when this training is due. Completions are tracked in TEDS. Subcontractor personnel who do not have access to the SRN may access and complete the training on the Security Toolcart. SEC100 completion forms can be emailed to security@sandia.gov, or faxed to 505-844-7802.

If an individual's badge has been deactivated due to non-compliance with SEC100 (e.g., passed due date in TEDS):

- Subcontractor personnel with SRN access—Enroll and complete the online SEC100 course through TEDS, print the completion email from TEDS and deliver the completion to the appropriate site badge office for verification and reactivation of the badge.
- Subcontractor personnel without SRN access—Go to the Security Toolcart to access and complete the training. Take the SEC100 completion form to the appropriate site badge office for verification and reactivation of the badge.

5.1.4. *Security Termination Briefing (SEC225)*

A Security Termination Briefing is required when a DOE personnel security clearance has been, or will be, terminated. The security briefing is provided in addition to the DOE F 5631.29, Security Termination Statement. The purpose of the briefing is to reiterate to the individual their continuing responsibility to not disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the FSO, SDR, or SNL manager.

The FSO or SDR will provide the combined form DOE F 5631.29, *Security Termination Statement and Security Termination Briefing*, to terminating/departing subcontractor personnel. The individual keeps the Security Termination Briefing and the SNL Clearance Office will submit DOE F 5631.29 to DOE and ensure subcontractor personnel badges are returned.

5.2. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

The SF-312, *Classified Information Nondisclosure Agreement,* is a contractual agreement between the U.S. Government and a cleared individual, in which they agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform the individual of (1) the trust that is placed in them by providing them access to classified information; (2) their responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from their failure to meet those responsibilities.

As a condition of access, a cleared individual must complete an SF-312 prior to accessing classified information or matter, or SNM. Subcontractor personnel will complete the SF-312 when they visit a SNL Badge Office upon notification that their clearance has been granted and a cleared badge is available for pick-up. If subcontractor personnel are offsite and not located near a SNL Badge Office or remote site, their FSO may execute the SF-312. An approved FSO or KMP may witness the signing of the SF-312. Signed copies of the SF-312 become OUO when completed and should be emailed via a secure method (encrypted, password protect etc.) to security@sandia.gov. The FSO is responsible for executing and retaining original SF-312s completed by their personnel.

5.3. DOE/SNL – Individual Reporting Requirements

All applicants and holders of a DOE personnel security clearance are required to report any information that they believe raises a potential security concern about themselves or another clearance applicant/holder. The FSO must ensure that all persons under their cognizance are aware of and fully comply with these reporting requirements, and must assist individuals as necessary. DOE and Sandia Individual Reporting Requirements are detailed here.

5.3.1. *Other Reporting Requirements*

The following conditions must be verbally reported by the FSO to SNL/NM Clearance Office (505) 284-3103 or SNL/CA Visitor Control Office (925) 294-2061 within 2 working days of the event, followed by written confirmation to clearance-nm@sandia.gov or clearance-ca@sandia.gov within the next 3 working days:

- When a clearance applicant declines an offer of employment or fails to report for duty.
- When made aware of any other information of a personnel security interest, as delineated under the "DOE/SNL - Individual Reporting Requirements" section above, concerning a clearance applicant or holder.
- When a clearance holder's access to classified information or SNM is restricted or withdrawn without DOE or SNL direction.
- When made aware of the death of a clearance applicant or holder.
- When a clearance applicant or holder is affected by any change that results in no longer requiring sponsorship of their clearance by SNL.

5.3.2. *Reporting Counterintelligence Interests*

Clearance applicants and holders must report matters of potential counterintelligence interest, including foreign travel and approaches by individuals seeking unauthorized access to classified information or SNM, to SNL Counterintelligence. Review the DOE and Sandia Individual Reporting Requirements matrix for details on how and when to report the interests below.

The FSO must ensure counterintelligence interest is reported, such as:

- Official foreign travel to sensitive countries regardless of whether the traveler possesses a security clearance.
- Travel to any country where the traveler intends to have, or has had, discussions with sensitive country foreign nationals regarding sensitive subjects. This includes travel that will involve meetings with sensitive country, foreign nationals (known in advance), or chance meetings where foreign nationals from sensitive countries are in attendance.
- All travel to any country when areas determined to be sensitive subjects will be discussed.
- Any substantive professional, personal, or enduring financial relationship (one that has existed, or is expected to exist, for a substantial period of time [months or years]) with foreign nationals affiliated with sensitive countries.
- Any contact with foreign nationals who make requests that could be attempts at exploitation or elicitation, such as:
    - Request for documents or information that is viewed by the traveler as unexpected or unrelated to the purpose of the interaction.
    - Request for the traveler to transport back to the U.S. any package(s) or letter(s) for mailing in the U.S.
    - Request of any kind that causes the traveler to feel uncomfortable or call into question the purpose of the request.
    - Professional contact or relationship with sensitive country foreign nationals, whether they occur at one's worksite or abroad.
    - Any foreign travel for which foreign monetary support is provided, whether to a sensitive or a non-sensitive country.
- Request for unauthorized access to classified or otherwise sensitive information.

The FSO must inform clearance applicants and holders that they have a specific obligation to truthfully provide all information requested for personnel security purposes. Failure or refusal to cooperate with any of these activities may prevent DOE from granting or continuing a security clearance. In this event, any current security clearance may be terminated or, for subcontractor applicants, further processing of a security clearance request may be suspended. Clearance applicants and holders must:

- Provide full, frank, and truthful answers to relevant and material questions.
- Furnish, or authorize others to furnish, if necessary, information that is deemed necessary to the security clearance eligibility process.
- Notify SNL upon learning of the presence of any reporting requirement, situation, or incident regarding anyone known to possess a DOE security clearance, or to be in the process of obtaining a DOE security clearance, no later than 2 working days after the event.

6.0 SAFEGUARDS & SECURITY TRAINING PROGRAM

CSM is responsible for relaying training requirements to designated FSOs. PHY-210DE, *Facility Security Officer Overview,* is a self-study correspondence course that provides an overview of the roles and responsibilities of the DOE or DOE-contractor FSO. The course emphasizes facility

clearance requirements, personnel security, information security, incident reporting, and other related programs. The course references the *National Industrial Security Program Operating Manual* (NISPOM) (DoD 5220.22-M) and a comprehensive listing of DOE orders, manuals, guides, forms, and notices. Upon successful completion of this course, participants will have a basic understanding of FSO roles and responsibilities. PHY-210DE must be completed by the FSO prior to the processing of the FCL. DOE FSOs of DOD-cleared companies are not required to complete PHY-210DE. FSO training provided by DSS is sufficient for DOE's purposes.

SNL managers and SDR's are responsible for ensuring that subcontractor personnel are properly trained to perform their duties. SNL managers and Training Coordinators work together to ensure that all required security training is input into each individual's "to-do list" in TEDS.

For a comprehensive list of security training, subcontractor personnel may review the SNL Corporate Security Training Decision and Self-Assessment Tool on the Security Connection webpage. Security training is provided in the subjects listed below, among others.

- Cyber Security Awareness Training (COM100)
- Annual Counterintelligence Training (CI100)
- Sensitive Information and Trade Compliance (SNL330)
- OUO Basics: Understanding Official Use Only (OUO101)

7.0 INFORMATION SECURITY

Classified matter is processed and handled within SNL Limited Areas and Temporary Limited Areas. Classified matter is stored within U.S. General Services Administration approved containers and vault-type rooms. A non-possessing subcontractor may not conduct, generate or store classified at their facility. Authorized subcontractor personnel may access, generate, perform and store classified at SNL, or another cleared facility, per the requirements of their approved CSCS. Access controls are also applied at SNL to limit access to subcontractor personnel with the appropriate security clearance and need-to-know.

7.1. CLASSIFIED INFORMATION

Subcontractor personnel working in a potentially classified subject area who may generate documents or material, must obtain a subject-matter-related briefing (SMB) directly from either their SNL manager, a Derivative Classifier (DC) who is knowledgeable of the subject area, or a Classification Officer. CLA102, *Classification Fundamentals,* may be assigned to subcontractor personnel working in a potentially classified subject area. CLA102 is designed to aid individuals in identifying critical information related to the programs and activities associated with their work.

Subcontractor personnel must request a DC review when working on:

- Documents or material in a potentially classified subject matter.
- Revisions of a previously reviewed classified document or material, including pen-and-ink notes, Post-its, and edits or changes that affect the technical information in the document or material.

- Extracting information from a classified document.
- Existing documents or material that may be improperly classified.

Documents may be submitted for a classification review in one of the following ways:
- To a cognizant DC, using the programmatic or organizational review for internal or controlled distribution.
- Using the formal SNL Review & Approval (R&A) tool, if the intent is to release the document for an uncontrolled and/or external audience.
- Through an alternate approval mechanism approved by the author/originator's organization.

Documents must be protected at the highest potential classification level and category of information that is likely to be contained in the document until the appropriate DC review is obtained.

Note: All those who create and manage information must understand the intent, purpose, and destination of the information they create in order to manage and protect it properly. The SNL R&A Tool is SNL's process to ensure that information is ready for release. It is SNL's method to manage risk, prevent the unintentional release of classified or sensitive information, protect patentable inventions, and communicate a professional image.

Subcontractor personnel should read and become familiar with DOE's Classification Bulletin GEN-16, "No Comment" Policy on Classified Information in the Public Domain. Subcontractor personnel may not comment on:

- Classified information found in a public domain or forum (e.g., websites, blogs, wikis, news articles or magazines, videos, or other electronic or printed media).
- The classification status or technical accuracy of information found in the public domain.

7.2. CLASSIFICATION OFFICE

The primary purpose of the SNL Classification Office is to identify and properly characterize the sensitivity of information created during SNL's work so that inadvertent release of classified and other sensitive information may be prevented, and authorized releases of information deemed to be unclassified unlimited release may be allowed.

At SNL, DCs are members of line organizations who have been authorized by the SNL Classification Officer (CO) to derivatively classify SNL-generated matter, which includes both documents and material. DCs determine whether a document or material contains classified information. DCs are authorized to make derivative classification determinations based on their organizational assignments and designated areas of expertise. DCs are also expected to serve as a local resource and to brief members of their organizations regarding the sensitivity of information within their programs. They must be able to explain the reasoning behind their classification decisions to subcontractor personnel and to the CO. Classification Technical Reviewers (CTR) are also available in both Classification Offices (SNL/NM and SNL/CA) to assist subcontractor personnel and DCs in identifying information that must be protected in the

interest of national security. Subcontractor personnel are encouraged and expected to question the classification of information, documents, and material they believe to be improperly classified, and to obtain a resolution by working with their DCs and the SNL Classification Office. They are also allowed and encouraged to challenge a classification decision directly to DOE's Classification Office if they believe the DC or CO determination is incorrect. The SNL Classification Offices will assist the contractor if a challenge process is requested.

7.3. Classified Matter Protection and Control

The purpose of the SNL Classified Matter Protection and Control (CMPC) Program is to protect classified matter that is generated, received, transmitted, used, stored, reproduced, permanently buried, or to be destroyed.

The CMPC Program implements and communicates to subcontractor personnel, requirements for the management and control of classified matter entrusted to SNL. SNL Laboratory Policy SS003, *Classified Matter Protection and Control*, and its associated procedures, convey the measures for identifying and safeguarding classified information and/or material through its lifecycle—identification as classified [creation] through final disposition—including appropriate measures for storing and using the information or material.

Contractors with DOE Q personnel security clearances sponsored by SNL must complete SEC301, *Classified Matter Training*. SNL managers and/or SDRs will determine if DOE L cleared contractors must take SEC301. Contractors who create classified that will be finalized (e.g., reviewed by a derivative classifier) must complete SEC303, *Classified Marking Training* and any supplemental training identified by the program, information owner and/or SNL manager, and must comply with the CMPC requirements for the facility at which they perform classified work.

Subcontractor personnel may never process or work on information related to a classified subject area at home, or other location outside of SNL without specific authorization from SNL or the U.S. Government. All work related to a classified subject area should always be performed in an approved SNL Limited Area.

7.4. Unclassified Information

SNL management is responsible for ensuring that subcontractor personnel under their direction have received the proper information and training related to protecting and managing unclassified information. Subcontractor personnel are responsible for identifying the type and category of unclassified information, and protecting it accordingly. Unclassified information falls into 3 types (the last of which contains various categories and subcategories):

1. **Unclassified Unlimited Release (UUR)** — This is the only category of information that has been approved for public release. Information is identified as UUR only as a result of a formal review through the SNL Review and Approval process. This process ensures that information has been adequately reviewed and is presentable for dissemination.

2. **Non-Sensitive Information** — Special handling is not required for unclassified information if the requirements associated with Unclassified Controlled Information (UCI) do not apply (typically work in draft and developmental stages). Pertinent requirements are discussed throughout this procedure.
3. **Unclassified Controlled Information (UCI)** — Federal agencies require that controls be placed on the availability of certain information, even if that information is not classified. Additionally, certain information owned by SNL (i.e., information related to financial, employment, procurement, legal, and technology transfer matters) is identified as "SNL Proprietary." These kinds of sensitive information are covered under the general heading of UCI. This information type is equivalent to "Sensitive Unclassified Information (SUI)." SUI is not used by the Department of Energy.

For guidance on how to protect UCI, refer to SNL Laboratory Policy IT012: *Unclassified Controlled Information.*

7.4.1. *Personally Identifiable Information (PII)*

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, is collected and maintained for the purpose of conducting official SNL business, and is not solely comprised of information that is available to the general public.

Protect PII – At Your Company
For the full definition of PII and additional instruction, refer to the **Protection of Personally Identifiable Information Clause** found in the NTESS Subcontract Information General Provisions (Section II Terms and Conditions).

PII - At Sandia National Laboratories
For instructions on how to identify, mark, retain, disseminate, protect and dispose of PII, refer to SNL Laboratory Policy IT023: *Personally Identifiable Information*.

7.4.2. *Official Use Only Information*

OUO is unclassified information that may be exempt from public release under the Freedom of Information Act (FOIA). OUO has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not have a need-to-know of the information to perform their jobs or other DOE authorized activities. OUO information is a subset of UCI[2].

Understanding Official Use Only (OUO101) training outlines the process for identifying, accessing and using, marking, distributing, transmitting and reproducing, storing, and disposal of OUO information.

[2] Other UCI that may be OUO and require additional markings include, Applied Technology, Attorney-Client/Work Product, Protected CRADA Information, SNL Proprietary Information, Patent Caution, Privacy Act Information, Export Controlled Information and/or Third Party Proprietary.

OUO Information - At Sandia National Laboratories
For instructions on how to identify, mark, protect, disseminate, and dispose of OUO, refer to SNL Laboratory Policy IT012: *Unclassified Controlled Information* .

Protect OUO Information – At Your Company
For additional guidance, refer to the **Information Security Clause** and the **Export Control Clause** found in the NTESS Subcontract Information General Provisions (Section II Terms and Conditions).

7.5. OPERATIONS SECURITY

Operations Security or OPSEC is an analytical process used to deny or delay adversaries of SNL's critical information. Using OPSEC enhances mission success. Refer to the **Operations Security Clause** found in the NTESS Subcontract Information General Provisions (Section II Terms and Conditions) and the Operations Security section on the Security Toolcart.

OPSEC implementation resources are available from the SNL OPSEC Program Office. Call 505-844-OPSEC (6773) or email OPSEC@sandia.gov regarding OPSEC-related questions or concerns.

8.0 PHYSICAL SECURITY

Physical Security ensures SNL security interests are physically protected from malevolent acts such as theft, diversion, sabotage and events such as civil disorder by considering site and regional threats, protection planning strategies, and implementing protection measures. Contact with SNL Physical Security may be initiated through SNL Security Connection by phone 505-845-1321 or email security@sandia.gov.

8.1. SECURITY AREAS

The SNL-controlled premises continuum begins with GAAs, and extends to security areas and secure storage areas. Each of these area types affords different levels of protection to security assets. The following are types of security areas at SNL:

GAAs – Although GAAs are not security areas by definition, industry-standard business protection elements may be implemented to protect personnel, property, and facilities. GAAs are areas established to allow access to certain areas with minimum security requirements. At SNL, there are two types of GAAs: Public and Non-public Areas. These areas may or may not be equipped with physical security features.

Security Areas – The term security area refers to a physically defined space, identified by posted signs and some form of access control, containing SNM, classified matter, and/or U.S. Government property. There are two main types of security areas at SNL**:**

1. **Property Protection Area** (PPA) – An area established for the protection of DOE property. It may be established to protect against damage, destruction, or theft of Government-owned property.
2. **Limited Area** (LA) – A type of security area having Physical-Security-sanctioned boundaries defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized people to classified matter or SNM.

Secure Storage Areas – An approved storage area that includes high-security locks, physical barriers, special access requirements, and an intrusion alarm system. Secure storage areas include Vault-Type Rooms (VTR)/SCIF/Special Access Program (SAP).

Subcontractor personnel will comply with all requirements for designated security areas. In addition, subcontractor personnel will:

- Have the appropriate clearance (i.e., DOE personnel security clearance) for the security area, or be properly escorted within the security area.
- Adhere to all requirements for escorting individuals who are not authorized to be in a security area unescorted.
- Adhere to the posted requirements for entering any security area (e.g., clearance status, badge access status, training, and inspections).
- Use a badge valid for entering a security area and display the valid badge at all times, photo side out, above the waist, and in front of the body while in that area.
- Do not introduce prohibited articles into SNL-controlled premises. Do not introduce controlled articles into limited areas or secure storage areas without prior authorization.
- Cooperate with SNL security police personnel during badge checks and searches of vehicles, persons, and/or hand-carried items being brought into or out of a security area.
- Do not park or position equipment, portable toilets, or any other obstruction within 10 feet of security fencing.

WHO	General Access Area		Security Area			
	Public Badge is not required	Non-Public Badge is required	Property Protection Area (PPA) Badge is required	Limited Area (LA) Badge & PIN ARE required		Vault Type Room (VTR) Badge & PIN ARE required
	No Classified Processing				SECURE SPACE	
Q-cleared individual (with SNL LSSO badge or DOE HSPD-12 credential)	✓	✓	✓	✓	✓	✓ Access list or escort required
L-cleared individual (with SNL LSSO badge or DOE HSPD-12 credential)	✓	✓	✓	✓	✓	✓ Access list or escort required
Uncleared individual (with SNL LSSO 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 a full version of Sandia's COE (e.g. Windows laptops, Macbooks)	✓	✓	✓	✓	✓	NO, unless so authorized
Sandia-owned mobile devices* (e.g. Sandia iPads, iPhones)	✓	✓	✓	✓	NO	NO
Non-Sandia mobile devices* (e.g. cell phones, tablets, fitness trackers, smart watches)	✓	✓	✓	✓	NO	NO
Simple electronic devices (e.g. non-BT key fobs, garage door openers, calculators, radios)	✓	✓	✓	✓	✓	✓
Controlled articles† that **do not meet the definition of mobile device*** (e.g. cameras, lab equipment)	✓	✓	✓	✓‡	✓‡	✓‡
Electronic medical devices (including those capable of transmitting or storing data)	✓	✓	✓	✓	✓	✓ Must notify custodian
Prohibited articles (e.g. firearms, weapons, alcohol, marijuana, illegal/unprescribed drugs)	NO	NO	NO	NO	NO	NO

Note: Electronic medical devices require notification to the owner of the Vault Type Room.

8.2. Automated Access Control

For PPAs, automated access is controlled using a badge swipe or contactless badge reader. For automated access into LAs, contractors are required to swipe or use the DOE PIV credential-compliant contactless badge reader and input their personal identification number (PIN). Access is granted if the individual's badge authorization is active, the security clearance level is appropriate for the area, and, for LA access, the PIN entered matches the one on record.

8.3. Vehicles in Limited Areas

8.3.1. *Personal Vehicles*

Subcontractor personnel with medical disabilities may gain access to a LA in their personal vehicle to use "accessible" parking when they possess a State of New Mexico Handicap parking

placard that includes a photo, a permanent handicap license plate and registration, or a SNL Handicap/Temporary Medical Placard issued by SNL Medical.

All personnel entering the LA are required to ensure any electronic devices have Bluetooth and Wi-Fi turned off. Failure to do so prior to entering a LA is reportable to SNL SIMP.

8.3.2. *Subcontractor Vehicles (Construction/Maintenance and Service/Delivery)*

Subcontractor vehicles are admitted into LAs only on official business, and when either the driver or driver's escort is properly badged. Vehicles are subject to entry and exit inspections at the security area boundary. Requirements for construction/maintenance and service/delivery vehicles are included in applicable procedures of the SNL S&S Policy Area, which requires:

- Presenting work orders, invoices, shipping documents, or other proof of the work or service to be performed.
- Having company identification media affixed to their vehicles (e.g., decal with company logo).

8.4. CONTROLLED ARTICLES

Controlled articles are those items that have the potential to record, store, or transmit information electronically without authorization. Examples include, but are not limited to:

- GPS units
- Cellular phones
- Blackberries
- iPhones
- Cameras
- Fitness activity trackers
- Tape recorders
- iPads
- Digital picture frames
- MP3 players

Subcontractor personnel must comply with the physical security requirements of the SNL facility at which they are performing classified work.

8.4.1. *SNL-Owned Electronic Devices*

SNL-owned portable electronic devices allowed by Corporate Policy, or approved through the Controlled Articles Registration Process, may be brought into LAs, as long as they are clearly identified as government-owned property (e.g., labeled with an S number or blue property sticker). However, transmitting capabilities must be turned off, such as Bluetooth and Wi-Fi. Subcontractor personnel must work with their SNL manager to submit a Controlled Articles Authorization Request to obtain the required authorization prior to using controlled articles in LAs or more restricted areas at SNL.

8.4.2. *SNL-Owned Computer Media*

Use of U.S. Government or SNL-owned computer media such as thumb drives, CDs, or removable hard drives, with SNL computing resources are identified as government or SNL

property, if they were obtained through proper procurement channels. These media are used and permitted to perform SNL work.

8.5. Prohibited Articles

A prohibited article is any item administratively restricted from being introduced onto SNL-controlled premises. For government-owned prohibited articles required for official business, guidance is provided below.

- Prior to procuring, storing, or using hazardous materials, subcontractor personnel must obtain the required authorization, and implement relevant control measures defined in applicable SNL Safeguards & Security Policy.
- Prior to procurement, storage, or use within security areas of a prohibited article not governed by SNL Safeguards & Security-related policies, subcontractor personnel must consult with SNL Physical Security.

All personally owned items that meet the definition of "prohibited article" are prohibited on SNL-controlled premises. Examples include, but are not limited to:

- Explosives.
- Firearms.
- Instruments or material likely to produce substantial injury to persons or damage to property.
- Controlled substances (e.g., illegal drugs and associated paraphernalia).
- Alcohol.
- Hazardous radiological, chemical, or biological materials.
- Any other items prohibited by law.

8.6. Personally Owned Portable Electronic Devices (PEDS)

Personally Owned Electronic Devices (PED) is a generic term for small, easily transportable electronic items that are equipped with the capability to process, store, transmit, receive, and/or manipulate electronic data. SNL has authorized the admittance and use of non-SNL owned PEDs on SNL-controlled premises up to and including LAs.

Subcontractor personnel that are considered a Member of the Workforce may bring their personally owned PEDs into a LA if they:

- Are a U.S. citizen.
- Are DOE L or Q cleared.
- Are not disqualified by the eligibility criteria listed below.

The following are not eligible to bring in personally owned PEDs into a LA:

- Subcontractor personnel who cannot complete PEDS100 online.
- Subcontractor personnel who are foreign nationals.
- Subcontractor personnel who are uncleared.
- Visitors to SNL.

Subcontractor personnel that meet the criteria must read and acknowledge the PEDs Rules of Use (PEDS100) in SNLs TEDS prior to carrying or using a non-SNL owned PED in a SNL LA. There is not an offline alternative to completing the PEDS100 course.

PEDs usage at SNL is voluntary and a privilege that may be revoked by SNL at its discretion without prior notice and at any time. Subcontractor personnel who avail themselves of the privilege to use PEDs at SNL assume the risk for such usage, and SNL is not responsible for loss, damage or theft of personally owned equipment or data occurring as a result of PEDs usage at SNL.

9.0 INTELLIGENCE WORK

If the SNL subcontract requires access to intelligence work, the company has additional security requirements specified below.

9.1. PHYSICAL SECURITY

9.1.1. *Security Areas*

The company will follow internal procedures for physical security currently established on Intelligence Community Directives (ICDs), Director of Central Intelligence Directives (DCIDs), and Director of National Intelligence (ODNI) policy documents for the protection of classified in support of the SNL subcontract which includes other government agency information and property utilized in performance of the subcontract.

9.1.2. *Controlled Articles/Portable Electronic Devices*

Secure areas for intelligence work have additional requirements for controlled articles and portable electronic devices. Subcontractors are responsible for knowing these additional requirements and for contacting FIE security personnel regarding controlled article/portable electronic device questions.

9.2. INFORMATION SECURITY

9.2.1. *Classification Guidance*

Subcontractor personnel will ensure that the DCs, providing classification guidance regarding intelligence work, are authorized to do so.

9.3. PERSONNEL SECURITY PROGRAM

9.3.1. *General Requirements for DOE Personnel Security Clearances*

Subcontractor personnel accessing Sensitive Compartmented Information (SCI) under the SNL subcontract will also have documented SCI access. Access to classified information must not be permitted until the proper DOE personnel security clearance and accesses have been granted.

9.3.2. *DOE Personnel Security Clearance Types and Access*

Personnel security clearances denote an individual's eligibility for access to a particular level and category of classified information or material. If an individual performing on the subcontract has any clearance or access suspended or terminated, due to derogatory information, the FSO must report this information to the SNL Special Security Officer.

FSO is responsible for notifying the FIE Special Security Office as soon as it is known that an SCI is no longer needed. An SSO/ASSO will contact the individual to schedule a debrief and collect any SCI badges. Reasons for SCI debrief include:

- Subcontract and/or employment is terminated.
- Access is no longer required (change in job, in scope of work, etc.)
- Q clearance is terminated, suspended, or revoked.

9.3.3. *DOE Security Badges*

Subcontractor personnel will be required to obtain and use an additional badge for entering SCIFs. This badge will be issued by FIE Visitor Control and must be worn above the waist and visible while in a SNL SCIF. FSO is responsible for ensuring that all badges are returned to the FIE Special Security Office when no longer needed.

9.3.4. *Polygraph Designated Positions*

Subcontractor personnel applying for or maintaining SCI access are considered to be in Polygraph Designated Positions and are subject to polygraphs.

9.3.5. *Personnel Security Clearance Suspension, Revocation and Denial*

Upon receipt of notification of an individual's security clearance suspension, the FSO must ensure that the individual is precluded from access to classified information and SNM. Suspension, denial, or revocation of an individual's security clearance does not preclude the company from assigning or transferring the individual to duties that do not require a security clearance. Notify the SNL Special Security Officer of these actions when they involve personnel assigned to work on SNL intelligence work subcontracts.

9.4. Safeguards & Security Awareness

DOE cleared subcontractor personnel assigned to perform work on a SNL classified subcontract involving intelligence work shall receive the required security briefings identified by applicable ICDs/DCIDs. An initial briefing, annual security refresher briefing, and a termination briefing are required. Additional briefings/trainings will be assigned to subcontractor personnel as required.

9.4.1. *Reporting Requirements*

All applicants and holders of a SCI are required to report any information that they believe raises a potential security concern about themselves or another clearance applicant/holder as outlined in ICD/DCIDs. The FSO must ensure that all persons under their cognizance are aware of and fully comply with these reporting requirements and must assist individuals as necessary.

As outlined in ICDs/DCIDs, the FSO must ensure that all persons under their cognizance are aware of, and fully comply with, these reporting requirements, and must assist individuals as necessary. Personnel who hold SCI access are subject to the reporting requirements in accordance with applicable ICDs/DCIDs and will report to the agency which granted SCI access and SNL Special Security Officer through the FIE reporting system.

9.5. Cyber Security

All cyber systems located onsite at SNL, used to collect, create, process, transmit, store, and disseminate classified intelligence data must be approved under the auspices of the SNL FIE Information System Security Manager (ISSM). Subcontractor personnel will adhere to all local and IDC/DCID requirements for applicable cyber systems.

10.0 References

10.1. External Source (Requirements) Documents

In addition to the list of applicable DOE Directives (or successor documents that may superseded these requirements) referenced on the Security Toolcart Flowdown of Requirements webpage, the contractor shall also comply with referenced or supplementary directives, which are invoked by a Contractor Requirements Document (CRD). DOE establishes requirements for contractors (i.e. SNL) in the form of contractor requirements documents. The contractor (i.e. SNL) is responsible for flowing down requirements to subcontractors and lower-tier subcontractors, when applicable, to ensure compliance with the terms and conditions of the subcontract.

10.2. Related Documents

- SNL General Provisions Section II Terms & Conditions
- 10 CFR 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*

- DEAR 952.204-2, *Security Requirements*
- DEAR 952.204-70, *Classification/Declassification*
- DEAR 952.204-72, *Disclosure of Information*
- Atomic Energy Act of 1954, as amended
- Executive Order 12829, *32 CFR Part 2004, National Industrial Security Program*
- Executive Order 12968, *Access to Classified Information*
- Executive Order 13526, *Classified National Security Information*
- Executive Order 13556, *Controlled Unclassified Information*
- Title 18, United States Code Section 798, *Disclosure of Classified Information*

11.0 RELATED TOOLS & RESOURCES

Below are tools available to help you find documents and other helpful items:

- SNL Security Toolcart
- SNL External Corporate Forms
- Office of the Environment, Health, Safety and Security S&S Policy Information Resource
- DOE Directives, Delegations and Other Requirements

Sandia National Laboratories Security Connection Help Desk

SNL has a team of individuals available to answer your security questions. Security Connection hours of operation are 8:00 AM - 4:00 PM (Mountain Time) Monday through Friday. If no Security Connection Representatives are available, they will respond to your request within 24 hours or the next business day. Contact Security Connection at 505-845-1321 or via email at security@sandia.gov.

ACRONYMS

Acronym	Term
CFR	Code of Federal Regulations
CI	Counterintelligence
CMPC	Classified Matter Protection and Control
CRD	Contractor Requirements Document
CSA	Cognizant Security Authority
CSCS	Contract Security Classification Specification
CSM	Contract Security Management
CSMO	Contractor Senior Management Official
DC	Derivative Classifier
DCID	Director of Central Intelligence Directives
DEAR	U.S. Department of Energy Acquisition Regulation
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DRO	Designated Responsible Office
DSS	Defense Security Services
FCL	Facility Clearance
FDAR	Facility Data and Approval Record
FIE	Field Intelligence Element
FIO	Foreign Interactions Office
FNR SP	Foreign National Request Security Plan
FOCI	Foreign Ownership, Control, or Influence
FSO	Facility Security Officer
ICD	Intelligence Community Directives
IOSC	Incidents of Security Concern
KMP	Key Management Personnel
NNSA	National Nuclear Security Administration
ODNI	Office of Director of National Intelligence
OPSEC	Operations Security
PO	Purchase Order
S&S	Safeguards and Security
SAP	Special Access Program

Acronym	Term
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCORE	Sandia Contractor Review and Evaluation System
SP	Subcontracting Professional
SDR	Sandia Delegated Representative
SFO	NNSA Sandia Field Office
SNL/CA	Sandia National Laboratories, California
SNL/NM	Sandia National Laboratories, New Mexico
SNM	Special Nuclear Material
SRN	Sandia Restricted Network
SRP	Security Requirement Plan

DEFINITIONS

Term	Definition
Clearance Denial	A determination made by DOE to deny access authorization to classified or special nuclear materials.
Clearance Revocation	Final determination made by DOE to deny access authorization to classified or special nuclear materials.
Clearance Suspension	A preliminary removal of access authorization by DOE pending a final determination.
Cognizant Security Agency	Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. These agencies are: The Department of Defense, Department of Energy, Central Intelligence Agency and the Nuclear Regulatory Commission. The Secretary of Energy is the Cognizant Security Authority for DOE. *Sandia National Laboratories identifies the Department of Energy (DOE) as their CSA.*
Cognizant Security Office	The office assigned responsibility for a given security program or function. Where DOE cognizant security office is stated, the reference is to a Federal activity. *Sandia National Laboratories identifies the Sandia Field Office (SFO) as their CSO.*
Company	For the purposes of this document, the term company is synonymous with subcontractor, lower-tier subcontractor, facility, business, or firm, and applies regardless of the structure of the company (i.e., corporation, partnership, university, etc.).
Controlled Articles	Articles that are controlled because of their potential to be used to record, store, 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). Government-owned computers procured thorough SNL's JIT purchasing system are exempt from controlled-article registration requirements.
Facility Clearance	A Federal or contractor facility must be granted (also known as registered) approval to access, receive, generate, reproduce, store, transmit, or destroy classified matter, nuclear material, other hazardous material presenting a potential radiological, chemical, or biological sabotage threat; and/or NNSA property of significant monetary value. The approval is recognized as a facility clearance (also referred to as contractor company clearance).
Facility Security Officer (FSO)	A U.S. citizen with a security clearance equivalent to the facility clearance who is assigned the responsibility of administering the requirements of the safeguards and security program in the facility.
Flow-Down of Requirements	Requirements by which the parties incorporate the terms of the general subcontract between the subcontractor and the lower-tier subcontractor into the lower-tier subcontractor agreement. Such provisions state that the lower-tier subcontractor is bound to the subcontractor in the same manner as the subcontractor is bound to the owner of the prime subcontract. These provisions help to ensure that the lower-tier subcontractor’s obligations to the subcontractor mirror the subcontractor’s obligations to the owner.

Term	Definition
Foreign National	Any person who is not a U.S. citizen, which includes all lawful permanent residents. For the purposes of DOE O 142.3, Unclassified Foreign National Access Program, a foreign national is a person who was born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.
FOCI Mitigation	If DOE determines that a company is under FOCI, DOE will determine the extent to which and the manner in which the FOCI may result in unauthorized access to classified information or SNM and the types of actions that will be necessary to mitigate the associated risks to a level deemed acceptable to DOE.
General Access Area (GAA)	An area established to allow access to certain areas with minimum security requirements as determined by the Officially Designated Security Authority (ODSA). At SNL, there are two types of GAAs: Public and Non-public Areas. These areas may or may not be equipped with physical security features.
Illegal Drugs	Specific drugs, the possession or distribution of which is unlawful under the Controlled Substances Act or other provisions of Federal law. This term does not include controlled substances used with a valid prescription or other uses authorized by law. Use of Schedule I drugs by individuals in federally regulated workplaces is unacceptable, and any individual who tests positive for a Schedule I drug will be deemed to have a verified positive drug test.
Incident of Security Concern	Events that are of concern to the DOE safeguards and security program that warrant preliminary inquiry and subsequent reporting.
Need to Know	A determination made by an authorized holder of classified and/or sensitive unclassified information that a prospective recipient requires access to the information in order to perform or assist in a lawful and authorized governmental function. It is also a determination that the prospective recipient requires access to (including incidental access) knowledge or possession of the information to perform tasks or services essential to the fulfillment of a classified or sensitive unclassified contract or program. Need to know for the National Nuclear Security Administration (NNSA) includes physical access to storage areas as well as to information.
Non-Possessing Facility	A contractor that will not access, receive, generate, store or handle classified matter (to include classified meetings), or nuclear material at the contractor's place of business, but will require personnel security clearances for the contractor's employees to perform classified work at other cleared facilities, the Contractor must be processed for a facility clearance at the appropriate level and be designated as a non-possessing facility.
Personnel Security Clearance	For the purposes of this document, the term personnel security clearance is synonymous with DOE security clearance, access authorization, and clearance. An administrative determination that an individual is eligible for access to classified matter and/or special nuclear material. In DOE and NRC, security clearances are designated as Q and L. Security clearances at other Federal agencies are designated as Top Secret, Secret, or Confidential indicating that the recipient is approved for access to National Security Information or Formerly Restricted Data at a classification level equal to or less than his/her security clearance level.
Prescription Medication	Legally prescribed drugs which require a physician's order to obtain.

Term	Definition
Proprietary Information	[Procurement def] - Information contained in a bid or proposal, cost or pricing data, or any other information submitted to Sandia by a subcontractor or partner and designated as proprietary. Proprietary may be defined as information (data) that constitutes a trade secret and/or information that is commercial or financial and confidential or privileged. [Security def] - Information which contains trade secrets or commercial or financial information which is privileged or confidential, and may only include such information which: has been held in confidence by its owner; is of a type which is customarily held in confidence by its owner; has not been transmitted by the transmitting party to other entities (including the receiving party) except on the basis that it be held in confidence; and is not otherwise available to the receiving party from another source without restriction on its further dissemination.
Sandia Controlled Premises	Real property or buildings (or portions thereof) owned, leased, or withdrawn by or permitted to DOE and designated for Sandia National Laboratories. Includes leased or permitted commercial space (e.g., Research Park in Albuquerque, NM). It does not include sites where Sandia National Laboratories performs work but DOE has no legal interest (e.g., a courtesy office provided to a visitor on the premises of a technology transfer partner).
Security Requirements Plan (SRP)	A formal risk management plan that outlines the security responsibilities of the subcontractor, and if applicable, depicts the existing condition of site protection programs in place for meeting those requirements to ensure protection of Department assets and compliance with applicable security requirements.
Self-Assessment	An internal integrated evaluation of all applicable S&S topical areas at a contractor facility or site, to determine the overall status of the S&S program at that location and verify that S&S objectives are met.
Sensitive Compartmented Information Facility (SCIF)	An accredited area, room, group of rooms, or installation where Sensitive Compartmented Information may be stored, used, discussed, and/or electronically processed.
Special Access Program	A program created for a specific segment of classified information that imposes safeguards and access requirements that exceed those normally required for information at the same classification level and/or category.
Subcontract	Subcontract, Purchase Order, Price Agreement, Lower-Tier Subcontract, Ordering Agreement, or modifications thereof. Also, means any lower tier subcontract as indicated.
Subsidiary	A company having the majority of its stock owned by another company.
Substance Abuse	The use of controlled substances, drugs, or alcohol in violation of any state or federal law, including, ingestion to the point of individual impairment or exceeding the legal limits of state or federal laws.
Unclassified Controlled Information (UCI)	Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect the national security, Sandia National Laboratories, or our business partners. Identification and protection of this type of information is required by the code of federal regulations, public law, governmental directives, DOE Orders, subcontracts with business partners, or Sandia's processes to protect commercially valuable information.

CHANGE HISTORY

28 January 2021—Administrative Revision

What Changed

Modified:

	Hyperlinks to FSO Toolcart were changed to Security Toolcart sandia.gov/security
4.1	Reference to DOE O 232.2A, Chg 1, Occurrence Reporting and Processing of Operations Information
4.5	Reference to current Laboratory Policy EHS002.2
5.1.3	Reference to reflect SEC100 can be taken on the Security Toolcart (SON)
7.1	Reference to reflect training title for CLA102
7.3	Reference to current Laboratory Policy SS003
7.4	Reference to current Laboratory Policy IT012
7.4.1	Reference to current Laboratory Policy IT023
8.1	Definitions of PPA and LA
	Who and What Can Where graphic to most current
10 & 11	Broken hyperlinks

---

02 October 2018—Substantive Revision

What Changed

Modified:

Title	Changed title to Non-Possessing Subcontractor Security Requirements Plan
1.1	Content modified for clarity.
1.2	Explained role of CSM and provided program contact information.
2.1	Provided definition and role of the FSO.
2.2.2	Added “DOE” when FCL is referenced.
	Clarified SCORE notification process
2.2.3	Modified definition of “security incident”
	Removed the FSO and subcontractor company responsibility for funding SIMP inquiry travel.
	Removed FSO responsibility to report Incidents involving intelligence information or occurring inside a Sensitive Compartmented Information Facility (SCIF) to SIMP
2.3.1	Moved Security Management in Contracting to beginning of section.
2.3.2	Clarified who the plan is applicable to and defined what a non-possessor is.
2.3.5	Replaced organization with contract company.
2.3.12	Added link to SF 328.
2.3.15	Removed detailed list of significant changes and referenced SF-328
3.0	Provided an introduction to the Physical Security program and provided contact information.
3.1	Modified definitions for property protection area and limited area.
3.1	Updated section to match current corporate procedure.
3.2	Added information regarding government-owned electronic devices and computer media.
3.3	Modified definitions for property protection area and limited area.
3.3.5	Added reference to applicable DEAR clause
	Added requirement to verify no illegal drug use in past 12 months
3.3.8	Clarified when subcontractor has to be removed from subcontract based on clearance status
3.4	Added guidance related to government-owned prohibited articles for official business.

3.5	Updated section to match current corporate guidance.
4.0	Renamed section from Information Protection to Information Security. Clarified no processing of clearance until 12 months have passed from use of illegal drugs
4.3	Explained purpose of CMPC and listed required training.
4.4	Listed OUO training course.
4.4.3	Added information regarding disseminating OUO vie mail, email and fax.
4.4.4	Updated section to match current corporate procedure.
4.7	Added documented admittance of illegal drug use as an additional consequence for site removal
5.1	Documented purpose for DOE security badges and graphic of SNL badge types. Provided link to Contractor Badge Request and ECN Account Process Inserted information related to identity documents required in order to pick up SNL issued badge. Provided guidance regarding badge retrieval and responsibilities of FSO
5.2	Provided purpose of DOE personnel security clearances.
5.2.2	Modified link to SF 312 and documented purpose of the form.
5.2.3	Modified consequences of substance abuse.
5.2.4	Removed detailed list of reporting requirements and linked to DOE/SNL Reporting Requirements Matrix. Updated link to DOE F 5631.34
5.2.5	Updated link to DOE F 5631.29 and listed new form name
5.2.6	Provided definitions for clearance suspension, clearance revocation and clearance denial
5.3.2	Clarified that contractors may not be processed as visitors when on an active SNL contract.
5.4	Provided definition for foreign national.
6.0	Renamed section to Security Briefings & Training. Updated link to DOE F 5631.29 and listed new form name. Added Facility Security Officer Overview Training.
7.0	Added Intelligence Work to clarify addition requirements for SNL contracts associated with intelligence work.
9.3.2	FSO responsibilities related to subcontractor SCI access needs.
9.3.3	Instructions for FSO to return badges issue by the FIE Special Security Office.
9.5	Cyber Security FIE requirements

Deleted:

1.3	Records
2.1	Protection
2.3.5	Personnel Security Clearances
2.3.15	**Note**: If a facility is under DSS cognizance, all changes must be reported through e-FCL; however, as a courtesy, SNL requests that all significant changes also be reported to SNL to ensure conformity
4.2	Classification Guidance
4.2.2	Certifications
4.2.3	Using Published Classification Guidance
4.2.4	Derivative Declassification
References	DOE M 470.4-1, Chg. 2, *Safeguards and Security Program Planning and Management,* DOE M 470.4-6, Chg. 1, *Nuclear Material Control and Accountability,* DOE O 142.1, *Classified Visits Involving Foreign Nationals,* DOE O 472.2, *Personnel Security,* DOE O 475.2A, *Identifying Classified Information,* NAP 70.4, Chg. 1, *Information Security*

Reason for Changes

To flow-down current security requirements to SNL contractor and sub-contractor personnel.

30 November 2016 — Administrative Change

At the suggestion of Requirements Management, and with concurrence of the responsible programmatic SME, the document was marked with a disclaimer advising readers to consult the SME regarding specific information while the document is undergoing substantive review.

---

08 April 2013 — New Document

This is a new document.