STANFORD UNIVERSITY

SLAC National Accelerator Laboratory

Operated by Stanford University for the U.S. Department of Energy

DOE Order 470.7, Safeguards and Security Program (08/05/2026)

Site Compliance Plan (11/02/2026)

Contents

Contents 1
Introduction 1
Attachment 1 – Contractor Requirements Document 2
Attachment 2 – Safeguards and Security Program 3
Concurrence 25
Revision History 25

Introduction

This Site Compliance Plan (SCP):

a) corresponds with the version of the DOE Directive listed in the Prime Contract,
b) states how the Laboratory complies with applicable requirements as tailored to the risks at the Laboratory, and
c) documents DOE-approved methods of compliance for applicable requirements and that there are no recurring deliverables*.

Impact on the Contract:
Under the SCP, sections of the CRD are incorporated into the Contract as-is, unless the SCP indicates that a section or portion thereof is inapplicable, or the section has been changed. Thus, for example, if "in compliance" is listed next to a CRD section, that section is incorporated into the Contract as-is. However, where an SCP indicates that a section or portion thereof is inapplicable, the section or portion thereof is excluded from the Contract. In addition, where a section or portion thereof is applicable, but changes to the section have been agreed by the Parties, the section, as modified by the Parties, shall be incorporated into the Contract.

This SCP also clarifies SLAC's interpretation of the requirements, memorializes the Parties' agreement on how SLAC will comply with sections of the CRD (whether or not modified) and identifies the Laboratory programs and processes established to fulfill the respective requirements.

Attachment 1 – Contractor Requirements Document

The table below identifies the applicable CRD requirements, compliance status, and SLAC's method of compliance.

§	Requirements from Attachment 1 – CRD	Compliance Status	Method of Compliance
	This Contractor Requirements Document (CRD), which includes the requirement in Attachment 2, specifies key, measurable performance requirements for Safeguards and Security by Department of Energy (DOE) and National Nuclear Security Administration contractors. Contractors with the CRD incorporated into their contracts must demonstrate compliance by meeting defined performance outcomes. Contractor performance requirements will be defined in contractual language. Contractors are expected to regularly assess and report their performance against these requirements, ensuring all safeguards and security obligations are met consistently and measurably throughout the contract period. A violation of the provisions of this CRD relating to the safeguarding or security of restricted data, special nuclear material, or other classified information or matter, may result in a civil penalty pursuant to section 234B of the Atomic Energy Act of 1954, as amended (42 United States Code § 2282b). The procedures for the assessment of civil penalties are in Title 10 Code of Federal Regulations § 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations. Any site security plan approved by an Officially Designated Federal Security Authority has the force and effect of a DOE Order or Manual; therefore, it is enforceable under 10 CFR § 824.	In Compliance	SLAC acknowledges this section.

Attachment 2 – Safeguards and Security Program

This attachment provides requirements associated with Department of Energy (DOE) Order (O) 470.7 and requirements applicable to contracts in which the associated Contractor Requirements Document (CRD; Attachment 1 to DOE O 470.7) are inserted.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
1	SECURITY PLANNING. The contractor is required to establish and maintain a Safeguards and Security (S&S) program that prioritizes implementing risk-based planning activities, as approved by the Officially Designated Federal Security Authority (ODFSA). This approach includes developing ODFSA-approved site-specific security plans and analyses that address identified risks to DOE assets, personnel, and operations, and regularly assess and report performance.	In Compliance	SLAC has an established risk-based Safeguards and Security program compliant with all applicable requirements of this order. SLAC has a DOE approved Site Security Plan (SSP).
1.a	The purpose of this section is to establish the DOE's physical protection strategies for safeguarding Departmental assets.	In Compliance	SLAC acknowledges this section.
1.b	For the NNSA and its subordinate offices, the Design Basis Threat (DBT), as defined in DOE O 470.3, serves as the baseline planning document. The DBT provides a starting point for analyzing potential threats against DOE assets.	N/A	SLAC is not an NNSA or NNSA subordinate office
1.c	All other Departmental elements must tailor their physical protection strategies to site specific conditions. Using threat results approved by the ODFSA, these organizations must develop:	In Compliance by 2/28/2027	SLAC Security has a DOE approved SSP

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	(1) Adversary characteristics, including numbers, capabilities, equipment, and tactics. (2) Analytical methods for risk assessment and reporting. (3) Risk acceptance thresholds consistent with mission and protection needs. (4) Risk reporting expectations and processes. (5) Defined risk acceptance authorities.		
1.d	Security Asset Categorization. DOE possesses assets that must be protected by S&S systems against site-specific threats based on the consequences of loss or sabotage with effects outside the distance established by the ODFSA. These assets include: (1) Special nuclear material (SNM). (2) Chemical and radiological material, nuclear material, and select agents and toxins. (3) Classified matter.	In Compliance	SLAC has been approved to have limited amounts of Category IV SNM and has a DOE approved SNM plan. SLAC does not possess classified matter. Chemical and radiological material and SNM protection is covered in SSP.
1.e	Security Risk Acceptance. Contractors must use a vulnerability assessment or security risk assessment, as applicable, to analyze and communicate system effectiveness or overall security risk to DOE.	In Compliance	SLAC has utilized the assessment SRAM software (Security Risk Assessment Matrix) created for the DBT order and has completed security risk assessments (SRAs) for all areas designated as PL-6, including areas where SLAC has limited non-accountable SNM. SLAC SSP includes information and outcomes on the methodology used for conducted risk assessments. Assessment results are used to evaluate system effectiveness and overall security risk and are communicated to DOE for review and risk acceptance, as applicable. SLAC will work with DOE Site Office and conduct a vulnerability assessment to analyze and communicate system effectiveness.

DOE Order 470.7, Safeguards and Security Program (08/05/2026)

Site Compliance Plan (11/02/2026)

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
1.f	Graded Protection Concept. DOE must provide each site with the items listed in Section c (1-5) based on site-specific threat results. The graded protection approach categorizes DOE assets.	SLAC acknowledges this requirement for the DOE to provide this list	
1.g	Roll-up of SNM. Roll-up must be considered when a defined threat has the capability to accumulate lower categories of SNM into greater quantities, thereby raising the total quantity to a higher SNM category. Accumulation occurs when the defined roll-up threat could move material to a single location and complete adversarial tasks. Site-specific threat results, material characterization, and associated analysis provide the basis for determining the credibility of roll-up. The ODFSA will approve the SNM configuration that requires a roll-up analysis and the scenarios, level of rigor, and documentation required for that analysis, and initiates consultation with the Material Risk Review Committee (MRRC), if deemed necessary by the ODFSA, before making a decision.	In Compliance	SLAC maintains a DOE approved Nuclear Material and Accountability Program that details its SNM roll-up evaluation in section "3.4.5 Roll-up Evaluation". See Nuclear Material and Accountability plan table of revision dated 8/16/2026, this issue was addressed.
2.	INSIDER THREAT. Requirements applicable to the Insider Threat Program are contained in DOE O 470.5A, Insider Threat Program, current version.	SLAC acknowledges these requirements are found in this referenced order.	
3.	PERFORMANCE ASSURANCE. Contractor will implement a performance assurance program as outlined in contractual language.	In Compliance by Jan 30, 2027	SLAC is developing a Performance Assurance Program
4.	SAFEGUARDS AND SECURITY TRAINING	In Compliance by	SLAC maintains an internal Safeguards and Security training

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	PROGRAM. Contractor will establish an Officially Designated Security Authority (ODSA) approved training program that aligns with the knowledge, skills, and abilities based on appropriate job task analysis.	Jan.30, 2027	program designed and approved by the ODSA.
5.	SAFEGUARDS AND SECURITY AWARENESS. Contractor will implement an S&S awareness program that provides briefings and supplemental awareness activities to all individuals to communicate personal security responsibilities. The program will: a. Ensure initial, periodic, and termination briefings are conducted as required for cleared individuals covering relevant security topics. b. Ensure that all individuals granted security clearances execute an SF 312, Classified Information Nondisclosure Agreement, prior to accessing classified information.	In Compliance	SLAC has a Safeguards and Security awareness program detailed in its SSP
6.	PROGRAM MANAGEMENT. The contractor will implement programs covering facility clearance (FCL), foreign ownership, control, or influence (FOCI) reviews, Departmental and foreign classified visits, and reporting of incidents of security concern (IOSCs).	In Compliance	SLAC is in compliance with all the requirements in this section of the FOCI program. Details are in the PSP (Personal Security Program) policy.
7.	RECORDS. Security-related records must be retained in accordance with the National Archives and Records Administration General Records Schedule (GRS) 5.6, Security Records, and DOE Administrative Records Schedule 18, Security, Emergency Planning, and Safety Records.	In Compliance	SLAC maintains a records management program and schedule in which security and safety records are subject.

DOE Order 470.7, Safeguards and Security Program (08/05/2026)

Site Compliance Plan (11/02/2026)

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
8.	FACILITY CLEARANCES AND REGISTRATION AND FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE DETERMINATIONS. DOE contractors require an active FCL and favorable FOCI determination, and designation of a facility security officer when the contract or subcontract to be awarded is expected to require the officer to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter; SNM; other hazardous material presenting a potential radiological, chemical, or biological sabotage threat; and/or DOE property of significant monetary value, exclusive of facilities and land values. Contractor procedures applicable to the FOCI program must be documented in an ODFSA approved site security plan.	In Compliance	SLAC maintains a DOE facility clearance and designated Facility Security Officer. SLAC provides the information and organizational support necessary for DOE to conduct FOCI reviews and determine continued facility-clearance eligibility. DOE retains responsibility for the FOCI determination and approval of the facility clearance.
8.a	If an FCL or FOCI determination is required, Contractors will submit information to DOE in accordance with 32 CFR § 117, National Industrial Security Program Operating Manual, 48 CFR § 904.70, Facility Clearance, 48 CFR § 952, Solicitation Provisions and Contract Clauses, and 10 U.S.C. § 4874(a–b), Award of certain contracts to entities controlled by a foreign government: prohibition.	In Compliance	SLAC submits required facility-clearance and FOCI information to DOE through the applicable DOE review process and responds to requests for additional information. SLAC maintains supporting documentation and coordinates with Stanford University and the cognizant DOE security office in accordance with applicable federal and DOE requirements.
8.b	DOE granted FCLs based on a valid Department of Defense (DoD) FCL, Key management personnel (KMP) who do not need access to classified information are not required to obtain DOE access authorizations under 10 CFR § 710. Existing security clearances from another cognizant security agency fulfill KMP eligibility, with no	SLAC acknowledges this requirement.	

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	duplicative DOE processing needed unless access to DOE-classified information is required.		
9.	CONTROL OF CLASSIFIED VISITS. The contractor will establish and maintain a classified visit program, if required, in accordance with t in 32 CFR § 117.16, Visits and Meetings. Procedures applicable to classified visits must be documented in ODFSA approved site security plans.	N/A	SLAC does not host classified visits and SLAC is a non-possessing facility.
10.	INCIDENTS OF SECURITY CONCERN. a. Requirements. An IOSC is an action or inaction contrary to S&S requirements because it poses a threat to national security or DOE security assets, including property, personnel, information, capabilities, or systems. IOSCs are categorized by significance type: infraction or violation. A violation is an event in which loss or compromise occurred or is suspected. An infraction is a procedural noncompliance that did not result in loss or compromise but could do so if left uncorrected. The ODSA must establish and administer an IOSC program using a graded approach based on event significance. The ODSA also develops and approves the criteria and methodology for local implementation. This program, criteria, and methodology must be documented in the ODFSA approved site security plan. The ODFSA must be notified of all violations and infractions involving unclassified controlled nuclear information and unclassified naval nuclear propulsion information. b. Reporting. Initial and final reporting is imperative	In Compliance	SLAC does not possess classified material. SLAC has PSS approved established incident reporting protocols. All security/safety concerns are reported to senior management and the DOE Site Office. SLAC has a contract with LLNL to conduct investigations of incidents of security concern.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	because the ODFSA has specific responsibilities for notifying and coordinating with other agencies, governments, Departmental leadership, and Congress for selected IOSCs. Reports of loss, compromise, or suspected compromise of classified information, whether foreign or domestic, must be reported to the cognizant security agency through the ODFSA in accordance with 32 CFR § 117.8.		
11.	NUCLEAR WEAPONS DATA/CNWDI/SIGMAS. The contractor will authorize and control the receipt, handling, and storage of Nuclear Weapons Data, Critical Nuclear Weapon Design Information (CNWDI), and Sigmas in accordance with DOE O 452.8.	N/A	SLAC does not possess Nuclear Weapons Data, Critical Nuclear Weapon Design Information (CNWDI) and DOE O 452.8 is not in the SLAC contract
12.	UNCLASSIFIED FOREIGN NATIONAL ACCESS PROGRAM. Requirements applicable to unclassified foreign national access are contained in DOE O 142.3C.	SLAC acknowledges these requirements are found in this referenced order and is in compliance with DOE O 142.3C and has an approved site compliance plan.	
13.	PROTECTIVE FORCE OPERATIONS. The contractor will establish and maintain standardized requirements for managing, administering training programs, maintaining qualifications, and executing operations for various Protective Force (PF) activities. In addition, the contractor will implement a risk-based approach to establish posts and patrols, optimizing resource utilization. The contractor will:	In Compliance by Jan 30, 2027	SLAC will develop and implement requirements for protective force training as described in 10 CFR 1046 by 01/30/2027.
13.a	Implement the requirements within 10 CFR §851, Worker Safety and Health Program; Appendix A to §	In Compliance	SLAC is in compliance with the approved variance to 10 CFR 851. SLAC maintains an Injury Illness and prevention Program (IIPP)

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	851, “Worker Safety and Health Functional Areas”; 10 CFR § 1046, Medical, Physical Readiness, Training, and Access Authorization Standards for Protective Force Personnel; 10 CFR §1047, Limited Arrest Authority and Use of Force by Protective Force Officers; and 10 CFR §1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve, as applicable.		that exceeds federal requirements. SLAC relies on local law enforcement for armed response. 10 CFR 1047 and 1049 do not apply since SLAC does not have armed protective force, Officers are "observe and report" with the majority being certified emergency medical technicians (EMTs). SLAC Security/EMT officers respond to all security/safety and emergency incident on site.
13.b	Management and Planning. Contractors must establish and operate PF programs that align with DOE requirements. This includes clearly identifying the protection mission, documenting resource needs, tracking personnel and equipment, and developing funding requirements. (1) PF planning is based on threat guidance and adversary capabilities. (2) Site-specific rules of engagement must be developed, incorporating the concept of hostile intent, considering protected assets, and establishing clear conditions for the use of deadly force, requiring approval from the ODFSA and local Office of General Counsel. (3) Contractors must develop site-specific fresh pursuit procedures, approved by the ODFSA, that guide PF personnel in pursuing suspected criminals across jurisdictional lines, emphasizing safety and legal considerations. (4) Contractors must develop formal officer-involved shooting procedures that provide clear guidance for PF personnel covering required actions, evidence	N/A	Section 13.b 1-6a does not apply. SLAC Security officers observe and report only.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	preservation, reporting, and post-incident responsibilities. These procedures must be submitted to the ODFSA for approval. (5) Contractors must implement approved work stoppage contingency plans that are approved by the ODFSA. (6) Specialized functions (e.g., unmanned aerial systems or counter unmanned aerial systems operations) must conform to 10 U.S.C. § 6227, be based on identified risk, and be approved by the cognizant Program Secretarial Office. (a) Contractors must ensure personnel are trained and programs are approved by the ODFSA.		
13.a	Medical, Physical Readiness, and Training Requirements for PF Personnel. The contractor must establish and implement medical, physical readiness, and training requirements to ensure that PF personnel can respond within site-specific response times in accordance with applicable regulations including 10 CFR § 1046. These requirements should be based on a site-specific analysis approved by the ODSA and directed by the ODFSA. Security police officers and candidates must demonstrate general fitness measures related to their site and position, including muscular strength, muscular endurance, aerobic endurance, anaerobic endurance, agility, power, and mobility.	In Compliance by01/30/2027	SLAC security teams have completed 10 CFR 1046 Medical and Physical Readiness training. SLAC will develop and implement requirements for protective force training as described in 10 CFR 1046 by 01/30/2027.
13.b	Duties. The contractor must establish and implement PF duties in accordance with applicable regulations, site-specific operational needs, and threat determinations.	In Compliance	SLAC has a DOE-approved SSP. The SSP covers all PF duties that apply to SLAC. In addition, SLAC has internal policies/protocols/procedures that are updated every 12 months and

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
			cover all the duties/responsibilities for security officer's work. SLAC security is unarmed and provides "observe and report" functions. SLAC will develop and implement requirements for protective force duties as described in 10 CFR 1046 by 01/30/2027.
13.c	Weapons and Munitions. The contractor must establish and implement PF weapons and munitions requirements in accordance with applicable regulations. (1) Firearms Modifications. The ODSA must provide written approval for firearms modifications. (2) Firearms and Munitions Handling and Storage. The ODSA must approve the storage of firearms, ammunition, pyrotechnics, and explosives. (3) Firearms and Munitions Inventory. The ODSA will approve the conduct and documentation for inventory of: (a) Firearms. (b) Ammunition, pyrotechnics, and explosives. (c) Firearms Safety. The contractor must stablish and implement PF Firearms Safety requirements in accordance with applicable regulations.	N/A	SLAC does not maintain armed protective force
13.a	Facilities and Equipment. The contractor will establish and implement PF facilities and equipment requirements in accordance with applicable DOE regulations and site-specific threat analysis results.	In Compliance	SLAC has a approved site security plan (SSP) and approved site compliance plans (SCP) for all the applicable DOE orders in the contract. The Physical Security Program is aligned with SLACs overall mission. SLAC security officers are observe and report and information pertaining to facilities and equipment is maintained within the SLAC SSP.
13.b	Performance Testing. The contractor must test or assess	In Compliance by	SLAC will develop protective force training as described in 10 CFR

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	site-specific essential PF job functions as outlined in the ODFSA approved security plan.	01/30/2027	1046 by 01/30/2027 which will cover Performance Testing.
14	PHYSICAL PROTECTION PROGRAM. The contractor must set and maintain performance standards for all physical protection activities, based on DOE or Program Office guidance, local threat assessments, and supported by ODFSA approved security analysis. Measures should be risk-based, focusing resources on significant risks and tailoring systems to each asset's vulnerabilities to support the facility mission.	In Compliance	SLAC has a Physical Protection Program and complies with all applicable requirements of this order as detailed in this SCP and has an ODFSA approved security analysis.
14.a	Physical Protection Planning. The contractor must develop local physical protection strategies, incorporating security systems, documented in the ODFSA approved site security plan. All security strategies will be implemented in accordance with applicable federal regulations.	In Compliance	SLAC has developed local physical protection strategies, incorporating security systems and is captured the DOE-approved SSP.
14.b	The following plans, programs, and strategies must be developed locally, based on local analysis and under the direction of the ODSA. They must be documented in an ODFSA approved site security plan in accordance with 32 CFR 2001.41: (1) Security locks and key program. (2) Physical barriers for classified information, safeguards information, and SNM. (3) Secure storage protection program. (4) Vault construction and protection.	In Compliance	SLAC develops and maintains locally based security plans, procedures, and strategies addressing applicable physical-protection activities. These requirements are documented in the ODFSA-approved Security Plan and supporting procedures and are based on local security risk assessments and operational needs. (1) Security has a key and locks program. (2) SLAC is a non possessing site. However, SLAC has a cyber security program that safeguards information. SLAC has a physical protection program for the limited amount of approved SNM. (3) N/A. SLAC is a non possessing site and does not have a

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	(5) Entry and exit screening plan. (6) Physical protection strategies for classified information and controlled unclassified information. (7) Physical protection strategies for assets. (8) Emergency response plan for security areas. (9) Protection measures for the transportation of SNM. (10) SNM storage locations and PF post construction requirements. (11) Prohibited and controlled articles. (12) Posting requirements that comply with applicable federal regulations.		secure storage protection program. (4) N/A. SLAC does not have a vault (5) N/A. SLAC does not have classified information. (6) SLAC is a non possessing site. SLAC has an approved CUI program. (7) SLAC has physical protection strategies documented in its DOE approved SSP. (8) SLAC has an emergency response plan for security areas documented in its DOE approved SSP. (9) SLAC has an DOE approved SNM program. (10) SLAC has established security protocols for areas that SNM are stored. (11) SLAC follows Stanford policies prohibiting or strictly regulating specific items. (12) SLAC has posting requirements documented in its DOE approved SSP.
14.c	Physical Protection Systems (PPS). (1) The contractor must implement the design, protection measures, testing, and maintenance for PPS. This may include PPS networks, physical access control systems, intrusion detection systems, video assessment and surveillance systems, plans, procedures, equipment, and strategies as documented in the ODFSA approved site security plan. (2) Special Access Program Facilities and Sensitive Compartmented Information Facilities (SCIFs) must adhere to applicable federal policies.	In Compliance	(1) SLAC has created and implemented PPS procedure . (2) Not applicable. SLAC is a non-possessing laboratory

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
15.a	VETTING. Personnel Security: Requirements applicable to determining eligibility for access to classified information, including Restricted Data (RD) and SNM, are contained in Atomic Energy Act of 1954, as amended, EO 12968, EO 10865, EO 13467, 10 CFR Part 710, DOE O 472.2A, Personnel Security (current version), and various Office of the Director of National Intelligence directives.	SLAC acknowledges these requirements are found in these referenced requirements.	
15.b	Badging. (1) The contractor will develop a site-specific Badge Program, utilizing a risk-based approach to determine credentialing and access requirements and will be documented in an ODFSA approved site security plan. The Badge Program must align with the applicable Homeland Security Presidential Directive 12 (HSPD-12) requirements that are outlined in DOE O 206.2, "Identity, Credential, and Access Management," and DOE O 472.2A, "Personnel Security." (2) The program should assess the level of risk associated with various roles and access areas, ensuring that badging procedures and access permissions are tailored to mitigate identified risks and support operational security needs.	In Compliance	SLAC has an established site-specific badge program that takes a risk-based approach to access and roles. SLAC has a PIV policy and an FTE dedicated to processing applications that align to HSPD-12 and is documented in the DOE approved SSP.
15.c	Human Reliability Program (HRP). Requirements applicable to HRP are contained in 10 CFR § 712, Human Reliability Program. The contractor must ensure	The Human Reliability Program (HRP) is not applicable to SLAC. SLAC does not have Cat 1 or 2 materials	

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	that only the minimum number of individuals necessary for effective operations are enrolled in the HRP. The contractor shall periodically review the list of HRP position designations and enrolled individuals to ensure minimum number of participants for effective operations.		
16	INFORMATION SECURITY. The contractor is responsible for establishing programs to safeguard and manage classified information and matter in accordance with applicable laws, regulations, EOs, government-wide policy directives and guidelines, as well as DOE policies and directives, which will be documented in an ODFSA-approved site security plan.	SLAC does not manage classified information	
16.a	Classification Program. Requirements applicable to Classification Programs are contained in the Atomic Energy Act (RD, formerly restricted data [FRD], and transclassified foreign nuclear information [TFNI]), EO 13526 (National Security Information [NSI]), 10 CFR § 1045, 32 CFR § 2001, and DOE O 475.2B, Identifying Classified Information.	SLAC does not manage classified information	
16.b	Classified Matter Protection and Control. Requirements applicable to marking, handling, protecting, storing, dispositioning, and destroying classified matter are contained in 32 CFR § 2001, 32 CFR § 117, and 10 CFR § 1045. (1) The contractor will maintain a program that protects and controls classified matter based on federal requirements as implemented by ODFSA-approved security measures that result in protection, storage, or	SLAC does not manage classified information	

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	disposition effectiveness for classified matter. (2) Processes and procedures related to the protection and control of classified matter will be documented in an ODFSA-approved security plans and procedures, reference documents, and training material.		
16.c	Unclassified Controlled Nuclear Information. Requirements applicable to unclassified controlled nuclear information (UCNI) are contained in 10 CFR § 1017, Identification and Protection of Unclassified Controlled Nuclear Information. DOE federal and contractor employees must submit specific requests to deviate from the CFR to the Director, Office of Classification, for approval, in coordination with the Associate Administrator for Defense Nuclear Security for requests within NNSA.	N/A	SLAC does not manage UCNI.
16.c.(1)	The ODFSA-approved site security plan must establish the process for designating UCNI reviewing officials and prescribe procedures to be followed when UCNI guidance is unclear or when no applicable guidance exists.	N/A	SLAC does not manage UCNI.
16.c.(2)	Nomination. An employee nominated to be a Reviewing Official must be competent in the subject areas in which the authority will be used and familiar with DOE UCNI policy, procedures, and guidance.	N/A	SLAC does not manage UCNI.
16.c.(3)	Headquarters. The immediate supervisor of an employee being nominated for Reviewing Official Authority must	N/A	SLAC does not manage UCNI.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	submit the required information identified in paragraph 16.c.(5), below, through the Headquarters Classification Representative.		
16.c.(4)	Field. The immediate supervisor of an employee being nominated for Reviewing Official authority must submit the information identified in paragraph 16.c(5) below to the Classification Officer or, if there is no Classification Officer, to the Director, Office of Classification, for DOE elements or to the Associate Administrator for Defense Nuclear Security for NNSA elements.	N/A	SLAC does not manage UCNI.
16.c.(5)	Required Information. a. The employee's name, organization, mailing address, telephone number, and e-mail address. b. Subject areas in which the authority will be used. c. Desired jurisdiction. d. Any special limitations on the authority.	N/A	SLAC does not manage UCNI.
16.c.(6)	Training. The nominated employee must successfully complete the training for Reviewing Official Authority prior to appointment, which must include a practical examination using applicable UCNI guidance and applying UCNI markings. The required training and/or examination may be waived if the nominated employee has completed the training and/or examination within the last three years. However, the expiration date for the authority must be no longer than three years from the most recent successfully completed training.	N/A	SLAC does not manage UCNI.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
16.c.(7)	Appointment. The appointment must be in writing and must provide a description of the authority that includes the individual's name, organization, the effective date, the specific subject areas covered by the authority, the jurisdiction of the authority, the expiration date, and any special instructions or limitations on the authority. The appointing official must notify the employee and the employee's supervisor. At Headquarters, the appointing official must also notify the Headquarters Classification Representative.	N/A	SLAC does not manage UCNI.
16.c.(8)	Authority Limitations. An employee may exercise his or her Reviewing Official authority only in the specific subject areas and jurisdiction covered in his or her authority description and in keeping with any special limitations imposed. The employee may not redelegate the authority. If an employee changes positions, the employee may retain the Reviewing Official authority with written approval of their new supervisor. The supervisor must then notify the appointing official of this action.	N/A	SLAC does not manage UCNI.
16.c.(9)	Reappointment. If the authority is still needed after the initial three-year period, the employee must successfully complete an examination that retests his or her proficiency in using UCNI guidance and applying UCNI markings. If this examination is not successfully completed before the authority expires, the appointing official may grant a one-time three-month extension of the authority. If the examination is not successfully	N/A	SLAC does not manage UCNI.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	completed by the end of the three-month extension, the authority must be terminated.		
16.c.(10)	Cancellation of Authority. An employee's supervisor, the Classification Officer, or the appointing official may cancel this authority when an employee no longer requires such authority or if the employee does not exercise the authority reliability. Notification must be made to the employee and other parties identified above of the cancellation and effective date.	N/A	SLAC does not manage UCNI.
16.d	Controlled Unclassified Information. Requirements applicable to CUI are contained in 32 CFR § 2002, Controlled Unclassified Information (CUI).	In Compliance	SLAC has a DOE approved CUI program
16.e	Operations Security. Develop Operations Security plans at the direction of the ODSA and document them in local procedures to integrate with applicable programs to protect identified critical program information as set forth in the National Security Presidential Memorandum-28. Threat analysis will be documented in the ODFSA approved site security plan.	In Compliance	SLAC has standard security operations Procedures
17	TECHNICAL SECURITY. Requirements applicable to the Technical Security Program are contained in DOE O 470.6, Technical Security Program, current version.	N/A. This DOE order is not in the SLAC contract.	
18	NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY (MC&A). Contractors must establish an ODFSA approved graded MC&A program	In Compliance	SLAC maintains a Nuclear Material Control and Accountability Program that has been approved by the DOE that is compliant with this order.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	for controlling, accounting for, and safeguarding SNM and other accountable nuclear material.		
18.f	The Nuclear Materials Management and Safeguards System User Guide is used for nuclear materials management and Safeguards System reporting and data submission.	In Compliance	SLAC complies with this requirement as documented in its Nuclear Materials Control and Accountability Plan, Section 3.7 -Reporting requirements.
18.g	For DOE to Department of War (DoW) weapons transfers, SNM in weapons must not be transferred to DoW under 42 U.S.C. § 2121(b), "Material for Department of Defense Use," until DOE has received direction from the President.	N/A	SLAC does not receive/transfer weapons
18.h	Program Management. The contractor will develop a detailed ODFSA approved MC&A Plan that outlines specific roles, responsibilities, training, and procedures to promote clarity and accountability. The program should document control measures and program elements, be graded based on potential loss consequences, monitor effectiveness and respond to loss indicators, and integrate with S&S programs. This structured approach reduces confusion and ensures that all personnel are aware of their duties, leading to more efficient operations.	In Compliance	SLAC maintains Nuclear Material Control and Accountability Program that has been approved by the DOE.
18.i	Material Accounting. Each facility will have a system that tracks SNM inventories, documenting SNM transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and SNM gains or losses. Each facility must	N/A	SLAC does not possess SNM in accountable quantities.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	have an accountability system that provides continuity of knowledge for SNM from receipt or production to disposition and include access authorization to the accountability system. Each facility must be able to produce an inventory of all nuclear material in the accountability system upon request. The accountability system will be maintained and updated in a timely manner, as approved by the MC&A Plan. Material Balance Areas (MBAs) shall be used to identify the location and quantity of SNM and collocate credible substitution material in the facility. An MBA is an area that is both a subsidiary account of material within the accounting system at a facility and a specified geographical area that has defined boundaries.		
18.j	Material Control. Contractors must implement a material control program consistent with the graded safeguards concept to prevent unauthorized removal of SNM. (1) Ensure each facility implements a Material Control Program concept to ensure that SNM is not removed from an authorized location without approval or timely detection of an unauthorized removal. (a) This includes access controls, material surveillance, material containment, detection and assessment, portal monitoring, incident reporting and response.	N/A	SLAC does not possess SNM in accountable quantities.
18.k	Measurements. Ensure all facilities possessing SNM implement Measurements and Measurement Control programs. The Measurements program must provide	N/A	SLAC does not possess SNM in accountable quantities.

§	Requirements from Attachment 2	Compliance Status	Method of Compliance
	measured values with uncertainties sufficient to detect theft or diversion of SNM. The Measurement Control program must ensure the quality of measurements made for MC&A purposes. The Measurement program elements include measurement types, methods, control, bulk sampling. Measurements are required as directed in the MC&A Plan. Category IV sites where rollup to Category III has been deemed not-credible and items are not susceptible to theft or diversion, as determined by a vulnerability assessment, may be excluded from the requirements of section 1(g).		
18.1	Physical Inventory. A physical inventory program for SNM must be implemented to confirm materials are in their stated quantities and authorized locations, and to detect unauthorized removals or discrepancies. The Physical Inventory Program: (1) Will be conducted at a frequency approved by the ODFSA. (2) Outlines procedures for conducting, verifying, and reconciling inventories. (3) Ensures that discrepancies between the physical inventory and the accounting records system are detected and resolved. (4) Include periodic physical inventories, special inventories, and International Atomic Energy Agency inventories (if applicable). (5) The risk associated with substitution material should be considered in the facility Physical Inventory Plan.	N/A	SLAC does not possess SNM in accountable quantities.

DOE Order 470.7, Safeguards and Security Program (08/05/2026)

Site Compliance Plan (11/02/2026)

Concurrence

Name	Title	Signature
Simon Ovrahim	Security Manager - SLAC	Simon Ovrahim Simon Ovrahim (Nov 4, 2026 10:58:38 PST)
Ian Evans	Director, ES&H - SLAC	Ian Evans Ian Evans (Nov 4, 2026 11:05:08 PST)
Charina Rockwell	Director of Operations, DOE-SSO	CHARINA ROCKWELL Digitally signed by CHARINA ROCKWELL Date: 2026.11.10 07:59:49 -08'00'
William W. Wheeler	Acting Manager, DOE-SSO	THOMAS RIZZI Digitally signed by THOMAS RIZZI Date: 2026.11.10 09:22:18 -08'00'

Revision History

Revision	Revision Date	Summary of Change(s)
R0	10/19/2026	Original release.
R1	11/02/2026	Made minor adjustments to align the SCP with the published DOE Order due to discrepancies identified in the previously signed version.