Sandia National Laboratories

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

SUBCONTRACTOR CERTIFICATION

Revision Date: June 2025

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: Nick Atencio (9213)

Issue Date: 08 April 2013

Revision Date: 29 April 2025

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

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 US 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's 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 (PLN) 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 US 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 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 Safeguards and Security [S&S] policies, Environment, Safety, and Health [ES&H] policies, 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 PLN.

If a subcontractor violates DOE policy and/or security requirements, that subcontractor must immediately contact their respective SNL management representative, subcontracting professional (SP), SDR, and CSM to report the violation. Failure to report may result in suspension of the FCL, a Cure Notice (used when a subcontractor has failed to meet the requirements of their contract), or termination of the subcontract (see Section 2.3.2.6, "DOE Facility Clearance Terminations").

In addition to the requirements in this PLN, any subcontractor, low-tier subcontractor, or sub-agreement involving approved safeguarding of Restricted Data (RD) or other classified information, must also comply with DOE regulations in 10 Code of Federal Regulations (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 PLN upon signature by authorized company key management personnel (KMP) (see Section 2.3.2.1, "Key Management Personnel") and the FSO. Questions about the requirements conveyed in this PLN may be directed to SNL CSM via email at farateam@sandia.gov.

1.2. APPLICABILITY

This plan applies to all non-possessing subcontractors and any lower-tier subcontractors performing work under a SNL subcontract.

1.3. OWNERSHIP

The manager of Contract Security owns this PLN. The SNL CSM team manages this plan, and with assistance from S&S program subject matter experts (SMEs), maintains, reviews, and updates it as necessary, but no less than every 2 years.

2.0 PROGRAM MANAGEMENT OPERATIONS

2.1. PROTECTION PROGRAM MANAGEMENT & ADMINISTRATION

The overall day-to-day security responsibility for the subcontractor facility rests with the appointed company Facility Security Officer (FSO). The company shall appoint an FSO in writing[1]. The FSO must be a US citizen, an employee of the company, and must obtain and maintain a DOE personnel security clearance commensurate with the facility clearance (FCL).

[1] If a facility is under Defense Counterintelligence and Security Agency (DCSA) cognizance, the DCSA Industrial Security Representative will facilitate the appropriate training requirements. Companies who hold an active US Department of Defense (DOD) facility clearance (FCL) are not required to complete additional training; however, the appointment or documentation of the appointed FSO may be required.

The FSO is assigned the responsibility of administering the requirements of the Safeguards and Security (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 their 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 (PLN) as well as the standards set forth in the attached references.

2.2. S&S CONTRACT SECURITY

2.2.1. Self-Assessment Program

Surveys and self-assessments 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, Contract Security Management (CSM) will conduct a Periodic Security Review (PSR) 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 to the FSO. On a case-by-case basis, results from the PSR may be shared with the Sandia-Delegated Representative (SDR), subcontracting professional (SP), S&S subject matter experts (SMEs), and others, as appropriate.

2.2.2. Findings and 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.

If, while conducting a self-assessment, the contractor finds that they are out of compliance with security requirements outlined in this PLN, the contractor is responsible for identifying the non-compliance and must complete the following.

1. Develop a process of corrective actions to address the non-compliance. Through this process the contractor will:
    a. Identify and document the nature of the non-compliance in an associated report.
    b. Create an action plan that will address and correct the non-compliance in a timely manner.

c. Prove that the actions within the plan are effective and sustainable.
d. Retain the self-identified finding and action plan in accordance with records-retention requirements.

2. Notify SNL of any currently open findings self-identified during their PSRs and other assessments.

The contractor will conduct analyses of non-compliances to determine if systemic and/or systematic factors underlie the self-assessment findings. If such factors are identified, the contractor's action plan must address them.

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.

Table 1. Escalation Process

Notification	Notification/ Distribution to	Content
Initial (First)	FSO	• Correspondence outlining requirements and importance of compliance and reporting of issue. • The FSO will be given 5 working days (or agreed upon due date) to take action on the issue. • The FSO is advised that if action is not taken within the maximum time allowed, the second notice (as described below) will result in notification to the SDR and SP.
Second	FSO, SDR, and SP	• Correspondence outlining requirements and importance of compliance. • Request to SDR and SP to address the matter with the FSO. • The FSO will be given 5 working days (or agreed upon due date) to take action on the issue. • If action is not taken, the company senior management official (CSMO), SDR, and SP will be notified for appropriate action and possible suspension or termination of the DOE FCL.
Third	FSO, CSMO, SDR, and SP	• Correspondence outlining requirements and importance of compliance. • Request to CSMO, SDR, and SP to address the matter with FSO, to include an advisory that, if action is not taken within 5 working days (or agreed upon due date), the fourth notice (as described below) will result in suspension or termination of the DOE FCL.

Final	FSO, CSMO, SDR, and SP	• Notification, at the discretion of CSM, to suspend or terminate the DOE FCL. • A separate communication is sent to DOE to suspend or terminate the DOE FCL.

2.2.3. Incident Reporting and Management

Incidents of Security Concern (IOSCs), 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 but are not limited to circumstances 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 programs' 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).

Subcontractors and any lower-tier subcontractors should strive to avoid and prevent security events, incidents, and adverse impacts to national security. Suspected or actual IOSCs must be immediately reported as stated below (also see: DOE and Sandia Reporting Requirements).

- At SNL/NM—contact the Security Incident Reporting Pager at 505-283-SIMP (7467).
- At SNL/CA—contact the CA inquiry official (IO) at 925-294-2600.
- At either site (SNL/NM or SNL/CA)—contact Security Connection at 321 from an SNL landline or 505-845-1321 from any phone.

An SNL IO will lead and organize an 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, DC 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 voicemail. 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 IOs 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 Counterintelligence and Security Agency (DCSA) 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 their 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 PSRs 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 US, Puerto Rico, or a US 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 PSR 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 DCSA cognizance, the DCSA Industrial Security Representative will facilitate the FOCI process. Companies who hold an active US DOD FCL through the DCSA 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 US 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 subcontractor's 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. 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.

No classified work may begin under a subcontract until the company has been registered and approved by DOE. Although SNL has an established FCL, the FSO must ensure that tier subcontract companies with established subcontracts have been properly registered.

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 (CSO), must be designated as KMP. At a minimum, KMP must include the CSMO 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 same level of the company's highest interest clearance level. 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 with DOE 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 to be excluded from access to classified information to be disclosed to the company.

Note: If a subcontractor is under DCSA cognizance, DOE requires that KMP must be in process for reciprocal DOE clearances. This is a requirement as part of the FCL process.

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. If cleared work will be further subcontracted, each tier subcontract company must possess a separate FCL under which personnel security clearances are requested and granted.

2.3.2.3. Facility Data and Approval Record (FDAR)

The purpose of the DOE F 470.2, *Facility Data and Approval Record (FDAR)*, is to document the approval or termination of the FCL, company information, and approved classified access levels. DOE registers the facility approval by entering the 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. Failure to do so could result in the suspension of the FCL, a Cure Notice, or termination of a subcontract.

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 (CSCS)

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", within each contract), part of the subcontract and is binding. The subcontractor company is required to adhere to the security specifications outlined in the CSCS and this PLN.

Subcontractors who further subcontract are responsible for flowing down the security clauses and requirements in a contractually binding manner. In addition, any lower-tier subcontractor that is issued a contract requiring personnel clearances must submit a CSCS form to specifically reflect the lower-tier subcontract and it 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), 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 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, PSR, inquiry, inspection, or evaluation may result in the suspension of a FCL 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 PLN.
- 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 their 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 (OGAs) 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 request transfer of the FCL to another DOE Designated Responsible Office (DRO).

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 FCL Subcontractor facilities holding a FCL must submit written reports of changed conditions and anticipated changes affecting the FCL.

If a facility is under DCSA cognizance, all changes must be reported to their representative. 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 CSO) through e-FOCI, which can be found on the FSO Security Toolcart.

A detailed list of significant changes that require reporting are outlined in the Contractor Requirements Document section of DOE O 470.1A, *Safeguards and Security Program Management Operations*, 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, the Federal Trade Commission, or the Department of Justice.

2.3.3.2. Reporting Anticipated Changes

Anticipated changes and actions are events that arise when the subcontractor or any of its tier parents enters 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 an email to 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-US 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-US citizen(s).

2.3.3.3. Reporting Other Changes

The FSO must immediately provide written notification to CSM via an email to farateam@sandia.gov and e-FOCI (if applicable) 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.
  Note: 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 US 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 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 DOE Acquisition Regulation (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. All lower-tier subcontractors must be processed for their personnel clearances under their respective company's FCL. Lower-tier subcontractors shall not be processed for a personnel clearance under the prime subcontractor's FCL. Rather, each lower-tier subcontractor will have their own personnel clearances processed under their respective FCL.

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 Clause 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 Controlled Unclassified Information (CUI), the requirements shall be incorporated in the solicitation and the subcontract.

2) **Determine FCL 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 security requirements plan (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 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

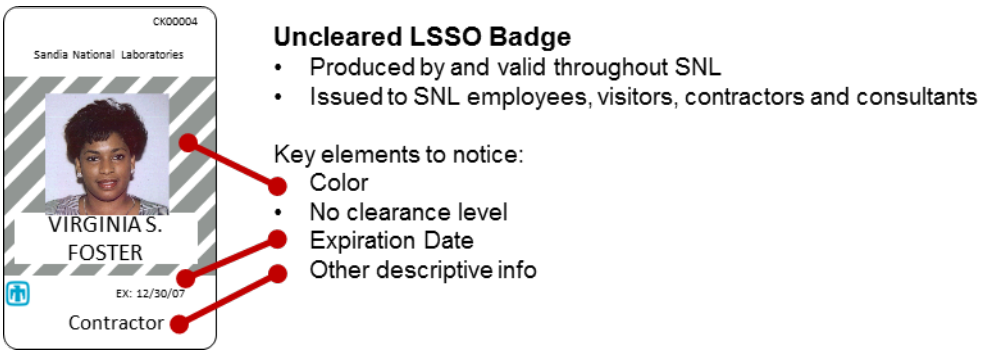
The SNL Background Review Office (BRO) assists SNL employees/sponsors in conducting due diligence reviews of their subcontractor personnel. The BRO also assists with consultants and visitors to understand the people with whom SNL does business. Prior to granting site or Sandia Restricted Network (SRN)/Sandia Classified Network (SCN) cyber access to subcontractor personnel, a check is conducted of public records and commercially available data sources. Any significant criminal information discovered will be verified. Failed validations occur when the BRO does not validate a specific individual to the level requested. In such cases, the SNL employee/sponsor will be notified, a failed validation entry will be made in Enterprise Person (EP), and a security hold will be placed on the individual's badge and/or badge authorization. A passing validation allows the individual to be further processed for access to SNL sites and cyber resources. Granting or denying physical site access is at the sole 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 Identity Verification (PIV) credentials (A.K.A. Homeland Security Presidential Directive 12 [HSPD-12] federal credential) are considered DOE security badges.



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:

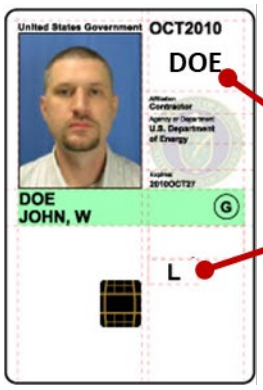
- Color
- No clearance level
- Issue and Expiration Date
- Other descriptive info

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 used to initiate badging requests for US citizen subcontractor personnel. For foreign national (FN) subcontractors, requirements detailed in Section 3.5, "Foreign National Access," must first be met. START requires cyber access to the SRN. Facility Security Officers (FSOs) without SRN access may be sponsored for access, with the concurrence of their Sandia-Delegated Representative (SDR). 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 a START request by an SNL manager, an uncleared badge authorization is initially created. This allows subcontractor personnel to obtain an SNL-issued, uncleared LSSO badge. The LSSO badge is valid and functional only through the expiration date printed on the badge. The date of expiration is determined when the START request is submitted.

Aside from the opportunity for initial uncleared badging for all subcontractors, those who require physical and/or logical access to SNL for greater than 179 calendar days and who are not otherwise in process for a DOE security clearance (i.e., a clearance applicant) must be processed under Uncleared PIV (UPIV) requirements for authorization of long-term uncleared access. As applicable, uncleared subcontractors are notified of their UPIV-related responsibilities and are expected to comply with all related instructions or tasks.

The badging process for subcontractor personnel on a cleared subcontract begins in the same manner as an uncleared subcontract, excluding the UPIV component. 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 previously 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 1 week or until the credential is available. In effect, the credential becomes the subcontractor's permanent cleared security badge.

Prior to a requesting renewal of a cleared badge in START, the contract Period of Performance must be extended by Procurement, the Contract Security Classification Specification (CSCS) must be revised by the SDR and approved by Contract Security Management (CSM), and the subcontractor's EP record must be updated. The SDR, the subcontractor's SNL manager and 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

One's identity must be verified to receive a badge. 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 current and valid 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 (e.g., US passport/card, US military ID) listed on the Department of Homeland Security Form I-9, *Employment Eligibility Verification,* may also be used as proof of identity.

Lost or stolen badges must be reported within 24 hours of discovery through submission of an SF 2730-LSB, *Reporting Lost, Stolen, Forgotten, and Unrecovered Badges.* Forgotten badges should be retrieved if circumstances permit. Otherwise, an SF 2730-LSB is required to obtain a temporary badge. Failure to fill out the required form will result in suspension of the facility clearance (FCL).

Recurrent reports of a lost, stolen, or forgotten badge by or on behalf of subcontractor personnel will result in administrative action consisting of an escalating series of automatic email notifications to management, advising them to conduct and document a discussion on the

importance of safeguarding badges with the badge holder. A delay in issuing a temporary badge may also be imposed.

Subcontractor personnel who find a security badge must promptly return it to the appropriate Badge Office in one of the following ways:

- In person
- In a badge drop box at one of the following locations:
    - Lobby of Innovation Parkway Office Center (IPOC) (SNL/NM)
    - B911 (SNL/CA)
    - Post 17 (SNL/CA)
    - General Access Area (GAA) roadway exit (SNL/CA)
- Via Sandia internal mail, using an Unclassified Controlled Information (UCI) envelope (see Badge/Credential Shipping Addresses)
- Via certified/signature-required delivery, as follows (see Badge/Credential Shipping Addresses):
    - DOE PIV credentials—via US Mail or common carrier (e.g., FedEx, UPS)
    - LSSO badges—via standard US Mail (see Badge/Credential Shipping Addresses)

3.2.4. Returning Badges

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 are promptly returned to the SNL Badge Office, regardless of the expiration date. The FSO is ultimately responsible for ensuring that badges or other credentials granting physical access to DOE/NNSA-owned or -leased facilities 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.

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*.

3.3. DOE Personnel Security Clearances

DOE Q and L security clearances are used at SNL and 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). Classified information categories are designated as Restricted Data (RD), Formerly Restricted Data (FRD), Trans-classified Foreign Nuclear Information (TFNI), and National Security Information (NSI).

The chart below shows the classification levels and categories 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	Increasing Risk
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	

Figure 1. Classification Categories and Clearance Levels

While SNL sponsors and initiates the clearance process for subcontractor personnel, only DOE makes the determination and will grant or deny the clearance request. If subcontractor personnel are hired and placed in a position prior to receiving a clearance, they may not access classified information, matter, or special nuclear material (SNM), until their clearance has been granted. DOE personnel security clearances are processed only for US citizens who are at least 18 years of age.

A company must have a registered, active FCL before their personnel can be submitted for personnel security clearances in performance of 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.

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 or SNM, or controlling dissemination of classified information on a need-to-know (NTK) 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.

Additionally, 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 used to initiate clearance actions for US 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) 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, the same parties will be notified directly by email of any tasks and associated deadlines necessary to complete the clearance request.

3.3.2. Clearance Action Applicant Tasks

The SNL/NM Clearance Office and SNL/CA Personnel Security Office will provide instruction to subcontractor personnel on how to complete all necessary elements of the clearance process, which include:

- SF-86, *Questionnaire for National Security Positions* (QNSP), and other documentation as necessary.
- Drug testing requirement within 90 calendar days of an individual's signed SF-86, *Questionnaire for National Security Positions*.
- PIV enrollment elements (e.g., ID, photo, fingerprints)
- DOE F 472.11, *Security Acknowledgement*.
- Failure to follow Personnel Security timelines could result in the suspension of the company FCL or withdrawal of personnel clearance requests.

3.3.3. Clearance Action FSO Responsibilities

The FSO must ensure that their personnel are advised of and comply with the requirement to properly complete all security forms in a timely manner, and that all related material will 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 also advise their personnel that clearance applicants should maintain copies of completed security forms for their personal records. Deficient security clearance requests will not be processed. If a request is found to be deficient, the FSO must ensure that the request is corrected and resubmitted to the SNL/NM Clearance Office or SNL/CA Personnel Security Office in a timely manner.

During the conduct of all background investigations, FSOs must assist in the timely processing of security clearance actions by ensuring the availability of their employees, as needed, to provide information, participate in personal interviews with investigative service providers, or consult with DOE Personnel Security staff.

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 USC 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. US Citizenship

Subcontractor personnel selected for positions requiring a DOE security clearance must provide evidence of US citizenship. The FSO must verify such evidence, verbally or otherwise, as

acceptable to the SNL party submitting an individual's security clearance processing request via START. Acceptable forms of evidence of US citizenship are listed below.

For subcontractor personnel born in the US, one of the following is required:

- Original or certified US birth certificate.
- Current or expired US passport or passport card.

For subcontractor personnel claiming citizenship by naturalization, the following (showing the individual's name) is required:

- A certificate of naturalization (Form N-550 or N-570).

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

- A Certificate of Citizenship (Form N-560 or N-561).
- *Consular Report of Birth Abroad of a Citizen of the U.S. of America* (State Department form FS 240).
- N-600, *Application for Certificate of Citizenship.*
- A Certificate of Birth (form FS 545 or DS 1350).
- Current or expired US passport or passport card.

Note: Form I-9, *Employment Eligibility Verification*, does not verify citizenship.

3.3.5. Subcontractor Personnel Reviews

In accordance with DOE Acquisition Regulation (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. The background review should be completed prior to selecting the individual for a position requiring a DOE personnel security clearance. Reviews help the company decide 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 Personnel Security 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 5 years and degrees or diplomas granted by an institution of higher learning.
- Contact with listed employers for the last 3 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 of the Civil Rights Act of 1964, and the Age Discrimination in Employment Act of 1967, 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.

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 or CSM, 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.

3.3.6. Clearance Termination

An individual's responsibility to protect classified and sensitive information continues long after they have terminated employment, are separated from SNL, or no longer require a security clearance.

Reasons for clearance termination include:

- Subcontract and/or employment is terminated.
- Clearance is no longer required.
- Access to classified matter or SNM is no longer required.

To simplify the clearance termination process, SEC225, *Security Termination Briefing*, is combined with DOE F 472.12, *Security Termination Statement*. An SNL manager, FSO, or SDR must ensure completion of the following steps:

- The subcontractor whose clearance is being terminated must review and sign DOE F 472.12, *Security Termination Statement,* and *Security Termination Briefing* (SEC225).
    - Though every effort should be made to obtain said signature, if obtaining it is not possible on the completed DOE F 472.12, an explanation is required in the field titled, "If person is not available for signature, provide reasoning below."

    - The person who signs as the Debriefing Official must also ensure that the "Remarks/Reason for Security Termination" field is both accurate and specific, especially when conditions of termination are unfavorable.
    - Under unfavorable circumstances, SNL Ethics/EEO Advisory & Investigative Services must be informed (505-845-9900).
- Sign as the "Debriefing Official".
- Return the completed DOE F 472.12, which is then designated Controlled Unclassified Information (CUI), to the appropriate SNL Clearance Office within 2 working days of termination. Failure to do so will be considered an issue of non-compliance.
    - Submit the form via an encrypted email to clearance-nm@sandia.gov or clearance-ca@sandia.gov, or handcarry. Do not use interoffice mail.

Note: Subcontractors may retain the *Security Termination Briefing* (SEC225) for their records.

3.3.7. Clearance In-Process Withdraw

If a clearance is in process but no longer required (e.g., due to termination of employment), immediately send a notification to clearance-nm@sandia.gov or clearance-ca@sandia.gov with the subcontractor's name, circumstances surrounding the withdrawal, and intent to withdraw the clearance.

3.3.8. Clearance Denials, Suspensions, and Revocations

Adverse security clearance determinations are rendered only by DOE/NNSA and include denials, suspensions, revocations, and administrative terminations for lack of cooperation. In such cases for subcontractors, the applicable SNL manager, SDR, and FSO are notified by SNL Personnel Security, informed (as required) of any associated actions, and must immediately ensure that the individual is precluded from all classified access.

Adverse determinations impact the subcontractor's security clearance eligibility and may, by association, impact their continued access to SNL. While the former is at the sole discretion of DOE/NNSA, the latter is at the discretion of SNL based, in part, on the nature of the contract under which the subcontractor is working, as well as a determination by the SNL FSO (i.e., SNL's Director of Safeguards and Security ([S&S]). All parties, including the affected subcontractor, are informed by SNL Personnel Security of subsequent actions or steps to be taken to determine continued access to SNL.

It is important to note that the subcontractor personnel's employment is an entirely separate matter, at the sole discretion of their employer. SNL has no influence on the employment relationship between individuals and their employers.

An SNL manager, SDR, or FSO may also restrict or withdraw a subcontractor's access to classified without DOE direction. Such action, however, must be immediately reported to SNL Personnel Security.

3.3.9. Clearance Reevaluations/Reinvestigations

As required by federal standards, the SNL Clearance Office will provide instructions to subcontractor personnel who are due for clearance reevaluation/reinvestigation. Selected

personnel must comply with such requests and adhere to deadlines to maintain their security clearance status. The FSO will be copied on all related notifications and must ensure the subcontractor fully cooperates.

3.4. CLASSIFIED VISITS

Classified information and matter must be protected by ensuring that only persons with the appropriate security clearances, NTK, 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 [OGA] 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 coordinates, as necessary, with 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 affiliated with OGAs who hold active non-DOE personnel security clearances and require unescorted access to Sandia-controlled premises for official business of a classified nature. Only a National Technology and Engineering Solutions of Sandia LLC (NTESS) employee can request and host an incoming classified visit on behalf of a subcontractor. SNL management approval is required for incoming classified visits.

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 badged as visitors at SNL.

3.5. FOREIGN NATIONAL ACCESS

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 FNs to its unclassified information, programs, and technologies—and consequently, to SNL sites. However, SNL must ensure that FN access does not pose a risk to national security. Along with other measures, SNL protects information, assets, etc. by establishing an effective identification, verification, tracking, review, monitoring, and approval process for controlling interactions with FNs. All FN subcontractor personnel who require access to DOE sites, information, or technologies—to include remote access—will (in accordance with Lab policy) be coordinated through the Foreign Interactions Office (FIO) at SNL/NM.

3.5.1. Onsite SNL Work

All FN subcontractor personnel are required to have an approved Foreign National Request Security Plan (FNR SP) from the SNL FIO prior to working onsite at SNL. The SNL designated host or SDR is responsible for submitting an FNR SP 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 FN subcontractor personnel at SNL must be a US citizen and an employee of NNSA or SNL. Subcontractor personnel are not authorized to host or co-host uncleared FNs at SNL. Subcontractor personnel may escort uncleared FNs at SNL if they:

- Are identified as an authorized escort on an applicable FNR SP.
- Complete EC100, *Export Control & Foreign Corrupt Practices Act Basics*, along with other required training.
- Possess a DOE-approved standard badge.
- Possess a clearance that is appropriate for the area in which escorting will occur.
- Are a US citizen.

3.5.2. Off-Site SNL Work

All FN subcontractor personnel are required to have an approved FNRSP from the SNL FIO office prior to access. For more on this process, please refer back to Section 3.5.1, "Onsite SNL Work".

Due diligence must be used when sharing information with FNs. 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 (TDPs). 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. 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

The table below exemplifies the different substance testing types and when those tests may occur, based on the requirements that need to be met.

Table 2. 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). The 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.
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's 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, *Procedures for Transportation Workplace Drug and Alcohol Testing Programs*, and 49 CFR 382, *Controlled Substances and Alcohol Use and Testing*) 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, *Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material or Eligibility to Hold a Sensitive Position*. 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 them 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).

4.2.1. Cannabidiol (CBD)

CBD is legal, but only if it includes Tetrahydrocannabinol (THC) under 0.3%. However, no agencies are currently investigating claims by manufacturers that their CBD products contain less than the allowed 0.3%. Consequently, some users of presumed-legal CBD have tested positive for illegal THC levels. Thus, DOE and other federal agencies have conveyed a "buyer beware" warning for those who want to use CBD.

Users of CBD who test positive for THC will be considered to have used an illegal drug. Ultimately, individuals have no legal right to have THC in their systems.

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 take 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 their 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 blood alcohol content (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 SNL110, *Drug-Free Workplace*, awareness training every 2 years. Subcontractor personnel must also provide the MRO with 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 Process EHW002.2, *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 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. FACILITY SECURITY OFFICER (FSO) RESPONSIBILITIES

The FSO is responsible for complying with substance abuse testing reporting notifications. FSOs 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 program staff with subcontractor personnel substance abuse testing reporting notifications if the SNL Drug Testing program 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 program 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 the 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 and Ethics/EEO Advisory and Investigative Services, who will contact the subcontracting professional (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 Sandia-Designated Representative (SDR).

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/EEO 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 Safeguards and Security (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 site as appropriate, or as assigned in SNL's Training and Employee Development System (TEDS) based on the criteria for briefings listed below.

5.1.1. Initial Security Briefing

All subcontractor personnel must receive SEC050, *Initial Security Briefing,* prior to being granted unescorted access to non-public areas at any SNL site. SEC050 must be completed before a badge is issued. The briefing may be found at the Briefings & Trainings page on the SNL Security Toolcart site. Documentation of SEC050 completion is maintained in conjunction with badging records.

5.1.2. Comprehensive Security Briefing

Subcontractor personnel must complete SEC150, *Comprehensive Security Briefing*, prior to or upon clearance grant and before receiving initial access to classified information, matter, or SNM. This requirement is applicable to all subcontractor personnel who are applying for or holding an SNL-sponsored security clearance. Subcontractor personnel will receive an email advising them of this briefing requirement and enrollment instructions.

Cleared subcontractor personnel who have not yet completed this briefing will not be permitted to hold a cleared security badge until they do so. If access is needed prior to the next available briefing, an equivalency process is provided in the clearance grant email, which must be coordinated with SNL Security Awareness (securityed@sandia.gov). Documentation for the completion of SEC150 is maintained in TEDS in conjunction with badging records.

5.1.3. Annual Security Refresher Briefing

All subcontractor personnel who have completed SEC150, *Comprehensive Security Briefing*, must complete SEC100, *Annual Security Refresher Briefing,* at approximately 12-month intervals while they are cleared or pending a clearance. Failure to complete SEC100 may result in badge deactivation.

SEC100 may be completed via TEDS and may also be found at the Briefings & Trainings page on the SNL Security Toolcart site. Documentation of SEC100 completion is maintained in the TEDS.

5.1.4. Security Termination Briefing

All subcontractor personnel must receive SEC225, *Security Termination Briefing*, when a security clearance has been or will be terminated.

SEC225 is provided as an addendum to the DOE F 472.12, *Security Termination Statement*. The combined form may be found at the Briefings & Trainings page on the SNL Security Toolcart site.

The Facility Security Officer (FSO) or Sandia-Delegated Representative (SDR) is responsible for providing the combined form to affected individuals who have been or will be terminated. The SEC225 briefing material is retained by the individual; DOE F 472.12 must be submitted to SNL Personnel Security. Documentation of DOE F 472.12 completion is maintained by SNL Personnel Security.

5.2. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

All subcontractor personnel must execute an SF 312, *Classified Information Nondisclosure Agreement*, at the time of or after completing SEC150, *Comprehensive Security Briefing*, and before receiving access to classified information, matter, or special nuclear material (SNM). Subcontractor personnel are required to execute an SF 312 prior to being granted a cleared DOE security badge and/or receiving authorization for an outgoing classified visit. Individuals who refuse to execute an agreement are reported to SNL's Personnel Security.

Subcontractor personnel may execute SF 312 with their FSO or Key Management Personnel (KMP), at a SNL Badge Office, or by coordinating with the SNL Security Awareness program (securityed@sandia.gov). Completed SF 312s must be submitted to the SNL Security Awareness program for review, acceptance, and retention via the above email address.

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 on the Security Toolcart site.

5.3.1. Other Reporting Requirements

The following conditions must be verbally reported by the FSO to the SNL/NM Clearance Office (505) 284-3103 or SNL/CA Personnel Security Office (925) 294-2061 within 3 working days of the event, followed by written confirmation to clearance-nm@sandia.gov or clearance-ca@sandia.gov within the next 10 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 Section 5.3, "DOE/SNL - Individual Reporting Requirements", 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 Counterintelligence interests.

6.0 SAFEGUARDS & SECURITY TRAINING PROGRAM

Contract Security Management (CSM) is responsible for relaying training requirements to designated Facility Security Officers (FSOs). PMC-110DE, *Facility Security Officer Overview,* is a self-study correspondence course found on the Security Toolcart site that provides an overview of the roles and responsibilities of the DOE or DOE-contractor FSO. The course emphasizes facility clearance (FCL) requirements, Personnel Security, Information Security, incident reporting, and other related programs. The course references the *National Industrial Security Program Operating Manual* (NISPOM) 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. PMC-110DE must be completed by the FSO prior to the processing of a FCL. DOE FSOs of DOD-cleared companies are not required to complete PMC-110DE . FSO training provided by the Defense Counterintelligence and Security Agency (DCSA) is sufficient for DOE's purposes.

SNL managers and SDRs 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 the Training and Employee Development System (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 on the subjects listed below, among others.

- Cyber Security Awareness Training (COM100)
- Annual Counterintelligence Training (CI100)
- Sensitive Information & International Trade Compliance (SNL330)
- Overview of Controlled Unclassified Information (CUI-100DE)

7.0 INFORMATION SECURITY

Classified matter is processed and handled in approved locations within SNL Limited Areas (LAs) and Temporary Limited Areas (TLAs). Classified matter is stored within US General Services Administration-approved containers, vaults, and Vault-Type Rooms (VTRs). 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 Contract Security Classification Specification (CSCS). Access controls are also applied at SNL to limit access to subcontractor personnel with the appropriate security clearance and need-to-know (NTK).

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 (CO). CLA102, *Classified Programs Initial Awareness Briefing (SRN),* 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 Information Review (IR) 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, category, and caveat (when applicable) 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 IR 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 unclassified information, protect patentable inventions, and communicate a professional image.

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

- Classified information found in a public domain or forum (e.g., websites, blogs, wikis, news articles, magazines, videos, 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 sensitive unclassified information may be prevented, and authorized releases of information deemed to be Unclassified Unlimited Release (UUR) may be allowed.

At SNL, DCs are knowledgeable and experienced Members of the Workforce who have been authorized by the SNL CO to derivatively classify SNL-generated matter, which includes both information, documents, and material. 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 regularly 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 (CTRs) are available in both Classification Offices (SNL/NM and SNL/CA) to assist all personnel and DCs in identifying information in classified subject matter areas that must be protected in the interest of national security.

Subcontractor personnel who work onsite with classified matter (whether electronic or material) may use the online application Jupiter to either locate a DC who supports their organization or program, or to apply to become an email-only derivative classifier (EDC). Subcontractor personnel who need access to a classified network to send classified emails must become EDCs by using Jupiter to request authorization. EDCs are authorized by the CO to perform classification of their own emails, but no other documents. Jupiter provides controlled access to classification guides to be used in the classification of information.

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. Additionally, if they believe that a DC or CO determination is incorrect, they are allowed and encouraged to challenge the classification decision by directly contacting DOE's Classification Office. The SNL Classification Office will assist the subcontractor if a challenge process is requested.

7.3. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

The purpose of the SNL CMPC program is to ensure appropriate marking and protection of classified matter that is generated, received, transmitted, used, stored, reproduced, or to be dispositioned/destroyed.

The CMPC program implements and communicates to subcontractor personnel requirements for the management and control of classified matter entrusted to SNL. SNL SS003, *Classified Matter Protection and Control (CMPC) Policy*, 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.

Subcontractors with DOE Q personnel security clearance badges sponsored by SNL must complete SEC301, *Classified Matter Training*. SNL managers and/or Sandia-Delegated Representatives (SDRs) will determine which L-cleared subcontractors work with, or have the potential to work with, classified matter and, therefore, must take SEC301. Subcontractors with the potential to create classified matter 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 at another location outside of SNL without specific authorization from SNL or the US government. All work related to a classified subject area must be performed in an approved location within an SNL LA.

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 three 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 IR 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 Controlled Unclassified Information (CUI) do not apply (typically work in draft and developmental stages).
3. **Sensitive Unclassified Information** — Federal agencies require that controls be placed on the availability of certain information, even if that information is not classified. Sensitive unclassified information has national security, governmental, proprietary, or personal privacy restrictions. Stewards of sensitive information must ensure that persons granted access have proper authorization (i.e., clearance) and NTK. Sensitive unclassified information includes government-owned information, such as CUI or Uncontrolled Unclassified Information (UUI). It also includes certain information owned by SNL (i.e., information related to financial, employment, procurement, legal, and technology transfer matters) that is identified as Sandia Proprietary Information (SPI).

For guidance on how to protect sensitive unclassified information, refer to SNL IT012, *Sensitive Unclassified Information Policy.*

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 Subcontractor Company

For the full definition of PII and additional instructions, refer to the "Protection of Personally Identifiable Information Clause" found in the NTESS Subcontract Information General Provisions (Section II, Terms and Conditions).

PII - At SNL

For instructions on how to identify, mark, retain, disseminate, protect and dispose of PII, refer to SNL IT023, *Personally Identifiable Information (PII) Policy*.

7.4.2. Controlled Unclassified Information (CUI)

CUI is government-owned, unclassified information that requires protections determined by a specific set of laws, regulations, or government-wide policies (LRGWP), also known as authorities. For information to be CUI, it must fall under a listed category on the CUI Registry and have an applicable LRGWP that requires or permits safeguarding. CUI may be exempt from public release under the Freedom of Information Act (FOIA). CUI has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not have a NTK of the information to perform their jobs or other DOE authorized activities. CUI information is a subset of sensitive unclassified information[2].

CUI-100DE, *Overview of Controlled Unclassified Information,* outlines the process for identifying, accessing, using, marking, distributing, transmitting, reproducing, storing, and disposing of CUI information.

CUI Information – At SNL

For instructions on how to identify, mark, protect, disseminate, and dispose of CUI, refer to SNL IT026, *Controlled Unclassified Information (CUI) Policy.*

Protect CUI Information – At Subcontractor 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).

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

[2] Other sensitive unclassified information that may require additional markings include: Attorney-Client/Work Product Privileged Information, Protected Cooperative Research & Development Agreement (CRADA) Information, SPI, Patent Caution, Privacy Act Information, PII, Unclassified Controlled Nuclear Information, Safeguards Information, and Export Controlled Information.

regional threats, protection planning strategies, and implementing protection measures. Contact with SNL Physical Security may be initiated through email via physicalsecurity@sandia.gov.

8.1. SECURITY AREAS

The SNL-controlled premises continuum begins with General Access Areas (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 are 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 special nuclear material (SNM), classified matter, and/or US 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 and used for the protection of classified matter and/or Category III quantities of SNM, where protective personnel or other internal controls can prevent access by unauthorized people to said 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 (VTRs)/Sensitive Compartmented Information Facilities (SCIFs)/Special Access Programs (SAPs).

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.
- Not introduce prohibited articles (see Section 8.5, "Prohibited Articles") into SNL-controlled premises.

- Not introduce controlled articles (see Section 8.4, "Controlled Articles") into LAs or secure storage areas without prior authorization.
- Cooperate with SNL security police personnel during badge checks and searches of vehicles, persons, and/or handcarried 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.

See *Who and What Can Go Where?* for additional guidance regarding access-controls associated with Sandia-controlled premises.

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 Personal Identity Verification (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 Security Incident Management Program (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 SS008, *Control Access to Information and Facilities Policy,* which require:

- 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 items, such as portable electronic devices (PEDs), both government- and personally-owned, that are capable of recording information or transmitting data (e.g., audio,

video, radio frequency, infrared, and/or data link electronic equipment). Examples include, but are not limited to:

- Global positioning system (GPS) units
- Cellular phones
- iPhones
- Cameras
- Fitness activity trackers
- iPads
- Digital picture frames
- MP3 players

Subcontractor personnel must comply with SNL Physical Security requirements for performing classified work.

8.4.1. Personally-Owned PEDs

PEDs are small, easily transportable, electronic items that are equipped with the capability to process, 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.

8.4.1.1. Mobile Devices

A mobile device is any portable computing device that:

- Has a small form factor, making it easily carried by a single individual.
- Is designed to operate without a physical connection (e.g., wirelessly transmit or receive information).
- Possesses local, non-removable data storage.
- Is powered on for extended periods of time with a self-contained power source.
- Possesses on-board sensors that allow the device to capture audio or video information.
- Does not utilize a desktop operating system that is safeguarded by an NNSA Cyber Security program, according to NNSA SD 205.1, *Baseline Cyber Security Program*.

Contact Physical Security (physicalsecurity@sandia.gov) for questions concerning mobile devices.

8.4.2. Secure Spaces

SNL Secure Space is (1) any location in which classified processing takes place, or (2) any classified conference room. All Secure Space is well-marked with signs.

Both SNL- and personally-owned mobile devices are prohibited in designated Secure Spaces and must be stored in approved storage locations. Any mobile device brought into Secure Space must be self-reported through the SIMP self-reporting tool at SIMP.sandia.gov.

8.4.3. SNL-Owned Computer Media

Use of US government- or SNL-owned computer media (such as thumb drives, CDs, or removable hard drives) with SNL computing resources that are identified as government or SNL

property only occurs when the computer media is obtained through proper procurement channels with the government or SNL. 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 Lab policies, including SS007, *Prohibited and Controlled Articles Policy*.
- Prior to procurement, storage, or use within security areas of a prohibited article not governed by SNL Safeguards & Security (S&S)-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.
- Chemical sprays of any size
- Controlled substances (e.g., illegal drugs and associated paraphernalia).
- Alcohol.
- Hazardous radiological, chemical, or biological materials.
- Any other items prohibited by law.

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 subcontractor company will follow internal procedures for physical security currently established in Intelligence Community Directives (ICDs) and Office of the Director of National Intelligence (ODNI) policy documents for the protection of classified in support of the SNL subcontract, which includes Other Government Agency (OGA) information and property utilized in performance of the subcontract.

9.1.2. Prohibited & Controlled Articles/Electronic Devices

Subcontractor personnel are responsible for reviewing the Field Intelligence Element (FIE) prohibited and controlled articles briefing for additional information on what cannot enter a Sensitive Compartmented Information Facility (SCIF) without prior authorization. Prior to bringing electronic and nonelectronic devices and/or equipment into a SCIF, subcontractor personnel must request and receive approval through the FIE Move in Log Logistics System

(MILLS). Contact an special security officer (SSO)/alternate special security officer (ASSO) for additional guidance regarding prohibited and controlled articles, and electronic devices in SCIFs.

9.2. INFORMATION SECURITY—CLASSIFICATION GUIDANCE

Subcontractor personnel will ensure that the derivative classifiers (DCs) who provide 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 an SNL subcontract will also have documented SCI access. Access to classified information must not be permitted until the proper DOE personnel security clearance (A.K.A. access authorization) has 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 matter. If an individual performing on the subcontract has any clearance or access suspended or terminated due to derogatory information, the Facility Security Officer (FSO) must report this information to the SNL SSO.

The FSO is responsible for notifying the SNL SSO as soon as it is known that an SCI is no longer needed. An SSO/ASSO will contact the individual to schedule an SCI 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, 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 an SNL SCIF. The Sandia-Delegated Representative (SDR) and FSO are responsible for ensuring that all badges are returned to the SNL SSO 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, thus, 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 special nuclear material (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. Notifications of these actions should be sent to the SNL SSO 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 an SNL classified subcontract involving intelligence work must receive required security briefings identified by applicable ICDs. An SCI indoctrination, *Annual Security Refresher Briefing* (SEC100), and SCI debriefing are required. Additional security briefings/trainings will be assigned to subcontractor personnel as required.

9.4.1. Reporting Requirements

All applicants and holders of an SCI authorization are required to report any information that they believe raises a potential security concern about themselves or another clearance applicant/holder, as outlined in ICDs. Personnel who hold SCI access are subject to other reporting requirements in accordance with applicable ICDs and will report to the agency that granted SCI access and to the SNL SSO through the FIE reporting system. As outlined in ICDs, 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.

9.5. CYBER SECURITY

All cyber systems located onsite at SNL that are used to access, 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 ICD requirements for applicable cyber systems.

10.0 SOURCE REQUIREMENTS DOCUMENTS

In addition to the list of applicable DOE directives (or successor documents that may supersede these requirements) referenced on the Security Toolcart "Flowdown of Requirements" site, contractors must comply with referenced or supplementary directives invoked by a Contractor Requirements Document. DOE establishes requirements for contractors (e.g., SNL) in the form of Contractor Requirements Documents. The contractor 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.

- 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*
- 5 USC 552a, *Privacy Act of 1974*
- 49 CFR 40, *Procedures for Transportation Workplace Drug and Alcohol Testing Programs*
- 49 CFR 382, *Controlled Substances and Alcohol Use and Testing*
- 10 CFR 710, *Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material or Eligibility to Hold a Sensitive Position*
- DOE O 232.2A, *Occurrence Reporting and Processing of Operations Information*
- NNSA SD 205.1, *Baseline Cyber Security Program*
- DOE O 142.3B, *Unclassified Foreign National Access Program*
- DOE O 470.1A, *Safeguards and Security Program Management Operations*

11.0 RELATED RESOURCES

Security Connection is a resource that includes a team of individuals who can answer security-related questions and a knowledgebase of hundreds of articles that focus on specific issues/topics. Security Connection hours of operation are 8:00 AM - 4:00 PM (Mountain Time) Monday through Friday. If no Security Connection representatives (SCRs) are immediately available to answer a call, callers can leave a message and an SCR will respond within 24 hours or the next business day. Contact Security Connection at 321 from an SNL landline, 505-845-1321 from any phone, or via email at security@sandia.gov.

12.0 WORK CONTROLS SUMMARY

Work Control	Applies To	Required	Recommended
Training	FSOs, Subcontracting personnel	SEC050, *Initial Security Briefing* SEC100, *Annual Security Refresher Briefing* SEC150, *Comprehensive Security Briefing* SEC225, *Security Termination Briefing* EC100, *Export Control & Foreign Corrupt Practices Act Basics*	N/A

Work Control	Applies To	Required	Recommended
		SNL110, *Drug-Free Workplace* PMC-110DE, *Facility Security Officer Overview* COM100, *Cyber Security Awareness Training* CI100, *Annual Counterintelligence Training* SNL330, *Sensitive Information & International Trade Compliance* CUI-100DE, *Overview of Controlled Unclassified Information* CLA102, *Classified Programs Initial Awareness Briefing (SRN)* SEC301, *Classified Matter Training* SEC303, *Classified Marking Training*	
Related Documents	FSOs, Subcontracting personnel	SS003, *Classified Matter Protection and Control (CMPC) Policy* SS007, *Prohibited and Controlled Articles Policy* *SS008, Control Access to Information and Facilities Policy* IT012, *Sensitive Unclassified Information Policy* IT023, *Personally Identifiable Information (PII) Policy* IT026, *Controlled Unclassified Information (CUI) Policy* EHW002.2, *Medical Restrictions Process*	N/A
Forms	FSOs, Subcontracting personnel	SF 328, *Certificate Pertaining to Foreign Interest* SF 27030-LSB, *Reporting Lost, Stolen, Forgotten, and Unrecovered Badges* SF-86, *Questionnaire for National Security Positions (QNSP)* SF 312, *Classified Information Nondisclosure Agreement* DOE F 470.2, *Facility Data and Approval Record (FDAR)* DOE F 470.1, *Contract Security Classification Specification (CSCS)* DOE F 472.11, *Security Acknowledgement* DOE F 472.12, *Security Termination Statement* Form I-9, *Employment Eligibility Verification*	N/A
Signs	N/A	N/A	N/A

Work Control	Applies To	Required	Recommended
Other	FSOs, Subcontracting personnel	N/A	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 GEN-16, *No Comment Policy on Classified Information in the Open Literature,* Classification Bulletin

13.0 RECORDS

All records will be maintained according to the *Sandia Records Retention and Disposition Schedule*.

ATTACHMENT A—ACRONYMS

Acronym	Term
ADA	American with Disabilities Act
ASSO	Alternate Special Security Officer
BAC	Blood Alcohol Content
BRO	Background Review Office
C	Confidential
CA	California
CAH	Crane and Hoist
CBD	Cannabidiol
CDL	Commercial Driver's License
CFR	Code of Federal Regulations
CMPC	Classified Matter Protection and Control
CO	Classification Officer
CRADA	Cooperative Research and Development Agreement
CSA	Cognizant Security Agency
CSCS	Contract Security Classification Specification
CSM	Contract Security Management
CSMO	Company Senior Management Official
CSO	Cognizant Security Office
CTR	Classification Technical Reviewer
CUI	Controlled Unclassified Information
DC	Derivative Classifier
DCSA	Defense Counterintelligence and Security Agency
DEAR	Department of Energy Acquisition Regulation
DOD	Department of Defense
DOE	Department of Energy
DRO	Designated Responsible Office
EDC	Email-Only Derivative Classifier
EP	Enterprise Person
ES&H	Environment, Safety, & Health
FCL	Facility Clearance
FDAR	Facility Data and Approval Record

Acronym	Term
FIE	Field Intelligence Element
FIO	Foreign Interactions Office
FN	Foreign National
FNR SP	Foreign National Request Security Plan
FOCI	Foreign Ownership, Control, or Influence
FOIA	Freedom of Information Act
FRD	Formerly Restricted Data
FSO	Facility Security Officer
GAA	General Access Area
HRP	Human Reliability Program
ICD	Intelligence Community Directive
IO	Inquiry Official
IOSC	Incident of Security Concern
IPOC	Innovation Parkway Office Center
IR	Information Release
ISSM	Information System Security Manager
KMP	Key Management Personnel
LA	Limited Area
LRGWP	Laws, Regulations, Government-wide Policies
LSSO	Local Site Specific Only
MILLS	Move In Log Logistics System
MRO	Medical Review Officer
NISPOM	National Industrial Security Program Operations Manual
NM	New Mexico
NNSA	National Nuclear Security Administration
NSI	National Security Information
NTESS	National Technology & Engineering Solutions of Sandia, LLC
NTK	Need-to-Know
OAA	Office Administrative Assistant
ODNI	Office of Director of National Intelligence
OGA	Other Government Agency
PED	Portable Electronic Device
PII	Personally Identifiable Information
PIN	Personal Identification Number

Acronym	Term
PIV	Personal Identity Verification
PLN	Plan
PPA	Property Protection Area
PSR	Periodic Security Review
QNSP	Questionnaire for National Security Positions
RD	Restricted Data
RFQ	Request for Quotation
S&S	Safeguards and Security
S	Secret
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCN	Sandia Classified Network
SCR	Security Connection Representative
SDR	Sandia Delegated Representative
SFO	Sandia Field Office
SIMP	Security Incident Management Program
SMB	Subject Matter-Related Briefing
SME	Subject Matter Expert
SNL	Sandia National Laboratories
SNM	Special Nuclear Material
SP	Subcontracting Professional
SPI	Sandia Proprietary Information
SRN	Sandia Restricted Network
SRP	Security Requirements Plan
SSIMS	Safeguards & Security Information Management System
SSO	Special Security Officer
SSSP	Safety and/or Security Sensitive Position
START	Sandia Total Access Request Tool
TDP	Testing-Designated Position
TEDS	Training and Employee Development System
TFNI	Transclassified Foreign Nuclear Information
THC	Tetrahydrocannabinol
TLA	Temporary Limited Area

Acronym	Term
TS	Top Secret
UCI	Unclassified Controlled Information
UPIV	Uncleared Personal Identity Verification
UUI	Uncontrolled Unclassified Information
UUR	Unclassified Unlimited Release
VTR	Vault-Type Room

ATTACHMENT B—BADGE/CREDENTIAL SHIPPING ADDRESSES

SNL/NM and Remote Sites	
Sandia Local Site-Specific Only (LSSO) Badges	**DOE Personal Identity Verification (PIV) (A.K.A. HSPD-12) Credentials**
Sandia Internal Mail (using Uncontrolled Classified Information [UCI] envelope) To: Personnel Security Badge Office Mail Stop: 1474	*Sandia Internal Mail (using UCI envelope)* To: Personnel Security Badge Office Mail Stop: 1474
Regular Mail Badge Office PO Box 5800 Mail Stop 1474 Albuquerque, NM 87185-(1474)	*Certified/Signature Required Mail* Sandia National Laboratories Badge Office IPOC Mail Stop 1474 1515 Eubank Blvd. SE Albuquerque, NM 87123
SNL/CA	
Sandia Internal Mail (using UCI envelope) To: Personnel Security/ Badge Office Mail Stop: 9113	*Sandia Internal Mail (using UCI envelope)* To: Personnel Security/ Badge Office Mail Stop: 9113
Regular Mail Carol D. James PO Box 969 Mail Stop 9113 Livermore, CA 94551-0969	*Certified/Signature Required Mail* Sandia National Laboratories Attn: Carol D. James 911, 102D Mail Stop 9113 7011 East Avenue Livermore, CA 94550

ATTACHMENT C—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 (CSA)	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 US industry. These agencies are: DOD, DOE, Central Intelligence Agency, and the Nuclear Regulatory Commission. The Secretary of Energy is the CSA for DOE. *Sandia National Laboratories identifies DOE as their CSA.*
Cognizant Security Office (CSO)	The office assigned responsibility for a given security program or function. Where DOE CSO 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 (e.g., corporation, partnership, university).
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 Just In Time (JIT) purchasing system are exempt from controlled article registration requirements.
Facility Clearance (FCL)	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 US 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.
Foreign National (FN)	Any person who is not a US citizen, which includes all lawful permanent residents. For the purposes of DOE O 142.3B, *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.

Term	Definition
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 (IOSC)	Events that are of concern to the DOE Safeguards and Security program that warrant preliminary inquiry and subsequent reporting.
Need to Know (NTK)	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. NTK 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 SNL. Includes leased or permitted commercial space (e.g., Research Park in Albuquerque, NM). It does not include sites where SNL 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 (SCI) may be stored, used, discussed, and/or electronically processed.
Special Access Program (SAP)	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, SNL, or its 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 SNL's processes to protect commercially valuable information.

CHANGE HISTORY

25 June 2025—Administrative Change

What Changed:

Added:

- 12.0 –Added DOE O 470.1A

Modified:

- 2.3.3.1 – Changed reference to DOE Order from 470.4B to 470.1A
- 7.4 – 8.5 – Modified links to all policy references since the link address recently changed

Deleted: N/A

Reason for Changes:

DOE O 470.1A is now the updated Order on SNL's contract for requirements.

---

29 April 2025—Comprehensive Review

What Changed:

Added:

- 9.0 Intelligence
- 4.2.1 CBD or Cannabidiols
- section in "Findings and Issue Resolution"
- 1.1, 2.3.2.3 Language to show that if changes occur with the subcontractor and CSM is not notified, they may be suspended, terminated or a Cure Notice will be issued
- 3.5 added language to clarify process.
- 7.2 was updated to provide information on Jupiter and Email-only Derivative Classifiers (EDCs) for subcontractors needing to send classified emails.
- 2.3.4 added minor clarifying sentence for respective FCLs.
- 2.3.2.1 added minor clarifying sentence for KMP clearances.
- 2.2.1 Added clarifying sentence regarding PSRs.
- 2.3.2.1 minor addition to section
- 2.3.2.6 minor addition to section
- 2.3.3. Minor addition to section2.3.2.1, Requirement for DCSA KMP to be processed for DOE Security Clearances added
- 3.1, Background Review and BRO
- 3.2.4, Requirement for Subcontractor personnel to report Lost, Stolen, Forgotten badges added
- 3.3.4, Note: Form I-9, Employment Eligibility Verification, does not verify citizenship.
- 3.3.8 , 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, and are not precluded from having personnel execute a DOE F 5631.29, Security Termination Statement and Security Termination Briefing, as necessary.

- 3.3.9 , There is an option to temporarily delay administrative termination of the clearance due to absence from work
- 3.3.9 , …for subcontractor personnel on an approved lease of absence (LOA) that by design or circumstances 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 manger must agree to initiate the waiver request.
- 5.1.1, The SEC050 Initial Security Briefing is provided at site Badge Offices or can be accessed by clicking on this link
- 5.1.2, SEC150 pdf
- 5.1.4, DOE F 5631.29, Security Termination Statement and Security Termination Briefing,
- 5.2, Use the FSO Witness Guide to ensure compliance with DOE and Sandia witnessing requirements
- 8.1, Medical devices that do not possess audio and/or video components (e.g., do not have microphones or cameras), but still have a wireless transmission capability (Bluetooth, cellular, etc.), may have other restrictions. Contact TEMPEST at telecomm@sandia.gov for guidance.
- 8.4, (Contractors must work with their SDR or SCR to gain authorization)
- 8.4.1, PEDS definition and explanation
- 8.4.1.1, Mobile device definition and description
- 8.4.1.1, Contact the Physical Security Department (physicalsecurity@sandia.gov) if you have a question concerning mobile devices.
- 8.4.2, Secure Spaces definition added
- Appendix, Badge/Credential Shipping Addresses
- 2.3.2.2, Additional language added to clarify lower tier subcontractor FCLs
- 2.3.4, "All lower-tier subcontractors must be processed for their personnel clearances under their respective company's FCL. Lower-tier subcontractors shall not be processed for a personnel clearance under the prime subcontractor's FCL. "

Modified:

- 2.3.2.1, 2.3.3.1, 2.3.3.3, 2.3.4 language for clarification
- 5.0 rewritten to align with the language used in Site Security Plans. Genericized descriptions to ensure information remains correct.
- Minor clarification made to target audience required to take CMPC related training.
- 3.5 Revised title to replace visits and assignments with "access" and
- 1.2 Modified to say Requirements Management rather than CSM.
- 2.3.2 Modified grammatical error.
- 2.3.3.3. Minor clarification
- 3.2.2 modified grammatical error.
- 6.0 minor clarification.
- Updated Escalation Table
- 3.0 multiple changes/updates for Personnel Security Section
- 4.0 minor changes to the Alcohol, Drugs and Tobacco at SNL section
- 5.0 comprehensive changes in Safeguards and Security Awareness Section

- 6.0 Course name changes/document title changes in Safeguards and Security Training Program section
- 7.0 CUI updates in Information Security section
- 8.0 minor edits to Physical Security section
- Table of contents, Updated to reflect added and deleted sections
- Throughout, References to DSS updated to Defense Counterintelligence Security Agency (DCSA)
- 3.3, Following statement moved to 2.3.2 "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."
- 5.3, Language modified to include counterintelligence reporting requirements.

Removed:

- No markings (UUR or otherwise) per Classification.
- Deleted information about pandemic-era specific processes for SF 312/SEC150 completions.
- 7.4.2 Removed OUO section
- 2.3.4 removed CSM helpline
- Material has been deleted throughout the entirety of the document over the span of nearly every section. This is due to the update being so overdue.
- 2.2.3, Reference to FIE and SCIF incident reporting removed
- 2.2.3, Reference to CI reporting removed
- 3.3.2 , DOE F 5631.18, Security Acknowledgment
- 3.3.2 , 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.
- 3.3.5, Requirement to test for illegal controlled substances for background review removed
- 3.3.8 , While only DOE/NNSA can render a formal personnel security clearance determination, SNL and/or the FSO are authorized to take action 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 631.19, Security Termination Statement and Security Termination Briefing, prior to the individual's departure.
- 5.3.2, Paragraph removed since clarifying language was modified in Paragraph 5.3
- 5.3.2, Counterintelligence Reporting Requirements removed
- 7.5, OPSEC section deleted
- 8.4.1, SNL-Owned Electronics being allowed in LA

- 8.4.1, Previous mobile device descriptions
- 8.4.2, Most building space within Sandia limited areas - except vestibules or entry areas approved for internal storage-has been identified as Secure Space.
- 8.6.1.1, Reference to PEDS100 requirements
- 9, Intelligence Work/FIE requirements removed

What Changed:

A periodic review was conducted; changes were made to reflect the current process and organizational change. Updated hyperlinks.

---

28 February 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.