



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

Contents

Introduction 1
 Attachment 1 – Contractor Requirements Document.....2
 Attachment 2 – Security Clearance Requests/Justifications and Access Authorizations37
 Attachment 3 – Limited Access for Non-U.S. Citizens42
 Attachment 4 – Temporary Eligibility.....48
 Attachment 5 – Reporting Requirements65
 Attachment 6 – Personnel Security Quality and Training82
 Attachment 7 – References.....88
 Attachment 8 – Definitions88
 Revision History.....92

Introduction

This Site Compliance Plan (SCP):

- a) corresponds with the version of the DOE Order Personnel Security listed in the Prime Contract,
- b) outlines the specific CRD sections that apply to SLAC and the respective method of compliance clarifies that the Lab “In compliance”. The applicable sections identified herein define SLAC’s Baseline Level of Protection (BLP) as it correlates with the CRD and the SLAC Site Security Plan (SSP), states how the Laboratory complies with applicable requirements as tailored to the risks at the Laboratory,
- c) correlates and compares SLAC’s Safeguards and Security Program and Site Security Plan with the CRD of this Order, and
- d) documents recurring deliverables* and DOE-approved methods of compliance for applicable requirements.

Impact on the Contract:

Under the SCP, sections of the Order 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 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. The SCP also memorializes the Parties’ agreement on how SLAC will comply with sections of the Order (whether or not modified).

**Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)*



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

Attachment 1 – Contractor Requirements Document

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1	GENERAL REQUIREMENTS FOR SECURITY CLEARANCES						
1.a	A security clearance request for Key Management Personnel (KMP) and other contractor employees where there is a pending Facility Clearance (FCL) request will be managed in accordance with DOE O 470.4B and the NISPOM.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC has identified Key Management Personnel. SLAC will comply per our Personnel Security Program	n/a	n/a	n/a	n/a
1.b	Security clearances must only be requested and maintained at the minimum number necessary to ensure operational efficiency.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware of and will comply with this directive by only requesting and maintaining security clearances at the minimum number necessary to ensure operational efficiency.	n/a	n/a	n/a	n/a
1.c	A security clearance request must be submitted to DOE only after the contractor determines that the security clearance is essential for the individual to perform tasks or services stipulated in the contract.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program SLAC will only submit a security clearance	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			request after SLAC has determined that the security clearance is essential for the individual to perform tasks or services stipulated in the contract				
1.d	<p>A security clearance must not be requested to:</p> <p>(1) Avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas, or to alleviate responsibilities for escorting persons without security clearances within a controlled area. In certain instances, contractor employees who do not otherwise require access to classified information or SNM may be organizationally and/or physically situated such that they may inadvertently be exposed to classified information or SNM in the course of their duties. Federal site managers may require such contract employees to have security clearances if, in their judgment, operational necessities or cost considerations require it and inadvertent access to classified information or SNM by these individuals cannot otherwise be reasonably prevented;</p> <p>(2) Alleviate individual or management responsibilities for properly protecting</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will per our Personnel Security Program.</p> <p>SLAC will not submit clearance requests for the following reasons:</p> <p>To Avoid the use of access controls or physical barriers to distinguish perimeters among security areas or between security and open areas, or to alleviate responsibilities for escorting.</p> <p>To Alleviate individual or management responsibilities for properly protecting classified information or SNM or controlling dissemination of classified information or SNM on a need-to-know-basis.</p> <p>To determine an individual’s fitness for employment with SLAC.</p> <p>To establish a pool of SLAC employees with pre-existing security clearances.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	classified information or SNM or controlling dissemination of classified information or SNM on a need-to-know basis; (3) Determine an individual’s fitness for employment with the contractor; (4) Establish a pool of contractor employees with pre-existing security clearances; (5) Accommodate an individual’s personal convenience, expedience, gain or advantage; or (6) Anticipate unspecified classified work.		To accommodate an individual’s personal convenience, expedience, or to gain advantage. To anticipate unspecified classified work				
1.e	A security clearance must be requested only when required so as to avoid the unnecessary expenditure of DOE resources and the unwarranted invasion of an individual’s privacy	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Clearances will only be requested when required.	n/a	n/a	n/a	n/a
1.f	Individual access to classified information or SNM must not be permitted until notification has been	In Compliance	Section is addressed in SLAC Plan for Personnel Security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	received from DOE that a security clearance has been granted. Verbal notification from the CPSO may be accepted, to be followed by written confirmation of the action.		SLAC will comply per our Personnel Security Program. Individuals will not be allowed access to classified information until notification has been received from DOE that a security clearance has been granted				
l.g	Security clearances must be requested only for individuals who are U.S. citizens and are at least 18 years of age.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Security clearances will not be requested for individuals are not U.S. citizens or are at least 18 years of age.	n/a	n/a	n/a	n/a
l.h	Only authorized DOE Federal employees can render a formal security clearance determination; however, contractors are authorized to take actions that affect an individual’s access, such as restricting access to classified information or SNM when a security clearance is terminated or administratively withdrawn, or obtaining a DOE F 5631.29, Security Termination Statement, prior to the individual’s departure.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will comply and is aware we are authorized in taking actions needed that affect an individual’s access, such as restricting access to classified information when a security clearance is terminated or administratively withdrawn, or obtaining a DOE F 5631.29, Security Termination Statement, prior to the individuals departure.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1.i	Contractor personnel must provide Logistical assistance (see paragraph 4.e.) to DOE and Federal investigative agencies for conducting initial investigations, periodic reinvestigations, and additional investigations when authorized by DOE.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will comply and supply logistical assistance to the DOE and Federal investigative agencies in the conducting of initial investigations, periodic reinvestigations, and additional investigations when authorized by DOE.	n/a	n/a	n/a	n/a
1.j	DOE retains authority in all matters related to DOE personnel security activities. Personnel security activities are not subject to collective bargaining between contractor management and labor.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that the DOE retains authority in all matters related to DOE personnel security activities. Also, SLAC is aware personnel security activities are not subject to collective bargaining between SLAC management and labor.	n/a	n/a	n/a	n/a
1.k	The Contractor must not use an individual’s security clearance status must not be used as a determining factor for hiring, entering into a consultant agreement, or awarding a	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	subcontract.		SLAC is aware that an individual’s security clearance status must not be used as a determining factor for hiring, entering into a consultant agreement, or awarding a subcontract.				
1.l	Contractor Management Officials or other employees must not use DOE personnel security requirements and procedures to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation, or DOE directive.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware and will not use DOE personnel security requirements and procedures to coerce, restrain, threaten, intimidate, or retaliate against individuals for exercising their rights under the Constitution or under any statute, regulation, or DOE directive.	n/a	n/a	n/a	n/a
1.m	Unless otherwise stipulated, the contractor will not be required to reimburse DOE for DOE costs associated with processing the contractor’s applicants or employees for investigative or other types of actions related to security clearances.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that unless otherwise stipulated, SLAC will not be required to reimburse DOE for DOE costs associated with processing SLAC’s applicants or employees for investigative or other types of	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			actions related to security clearances.				
2.	SECURITY CLEARANCE AND ACCESS AUTHORIZATION TYPES						
2.a	Security clearances and access authorizations denote an individual’s eligibility for access to a particular type of classified information or material, such as National Security Information (NSI), Restricted Data (RD), Special Nuclear Material (SNM) or Sensitive Compartmented Information (SCI). Unless otherwise specified, access authorizations and security clearances will be commonly referred to as security clearances throughout this CRD.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC has received an FCL for a Non-Possessing Facility. Cleared SLAC personnel will have access to Classified Restricted data but will not possess this type of data on-site. SLAC will not have access to National Security Information (NSI), Special Nuclear Material (SNM) or Sensitive Compartmented Information (SCI).	n/a	n/a	n/a	n/a
2.b	This section describes those security clearances and access authorizations for which DOE cognizant personnel security offices (CPSOs) are responsible. Other access authorizations issued by DOE appear in Attachment 2.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC has received an FCL for a Non-Possessing Facility.	n/a	n/a	n/a	n/a
2.c	Security Clearances (1) Top Secret: A Top-Secret security clearance is required for access to NSI, as defined by Executive Order 13526, classified at the Top-Secret level and	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	Formerly Restricted Data (FRD, as defined by the Atomic Energy Act of 1954, as amended [AEA]) at the Top Secret level. A Top-Secret security clearance also permits access to NSI and FRD classified at the Secret and Confidential levels. (2) Secret: A Secret security clearance is required for access to NSI and FRD classified at the Secret level. A Secret security clearance also permits access to NSI and FRD classified at the Confidential level. (3) Confidential: A Confidential security clearance is required for access to NSI and FRD classified at the Confidential level.		SLAC has received an FCL for a Non-Possessing Facility. There will be no classified information or material at SLAC, but people with security clearance will have access to them at other facilities.				
2.d	Access Authorizations (1)Q: A Q access authorization is required for access to: (a)RD, as defined by the AEA, classified at the Top Secret or Secret level; (b)SNM, as defined by the AEA, designated as Category I and other categories with credible roll-up to Category I. (c)A Q access authorization permits access to information and material described below for L access authorizations. (d) A Q access authorization allows	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC has received an FCL for a Non-Possessing Facility. There will be no classified information or material at SLAC, but people with security clearance will have access to them at other facilities.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	access to information listed under TS, S, and C security clearances above (2)L: An L access authorization is required for access to: (a) RD classified at the C level and/or SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in associated site security plans mandate otherwise; (b) An L also allows access to information listed under S and C security clearances above.						
3	PRE-EMPLOYMENT AND PRE-PROCESSING REQUIREMENTS						
3.a	The contractor must require applicants and employees selected for positions requiring security clearances to provide evidence of U.S. citizenship and must verify such evidence to DOE when requesting that the individuals be processed for security clearances. Acceptable evidence of U.S. citizenship consists of the following:	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will verify evidence of U.S. citizenship by utilizing the documents listed in this section.	n/a	n/a	n/a	n/a
3.b	For an individual born in the United States, a current or expired U.S. passport or a birth certificate are the primary and preferred means of citizenship verification. Acceptable birth certificates must show that the	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>record was filed shortly after birth and must be certified with the registrar’s signature. The birth certificate must bear the raised, impressed, or multi-colored seal of the registrar’s office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate (one created when a record was filed more than one year after the date of birth) is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include baptismal certificates, hospital birth records or affidavits of persons having personal knowledge about the facts of the birth. Other documentary evidence can be early census, school, or family records; newspaper files; or insurance papers. All documents submitted as evidence must be original or certified.</p>		<p>For Individuals Born in the United States SLAC will use U.S Passport or birth certificate for citizenship verification</p>				
3.c	<p>For an individual claiming citizenship by naturalization, a Certificate of Naturalization (Form N-550 or N-570) showing the individual’s name is required.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will use Form N-550 or N-750 to verify citizenship for an individual claiming</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			citizenship by Naturalization				
3.d	<p>For an individual claiming citizenship acquired by birth abroad to a U.S. citizen, one of the following (showing the individual’s name) is required:</p> <p>(1) Certificate of Citizenship (Form N-560 or N-561),</p> <p>(2) Consular Report of Birth Abroad of a Citizen of the U.S. of America (State Department Form FS 240),</p> <p>(3) N-600, Application for Certificate of Citizenship,</p> <p>(4) Certificate of Birth (Form FS 545 or DS 1350), or</p> <p>(5) A current or expired U.S. passport, or passport card</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>When verifying U.S Citizenship for an individual claiming citizenship acquired by birth abroad to a U.S citizen SLAC will utilize one of the following:</p> <p>Certificate of Citizenship (Form N-560 Or Form N-561</p> <p>Consular Report of Birth Abroad of a Citizen of the U.S. of America (State Department Form FS 240)</p> <p>N-600, Application for Certificate of Citizenship</p> <p>Certificate of Birth (Form FS 545 or DS 1350</p> <p>A current or expired U.S. passport, or passport card</p>	n/a	n/a	n/a	n/a
3.e	The contractor must not concurrently submit an applicant or employee for a	In Compliance	Section is addressed in SLAC Plan for Personnel Security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	DOE security clearance and a security clearance with another Federal agency. If a security clearance is required to perform work on classified contracts at DOE and one or more other agencies, the contractor will submit the request for the highest security clearance necessary and rely upon reciprocity for lower clearances.		SLAC will comply per our Personnel Security Program. SLAC will not concurrently submit an applicant or employee for a DOE security Clearance with another Federal Agency. Reciprocity will be used for lower clearances.				
3.f	The contractor must furnish information pursuant to 48 CFR 952.204- 2(h)(2)(vi) [the DEAR Clause], if required by the CPSO.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will furnish information pursuant to 48 CFR 952.204- 2(h)(2)(vi) [the DEAR Clause], if required by the CPSO.	n/a	n/a	n/a	n/a
4	PROCESSING DOE SECURITY CLEARANCE REQUESTS						
4.a	Security clearance requests must be forwarded through established channels to the CPSO. Requests must include the following (additional documentation may be required by the CPSO): (1)A cover letter or form that requests the security clearance and provides the justification for processing. The justification must describe in detail	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Justification cover letters and security clearances will follow and contain information provided in this section.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

<p>(without revealing classified information) the duties of the position and the levels and types of classified information or SNM to be accessed. The contractor must also indicate whether the individual holds or has held a security clearance issued by DOE or any other Federal agency. General statements such as “A security clearance is required to perform contractual duties” are unacceptable, as are statements that corporate policy requires all applicants or employees to be processed for security clearances. The following represents an acceptable justification: “Mr./Ms. _____ is a computer systems engineer with ABC, Inc. involved in systems analysis in support of XE-50. The duties of the position will require access to plans and operations concerning the Tritium Recovery Facility for the MHGTR, which are classified as Secret.”</p> <p>(2) Verification of the individual’s evidence of U.S. citizenship, as detailed in paragraph 3.b. above.</p> <p>(3) The DOE contract or subcontract number under which the security clearance is being requested.</p> <p>(4) Information regarding contractor reviews, pursuant to 48 C.F.R. 952.2042(h)(2)(vi) [the DEAR Clause], if required by the CPSO, and</p> <p>(5) Additional documentation set forth in Attachment 2.</p>						
---	--	--	--	--	--	--

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
4.b	<p>The contractor must also:</p> <p>(1) Designate certain employees to review completed security forms and all related material for adequacy and completeness before they are submitted to DOE.</p> <p>(2) Advise employees and applicants for employment in writing that their forms will be reviewed only by those designated employees and that such information will not be used for any other purpose within the company.</p> <p>(3) Elect whether to maintain copies of the individual's security forms in paper or electronic format. If the contractor elects to maintain copies of the individual's security forms, the individual must be informed of the contractor's policy concerning copies of the security forms, the contractor's procedures for protecting the information from unauthorized disclosure, and the procedures by which the individual may obtain access to, or copies of, the security forms maintained by the contractor. The contractor should recommend to the individual that they maintain copies of their completed security forms for</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC has designated certain employees to review completed security forms and all related material for adequacy completeness before they are submitted to DOE.</p> <p>SLAC will advise its employees and applicants for employment in writing that their forms will be reviewed only by those designated employees and that such information will not be used for any other purpose withing the company.</p> <p>SLAC will elect whether to maintain copies of individual's security forms in paper or electronic format. If SLAC elects to maintain copies of the individual's security forms, the individual will be informed of SLAC's policy concerning copies of the security forms, SLAC's procedures for protecting the information from unauthorized disclosure, and the procedures by which the individual may obtain access to, or copies of, the security forms maintained by SLAC. SLAC will recommend to the individual that they maintain copies of their completed security forms for personal records.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	personal records.						
4.c	<p>Contractors must establish written procedures for the protection of security clearance request information, including procedures for the following.</p> <p>(1) Designating responsible employees who are trained in the procedures for reviewing completed security forms before their submission to DOE.</p> <p>(2) Informing all employees with access to completed security forms, pre-employment or pre-processing check information and other security clearance-related information of their responsibility to protect the information from unauthorized disclosure.</p> <p>(3) Ensuring individuals have the opportunity to complete and submit all forms or other data collections required during the security clearance process in private. Assistance in completion of any forms will be provided by a contractor employee who has been specifically designated by the contractor to review such forms.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC Has established written procedures for the protection of security clearance request information, including procedures for the following.</p> <p>(1) Designating responsible employees who are trained in the procedures for reviewing completed security forms before their submission to DOE.</p> <p>(2) Informing all employees with access to completed security forms, pre-employment or pre-processing check information and other security clearance-related information of their responsibility to protect the information from unauthorized disclosure.</p> <p>(3) Ensuring individuals have the opportunity to complete and submit all forms or other data collections required during the security clearance process in private. Assistance in completion of any forms will be provided by a SLAC employee who has</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			been specifically designated by SLAC to review such forms.				
4.d	Deficient security clearance requests will be returned to the contractor by the CPSO with a clear indication of the nature of the deficiency(ies). The contractor must ensure that the request is corrected and returned to the CPSO in a timely manner.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Programs. When requests are returned by the CPSO for a deficiency(ies), SLAC will ensure that the request is corrected and returned in a timely manner.	n/a	n/a	n/a	n/a
4.e	The contractor must assist in the timely processing of security clearance actions by: (1)Ensuring the availability of the contractor applicants and employees for the conduct of personal interviews by the investigative agency or DOE personnel security staff, and (2)Ensuring that other employees are made available, as needed, to provide background information during the conduct of all personnel security background investigations.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure the availability of contractor applicants and employees for personal interviews by the investigative agency or DOE personnel security staff, and SLAC will ensure that other employees are made available, as needed, to provide background information during the conduct of all personnel security background investigations.	n/a	n/a	n/a	n/a
4.f	The contractor is responsible for reviewing, approving and submitting security clearance requests for its subcontractor, consultant, or agent	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	applicants or employees. Such requests must be kept to a minimum in accordance with DOE requirements		Security Program SLAC is aware of it’s responsibility to review, approve and submit security clearance requests for its subcontractor, consultant, or agent applicants or employees. Such requests must be kept to a minimum in accordance with DOE requirements				
5	Temporary Eligibility						
5.a	When urgent operational or contractual exigencies or exceptional circumstances exist, CPSOs may grant temporary security clearance eligibility in accordance with Attachment 4.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that when urgent operational or contractual exigencies or exceptional circumstances exist, CPSOs may grant temporary security clearance eligibility in accordance with Attachment 4	n/a	n/a	n/a	n/a
5.b	Temporary Access to Classified Information (Interim Security Clearances). Only under exceptional circumstances when such action is clearly consistent with Departmental and national interests will a contractor applicant or employee, pending completion of the appropriate investigation, be permitted to have temporary access to classified information. Interims are temporary measures pending completion of an	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will comply with information stated in the section when considering Interim Security Clearances.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	expedited investigation, which must be in process. Non-U.S. citizens are not eligible for interim access to classified information or SNM. Contractors may submit a request that a particular applicant or employee be considered for interim access when providing justification for the security clearance request [see paragraph 4.a.(1) above] but determinations regarding whether any individual is afforded such access is solely the purview of Federal CPSO staff. See Attachment 4 for additional information regarding interims.						
5.c	<p>Temporary Access to a Higher Level of Classified (Temporary Security Clearance Upgrades)</p> <p>(1) Circumstances may arise where an urgent operational or contractual exigency exists requiring a cleared DOE contractor employee to have one-time or short duration access to classified information or SNM at a higher level than is authorized by their existing security clearance. In some instances, the processing time required to upgrade the security clearance would prevent timely access to the classified information or SNM, adversely impacting mission needs.</p> <p>(2) In such situations, and only for</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will comply with information stated in the section when considering Temporary Security Clearance upgrades.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	compelling reasons in furtherance of the DOE mission, the contractor must certify the need in writing and submit it to the appropriate Federal Site Manager. If the Site Manager is satisfied that exigent circumstances exist, the Site Manager must certify the need for the security clearance in writing and submit it to the appropriate CPSO. The CPSO may consider the request and grant or deny the security clearance in accordance with procedures set forth in Attachment 3.						
5.d	<p>One-Time Access to Classified Information.</p> <p>(1) During exceptional circumstances, DOE contractor employees may be approved for one-time access to classified information when it is determined to be in the national security interest. One-time access will be limited to DOE contractor employees whose expertise offers specialized and important benefit and value to the United States Government (USG), or to individuals to whom access to classified information needs to be provided in the interest of national security.</p> <p>(2) One-time access must be limited to</p>	Non-Applicable	As a Non-Possessing Facility SLAC does not foresee the need for applying or a One-Time access to Classified Information	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>the period needed to accomplish the national security requirement and must not exceed one year. Where access is expected to be more than one year, the contractor employee is required to be sponsored for a security clearance.</p> <p>(3) One-time access will only be granted to U.S. citizens with a willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A request by a contractor to process one-time access to classified information must be approved by the most senior DOE-cleared management official of the company holding the affected contract and the DOE Program Secretarial Officer with jurisdiction over the office where the contractor employee will be employed. Specific requirements and processes related to the issuance one-time access to classified information is set forth in Attachment 4.</p>						
6.	Limited Access Authorizations (NON-U.S. CITIZENS.)						
6.a	Only U.S. citizens are eligible for a security clearance. Contractors must make every effort to ensure that non-U.S. citizen employees are not assigned	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply with information stated in	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	to perform duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen contractor employee. Where a non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific Departmental mission involving access to classified information, and a qualified U.S. citizen eligible for such access is not available, contractors may submit non-U.S. citizens for consideration of a Limited Access Authorization (LAA). LAAs provide limited access to certain types of classified information by non-U.S. citizens, and are subject to strict controls and conditions. Such submissions must include detailed information concerning the steps the contractor took to secure the services of a United States citizen.		the section when considering interim security clearances. SLAC will make every effort to ensure that non-U.S. citizen employees are not assigned to perform duties that may require access to classified information. Although if necessary SLAC will comply with all directives in regards to submitting a non-U.S. citizen for a Limited Access Authorization.				
6.b	LAAs will not permit access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which an individual is currently a citizen. DOE’s Headquarters Office of the General Counsel will make this assessment.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC is aware that an LAA will not permit access to any greater level of classified information than the U.S Government has determined may be releasable to the country of which an individual is currently a citizen.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	LAA's may only be approved if a background investigation at the level required by Executive Order 12968, or successor national-level standards is conducted.		Also, that an LAA may only be approved if a background investigation at the level by Executive Order 12968, or successor national-level standards is conducted.				
6.c	A request by a contractor to process a non-U.S. citizen for an LAA must be approved by the most senior DOE-cleared management official of the company holding the affected contract and the DOE Program Secretarial Officer with jurisdiction over the office where the contractor employee will be employed. Specific requirements and processes related to the issuance of LAA's are set forth in Attachment 3.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC is aware that a request to process a non-U.S. citizen for an LAA must be approved by the most senior DOE-Cleared management official of SLAC.	n/a	n/a	n/a	n/a
7	REPORTING AND OTHER REQUIREMENTS.						
7.a	All cleared contractor employees (including individuals with a suspended clearance) and applicants must follow the guidance in Attachment 5. Cleared contractor employees incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware of and will convey to all cleared contractor employees (including individuals with a suspended Clearance) and applicants that they must follow the guidance in Attachment 5. Also, that all cleared contractor employees incur a special and continuing security obligation to be aware of the risks associated with foreign intelligence	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			operations and/or possible terrorist activities directed against them in the U.S. and abroad.				
7.b	Cleared contractor employees also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility. Cleared contractor employees must report any planned or actual involvement in any of the activities as indicated in Attachment 5, or otherwise as soon as possible following the start of their involvement	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will convey to all cleared contractor employees that they also have a responsibility to recognize and avoid personal behaviors and activities that may adversely impact their continued national security eligibility. Cleared contractor employees must report any planned or actual involvement in any of the activities as indicated in Attachment 5, or otherwise as soon as possible following the start of their involvement</p>	n/a	n/a	n/a	n/a
7.c	Failure to comply with reporting requirements may result in administrative action that includes, but is not limited to, revocation of the cleared contractor employee's security clearance..	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC is aware and will convey to all cleared contractor employees that failure to comply with reporting requirements may result in administrative action that includes, but is not limited to, revocation of the cleared</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			contractor employee’s security clearance.				
7.d	Reportable Information (see Attachment 5) must be reported verbally or in writing directly to the CPSO immediately upon the individual becoming aware of the situation or incident. If the information is verbally reported, a written confirmation must be submitted within three (3) working days after the situation or incident.	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that all reportable information is reported verbally or in writing directly to the CPSO immediately upon the individual becoming aware of the situation or incident. If the information is verbally reported, a written confirmation will be submitted within three (3) working days after the situation or incident.</p>	n/a	n/a	n/a	n/a
7.e	<p>Contractors must notify the CPSO of any of the following conditions affecting the status of a contractor applicant's or employee's security clearance. All notifications under this paragraph must be made within three (3) working days followed by written confirmation within the next ten (10) working days.</p> <p>(1) When made aware of any other information of a personnel security interest, as delineated in Attachment 5,</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will notify the CPSO of any of the following conditions affecting the status of a contractor applicant’s or employee’s security clearance. All notifications under this paragraph will be made within three (3) working days followed by written confirmation within the next ten (10) working days.</p> <p>(1) When made aware of any information of</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>concerning a contractor applicant or employee;</p> <p>(2) When the contractor restricts or withdraws a contractor employee's access to classified information or SNM without DOE direction;</p> <p>(3) When a cleared employee is terminated under unfavorable circumstances, regardless of the reason for the termination;</p> <p>(4) When made aware of the death of a contractor applicant or employee; or</p> <p>(5) When a cleared contractor employee is transferred to another location (minimally, this will apply when a contractor employee's security clearance moves to the jurisdiction of another CPSO).</p>		<p>a personnel security interest, as delineated in Attachment 5, concerning a SLAC applicant or Employee;</p> <p>(2) When SLAC restricts or withdraws a employee's access to classified information or SNM without DOE direction;</p> <p>(3) When a cleared employee is terminated under unfavorable circumstance, regardless of the reason for the termination;</p> <p>(4) When made aware of the death of a SLAC applicant or employee; or</p> <p>(5) When a cleared SLAC employee is transferred to another location (minimally, this will apply when a SLAC employee's security clearance moves to the jurisdiction of another CPSO</p>				
7.f	<p>The contractor must inform contractor applicants and employees who are applying for or in possession of a security clearance that they have a specific obligation to truthfully provide all information requested for personnel security purposes to DOE. Contractors and clearance holders must:</p> <p>(1) Provide full, frank, and truthful</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will inform all contractor applicants and employees who are applying for or in possession of a security clearance that they</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

<p>answers to relevant and material questions.</p> <p>(2) Furnish, or authorize others to furnish if necessary, information that DOE deems necessary to the security clearance eligibility process, when requested.</p> <p>(3) Report any situations or incidents as they occur that may have the tendency to impact the individual's eligibility for a security clearance verbally and in writing and directly to DOE immediately upon the individual becoming aware of the situation or incident and in no event later than three (3) working days after the event (see Attachment 5).</p> <p>(4) Notify CPSO whenever they learn of the presence of any such situations or incidents that may have the tendency to impact an individual's eligibility for a security clearance regarding anyone they know to possess a DOE security clearance or to be in the process of obtaining a DOE security clearance immediately upon the individual becoming aware of the situation or incident and in no event later than three (3) working days after the event.</p> <p>(5) The foregoing responsibilities apply when completing security forms,</p>		<p>have a specific obligation to truthfully provide all information requested for personnel security purposes to DOE. Contractors and clearance holders must:</p> <p>(1) Provide full, frank, and truthful answers to relevant and material questions.</p> <p>(2) Furnish, or authorize others to furnish if necessary, information that DOE deems necessary to the security clearance eligibility process, when requested.</p> <p>(3) Report any situations or incidents as they occur that may have the tendency to impact the individual's eligibility for a security clearance verbally and in writing and directly to DOE immediately upon the individual becoming aware of the situation or incident and in no event later than three (3) working days after the event (see Attachment 5).</p> <p>(4) Notify CPSO whenever they learn of the presence of any such situations or incidents that may have the tendency to impact an individual's eligibility for a security clearance regarding anyone they know to possess a DOE security clearance or to be in the process of obtaining a DOE security clearance immediately upon the individual becoming aware of the situation or incident and in no event later than three (3)</p>				
---	--	---	--	--	--	--

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>during all personnel security investigations and at any stage of the security clearance process including, but not limited to letters of interrogatory, personnel security consultations, DOE-sponsored mental health evaluations and other authorized investigative activities.</p> <p>(6) All DOE contractor employee security clearance holders and applicants who are approached by any individual seeking unauthorized access to classified information or SNM, or who experience any other potentially counterintelligence-related incidents, must report such information in accordance with DOE O 475.1, Counterintelligence Program, current version.</p>		<p>working days after the event.</p> <p>(5) The foregoing responsibilities apply when completing security forms, during all personnel security investigations and at any stage of the security clearance process including, but not limited to letters of interrogatory, personnel security consultations, DOE-sponsored mental health evaluations and other authorized investigative activities.</p> <p>(6) All DOE contractor employee security clearance holders and applicants who are approached by any individual seeking unauthorized access to classified information or SNM, or who experience any other potentially counterintelligence-related incidents, must report such information in accordance with DOE O 475.1, Counterintelligence Program, current version.</p>				
7.g	<p>Failure or refusal to cooperate with any of these activities may prevent DOE from granting or continuing a security clearance. In this event, any current security clearance may be administratively withdrawn or, for contractor applicants, further processing of a security clearance</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC Is Aware that failure or refusal to cooperate with any of these activities may</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	request may be terminated.		prevent DOE from granting or continuing a security clearance. In this event, any current security clearance may be administratively withdrawn or, for contractor applicants, further processing of a security clearance request may be terminated.				
7.h	Contractor employees with active security clearances will be initially briefed and annually briefed regarding their personnel security responsibilities in accordance with the CRD attached to DOE O 470.4B	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that all security clearance applicants and holders under their cognizance are made aware of the foregoing reporting responsibilities, through initial briefings and annual briefings.	n/a	n/a	n/a	n/a
8	ADMINISTRATIVE WITHDRAWAL OF SECURITY CLEARANCES						
8.a	The contractor must request the CPSO administratively withdraw a contractor employee's security clearance when an individual terminates employment or when official duties no longer require access to classified information or SNM. The contractor must provide the CPSO a DOE F 5631.29, Security Termination Statement, completed by the contractor employee, within three (3) working	In Compliance	Sections is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will request the CPSO administratively withdraw a contractor employee's security clearance when an individual terminates employment or when	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	days upon termination of employment or when official duties no longer require access to classified information or SNM.		official duties no longer require access to classified information or SNM. The contractor must provide the CPSO a DOE F 5631.29, Security Termination Statement, completed by the contractor employee, within three (3) working days upon termination of employment or when official duties no longer require access to classified information or SNM.				
8.b	The purpose of DOE F 5631.29 is to ensure that the individual is aware of the continuing responsibility to protect classified information and SNM after withdrawal of a security clearance. In cases where it is not possible to obtain the individual's signature, the completed but unsigned DOE F 5631.29 must still be submitted. In addition, the contractor must provide an explanation to the CPSO of the circumstances surrounding the withdrawal and why the employee's signature could not be obtained.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program SLAC is aware of the purpose of DOE F 5631.29. SLAC will request the CPSO to administratively withdraw an employee's clearance even in cases where SLAC cannot provide a completed DOE F 5631.29 immediately. In these cases where it is not possible to obtain an individual's signature, SLAC will submit the completed but unsigned DOE F 5631.29 with an explanation to the CPSO of the circumstances surrounding the withdrawal and why the employee's signature could not be obtained.	n/a	n/a	n/a	n/a
9	SECURITY CLEARANCE PENDING REEMPLOYMENT/	In Compliance	Section is addressed in SLAC Plan for Personnel Security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>REASSIGNMENT</p> <p>The CPSO may approve a contractor request for an individual who is terminating employment with the contractor per paragraph 8.a(1) of this CRD to retain a security clearance when the contractor verifies that the individual will be reemployed or reassigned by the contractor within the next 60 calendar days to a position that will require a security clearance.</p>		<p>SLAC will comply per our Personnel Security Program</p> <p>SLAC is aware that the CPSO may approve a request from SLAC for an individual who is terminating employment with SLAC to retain a security clearance when SLAC verifies that the individual will be reemployed or reassigned by SLAC within the next 60 calendar days to a position that will require a security clearance.</p>				
10	<p>SECURITY CLEARANCE REINSTATEMENT REQUESTS</p> <p>The contractor must request that the CPSO consider reinstating a security clearance for a contractor applicant or employee when the contractor is aware that the individual previously held a security clearance. The CPSO will advise the contractor whether the individual must complete a new set of security forms, update information previously provided, or be subject to additional investigation per the provisions of the DOE personnel security Order.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program</p> <p>SLAC must request that the CPSO consider reinstating a security clearance for a SLAC applicant or employee when SLAC is aware that the individual previously held a security clearance. The CPSO will advise SLAC whether the individual must complete a new set of security forms, update information previously provided, or be subject to additional investigation per the provisions of the DOE personnel security order.</p>	n/a	n/a	n/a	n/a
11	<p>SECURITY CLEARANCE UPGRADE REQUESTS</p> <p>The contractor must request that the</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	CPSO upgrade a contractor employee’s security clearance in accordance with any new, higher access requirements associated with the duties of the position. The request must be accompanied by appropriate personnel security forms and a revised security clearance justification statement, as directed by the CPSO.		Security Program SLAC will request that the CPSO upgrade a SLAC employee’s security clearance in accordance with any new, higher access requirements associated with the duties of the position. SLAC will provide the appropriate personnel security forms and a revised security clearance justification statement as directed by the CPSO.				
12	SECURITY CLEARANCE DOWNGRADE REQUESTS The contractor must request that the CPSO downgrade a contractor employee’s security clearance in accordance with any new, lower access requirements associated with the duties of the position. The request must be accompanied by a revised security clearance justification statement.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program SLAC will request that the CPSO downgrade a SLAC employee’s security clearance in accordance with any new, lower any new, lower access requirements associated with the duties of the position. SLAC will provide a revised security clearance justification statement to the CPSO.	n/a	n/a	n/a	n/a
13	SECURITY CLEARANCE SUSPENSION, REVOCATION AND DENIAL						
13.a	Upon receipt of notification from the CPSO of an employee’s security clearance suspension or denial of final security clearance after previous approval of an interim, the contractor must ensure that the employee is	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	precluded from access to classified information and SNM		Upon receipt of notification from the CPSO of an employee’s security clearance suspension or denial of final security clearance after previous approval of an interim, SLAC will ensure that the employee is precluded from access to classified information. NO SNM at SLAC				
13.b	Suspension, denial, or revocation of an individual’s security clearance does not preclude the contractor from assigning or transferring the individual to duties that do not require a security clearance.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that a suspension, denial, or revocation of an individual’s security clearance does not preclude SLAC from assigning or transferring the individual to duties that do not require a security clearance.	n/a	n/a	n/a	n/a
14	TRAINING. All cleared contractor employees and any contractor employees involved in personnel security activities must be fully qualified as necessary relative to their particular duties and responsibilities, in accordance with national and Departmental requirements.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware and will ensure that all cleared SLAC employees and any SLAC employees involved in personnel security activities will be fully qualified as necessary relative to their particular duties and	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			responsibilities, in accordance with national and Departmental requirements.				
15	RECORDS MAINTENANCE.						
15.a	The contractor must maintain current records that reflect, by contract numbers, all contractor employees granted security clearances. The records must include the contractor employee’s name, DOE file number, and the date the security clearance was granted.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will maintain current records that reflect, by contract numbers, all SLAC employees granted security clearances. The records will include the SLAC employee’s name; DOE file number, and the date the security clearance was granted.	n/a	n/a	n/a	n/a
15.b	Copies of correspondence to and from DOE that reflect security clearance matters for each contractor applicant and employee must be maintained including: the request for a security clearance, notification that security clearance action was effected, and security clearance termination and administrative withdrawal action. Such copies must be maintained while the individual holds a security clearance at the contractor’s request and for a period of two (2) years after the date the individual’s security clearance is terminated, at which time they may be destroyed.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will maintain copies of correspondence to and from DOE that reflect security clearance matters for each SLAC applicant and employee including: the request for a security clearance, notification that security clearance action was effected, and security clearance termination and administrative withdrawal action. SLAC will maintain copies while the individual holds a	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			security clearance at SLAC’s request and for a period of two (2) years after the date the individual’s security clearance is terminated, at which time they may be destroyed.				
15.c	All records and information pertaining to contractor applicant and employee security clearance matters, including copies of personnel security forms and information collected from the conduct of pre-employment or pre-processing checks, must be protected against unauthorized disclosure in accordance with the Privacy Act of 1974 (5 U.S.C 552a). Information collected by the contractor for security clearance processing must not be used by the contractor for any purpose other than that for which it is intended and must not be provided to non-contractor employees or any other entity or organization without prior approval from the CPSO	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will maintain all records and information pertaining to SLAC applicants and employee security clearance matters and protect these records against unauthorized disclosure. Also, any info collected by SLAC for the purpose of security clearance processing will not be used by SLAC for any other purpose other than that for which it is intended and will not be provided to non-SLAC employees or any other entity or organization without prior approval from the CPSO	n/a	n/a	n/a	n/a
16	RECERTIFICATIONS AND REINVESTIGATIONS						
16.a	The contractor must comply with periodic DOE requests to recertify its employees’ security clearance status.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			SLAC will comply with all periodic DOE requests to recertify its employees' security clearance status.				
16.b	The contractor must comply with a request for recertification or for an examination of security clearance or other records that may be requested during the conduct of a DOE security survey or special survey.	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will comply with all requests for recertification or for an examination of security clearance or other records that may be requested during the conduct of a DOE security survey or special survey.</p>	n/a	n/a	n/a	n/a
16.c	The contractor must ensure that cleared contractor employees cooperate fully with DOE requirements concerning reinvestigations.	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that cleared SLAC employees cooperate fully with DOE requirements concerning reinvestigations.</p>	n/a	n/a	n/a	n/a
17	ACTIONS BY THE SECRETARY. Nothing in this CRD will be construed to limit the Secretary's authorities and responsibilities under Executive Order 12968 (section 1.2(b), et al), Executive Order 10865 (section 9) or the AEA to grant, continue, deny or terminate a	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	security clearance in the interest of national security, or to modify or withhold certain due process procedures set forth at 10 CFR 710.		SLAC is aware of and will comply with the directives in this section.				

Attachment 2 – Security Clearance Requests/Justifications and Access Authorizations

This attachment provides information and/or requirements associated with DOE O 472.2 and is applicable to contracts in which the associated CRD (Attachment 1) is included.

§	Requirement from Attachment 2 – Security Clearance Requests/Justifications and Access Authorizations	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1	<p>1. In addition to the information set forth elsewhere in the body of this Order and in the CRD, all justifications for security clearances (for both initial and reinvestigation actions) must contain the following:</p> <p>a. Full name of the individual.</p> <p>b. Individual's Social Security Number.</p> <p>c. Date and place of birth.</p> <p>d. Individual's status (Federal employee/contractor employee).</p> <p>e. Contractor name (if contractor</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that all information listed in this section is contained in all justifications for security clearances (initial and reinvestigate actions). SLAC will comply per our Personnel Security Program.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 2 – Security Clearance Requests/Justifications and Access Authorizations	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>applicant/employee).</p> <p>f. Primary program code (e.g., EM - Environmental Management; FE – Fossil Energy and Carbon Management; IG - Inspector General; NE - Nuclear Energy; OE - Office of Enforcement; NNSA - Nuclear Security/Administrator for National Nuclear Security Administration; SC - Office of Science).</p> <p>g. Facility code (if contractor employee).</p> <p>h. Level of security clearance required, i.e., TS, S, C, Q or L.</p> <p>i. A detailed description (without revealing classified information) as to why the individual requires access. The description must include a full explanation of the information to be accessed, how often the access is needed, and for what programs/projects the information is needed.</p> <p>j. Full name, title, and telephone number of the requester.</p> <p>k. Signature of the requester.</p>						
2	All initial security clearance requests (to	In Compliance	Section is addressed in SLAC Plan for	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

	<p>include first-time clearance requests and reapprovals) must include the justification, as set forth in 1. above, except in cases where reciprocity applies, as indicated by an '*':</p> <p>a. Negative results of a drug test dated no more than 90 calendar days prior to the individual's SF-86 signature or, for cases being considered under reciprocity, no more than 90 calendar days prior to the date of the security clearance request (not required for employees of state or local governments).</p> <p>b. An SF-87, Fingerprint Chart (for Federal employees); an FD 258, Applicant Fingerprint Chart (for all others); or fingerprints taken electronically via an approved capture method (e.g., at a GSA-provided Homeland Security Presidential Directive-12 enrollment center), when available. Note: Fingerprints are not required if a previous investigation included a classifiable fingerprint search by the Federal Bureau of Investigations.</p> <p>c. DOE F 5631.18, Security Acknowledgement.</p>		<p>Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that all initial security clearance requests include justification and all the documentation listed in this section.</p>				
3	In addition to TS, S, and C security clearances and L and Q access authorizations, all of which are granted	In Compliance	Section is addressed in SLAC Plan for Personnel Security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

<p>by CPSOs, the DOE issues several other types of access authorizations. These other access authorizations are issued by the DOE office indicated:</p> <p>a. Sensitive Compartmented Information (SCI). SCI access must be approved by the DOE Senior Intelligence Officer or their designated representative within the Office of Intelligence and Counterintelligence.</p> <p>b. Cryptographic Information (CRYPTO). CRYPTO access is approved by the Office of Technical Security.</p> <p>c. Communications Security (COMSEC). COMSEC access is approved by the Office of Technical Security.</p> <p>d. Nuclear Weapon Data. Requirements and procedures for access to nuclear weapon data (categorized as SIGMA information) is determined and promulgated by the National Nuclear Security Administration (NNSA) using DOE and NNSA directives. For additional information, consult DOE O 452.8, Control of Nuclear Weapon Data, current version; DOE O 452.7, Protection of Use Control Vulnerabilities and Designs, current version; and DOE O 457.1, Nuclear</p>		<p>SLAC will comply per our Personnel Security Program.</p> <p>The sole purpose for SLAC holding an FCL is to process security clearance requests for SLAC employees for work on DOE projects or DOE facilities outside of SLAC. Any additional access authorizations will be approved by the appropriate authority.</p>				
---	--	--	--	--	--	--

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 2 – Security Clearance Requests/Justifications and Access Authorizations	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>Counterterrorism, current version.</p> <p>e. Special Access Program (SAP). A SAP is 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. Access to any SAP must be granted in accordance with procedures established within DOE O 471.5, Special Access Programs, current version.</p> <p>f. North Atlantic Treaty Organization Information (NATO). NATO access requires NNSA approval from the Office of Security Operations and Performance Assurance.</p>						

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

Attachment 3 – Limited Access for Non-U.S. Citizens

This attachment provides information and/or requirements associated with DOE O 473.3 and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1	Limited Access Authorizations for Non-U.S. Citizens						
1	This section deals solely with non-U.S. citizens who have not been investigated or cleared by any foreign government. Non-U.S. citizens who have been investigated and granted the equivalent of a security clearance by a foreign government may be granted access to classified information at DOE via the passing of a security assurance by the foreign government to DOE in accordance with DOE O 142.1, Classified Visits Involving Foreign Nationals, dated 01-13-04, or any successor directive	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
2	Where there are compelling reasons in furtherance of a DOE mission, non-U.S. citizens who possess a special expertise may be granted limited access to classified information only for specific programs, projects or contracts for which there is need for access. Such individuals will not be eligible for access to any greater level of classified information than the United States Government has determined may be	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	releasable to the country of which the individual is currently a citizen. The DOE Office of the General Counsel must be consulted by the Director to make this assessment. Such limited access may be approved only if an investigation of the level required by Executive Order 12968, or successor national standards, for a Top Secret security clearance can be conducted.						
3.	<p>A non-U.S. citizen granted an LAA is not eligible for access to SNM or to any of the following types of classified information:</p> <p>a. TS, Cryptographic (CRYPTO), Restricted Data, Formerly Restricted Data or Special Access Program information.</p> <p>b. Information that has not been determined by a USG Designated Disclosure Authority to be releasable to the country of which the individual is a citizen.</p> <p>c. Communication Security (COMSEC) information.</p> <p>d. Sensitive Compartmented Information</p>	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>(SCI) or Intelligence information.</p> <p>e. North Atlantic Treaty Organization (NATO) Information. However, a national of a NATO member nation may be authorized access to NATO information provided that a NATO Security Clearance Certificate is obtained by DOE from the individual's home country and such access is limited to performance on a specific NATO contract.</p> <p>(1) Information for which foreign disclosure has been prohibited in whole or in part (identified as Not Releasable to Foreign National (NOFORN)).</p> <p>(2) Classified information provided to the USG by a third party government and information furnished in confidence to the USG by a third party government.</p>						
4.	The Program Secretarial Officer with jurisdiction over the information to be released to the non-U.S. citizen must submit a detailed request and justification for the desired LAA to the appropriate Cognizant Personnel Security Office (CPSO).	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
5.	Upon receipt of the request, the CPSO will conduct an interview with the non	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>U.S. citizen to determine:</p> <p>a. The nature and extent of the individual’s contacts and continuing associations with persons outside the United States (to include family members);</p> <p>b. The degree to which the individual exercises his or her foreign citizenship;</p> <p>c. Whether the individual or any of the individual's associates (to include family members) are or have been affiliated with any foreign government, and</p> <p>d. After completion of the consultation, the CPSO may, through the local DOE counterintelligence office, request a preliminary counterintelligence-focused risk assessment. If the results of this risk assessment indicate that it would not be feasible to continue with the LAA process, the CPSO will notify the requesting Program Secretarial Officer.</p>		LAA's.				
6.	If the results of the risk assessment support continued processing, the CPSO will forward the results of the consultation and risk assessment, along with all other relevant information, to the Director.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
7.	After reviewing all available	Non-applicable	SLAC is a non-possessing facility as such	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	information, the Director in coordination with appropriate headquarters authorities, will: a. Determine to continue processing the LAA request, in which case the Director will notify the CPSO to commence processing the individual for a background investigation, or b. Determine that the individual will not be processed for an LAA. In this case, the Director will notify the CPSO and the applicable Program Secretarial Officer.		we do not foresee submitting requests for LAA's.				
8.	In the case of a determination as in 7.(a), above, the CPSO will process the individual for a background investigation in accordance with investigative and adjudicative procedures set forth in this Order.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
9.	When the CPSO has reached an adjudicative determination, the CPSO may coordinate a formal comprehensive counterintelligence-focused risk assessment with the local DOE counterintelligence office.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
10.	The CPSO will then forward the results of the adjudication and the risk assessment to the Director for concurrence.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 3 – Limited Access for Non-U.S. Citizens	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
11.	The Director will approve/concur and instruct the CPSO to grant the LAA or will disapprove/non-concur and notify the CPSO and the applicable Program Secretarial Officer. The Director's determinations in these cases are final.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
12	The CPSO must review all LAAs annually to ensure that they are still needed. The Program Secretarial Officer who initially requested the LAA must annually re-justify each request. Annual re-concurrence of the Director is not needed, provided the CPSO has no reason to believe the individual may no longer meet the requirements of the LAA. The Department retains authority to conduct routine reinvestigations as needed for individuals granted LAAs.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
13.	LAAs must be administratively withdrawn by the CPSO immediately upon receiving confirmation that the individual is no longer affiliated with DOE or otherwise no longer requires the access for which the LAA was granted, or at the direction of the Director.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a
14.	The CPSO must immediately withdraw an LAA upon receiving confirmation that the individual is no longer affiliated with DOE or otherwise no longer requires the access for which the LAA was granted, or at the direction of the Director.	Non-applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for LAA's.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

Attachment 4 – Temporary Eligibility

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1.	When urgent operational or contractual exigencies or exceptional circumstances exist CPSO's may grant temporary security clearance eligibility in accordance with Security Executive Agent Directive 8 and this attachment.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that when urgent operational or contractual exigencies or exceptional circumstance exist CPSO's may grant temporary security clearance eligibility in accordance with Security Executive Agent Directive 8 and this attachment.	n/a	n/a	n/a	n/a
2.	Temporary Access to Classified Information (Interim Security Clearances).			n/a	n/a	n/a	n/a
2.a	The need for temporary access to classified information must originate with the supervisory/management and be approved in writing by the Federal head of the applicable Departmental element in which the individual will be assigned (Note: individuals may not request temporary access on their own behalf).	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that the need for temporary access to classified information must originate with SLAC's supervisory/management and be approved by Site Office Lead in which the individual is assigned.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			SLAC is aware that individuals may not request temporary access on their own				
2.b	<p>All such requests must be provided to the CPSO and must include a detailed justification which explains why:</p> <p>(1) A serious delay of, or interference in, an operation or project essential to a DOE program will occur unless the individual is granted access to classified information or SNM before completion of the normal security clearance process, and</p> <p>(2) The services of a qualified person who is currently cleared to access the necessary classified information or SNM cannot be obtained.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will provide all such requests to the CPSO and will include a detailed Justification that explains why:</p> <p>(1) A serious delay of, or interference in, an operation or project essential to a DOE program will occur unless the individual is granted access to classified information or SNM before completion of the normal security clearance process, and</p> <p>(2) The services of a qualified person who is currently cleared to access the necessary classified information or SNM cannot be obtained</p>	n/a	n/a	n/a	n/a
2.c	<p>Temporary access to classified information may only be requested in conjunction with, or following, the submission of an associated security clearance request, as set forth in this Order, including Attachment 2.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC is aware temporary access to classified information may only be requested in conjunction with, or following, the</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			submission of an associated security clearance request, as set forth in this Order, including Attachment 2.				
2.d	The CPSO will review the individual's personnel security forms and PSF/ePSF (if one exists) to determine whether the case contains any information of a security concern. If so, the CPSO must notify the requester that the request for temporary access to classified information has been denied, and that the case must proceed according to normal processing procedures.	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC is aware the CPSO will review the individual's personnel security forms and PSF/ePSF(if one exists) to determine whether the case contains any information of a security concern. If so, the CPSO must notify the requester that the request for temporary access to classified information has been denied, and that the case must proceed according to normal processing procedures.</p>	n/a	n/a	n/a	n/a
2.e	<p>Requests for temporary access to classified information in cases for which there is no information of a security concern will be approved by the CPSO and processed accordingly provided that:</p> <p>(1) The appropriate investigation has been submitted and expedited to the Investigative Service Provider (ISP).</p> <p>(2) Approvals for Temporary Access to Confidential, Secret, and L require:</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC is aware that Requests for temporary access to classified information in cases for which there is no information of a security concern will be approved by the CPSO and processed accordingly provided that:</p> <p>(1) The appropriate investigation has been submitted and expedited to the Investigative</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	(a) Favorable review of a completed SF-86 by the authorized adjudicative agency; (b) Citizenship verification; and (c) Completion and favorable review of a Federal Bureau of Investigation (FBI) fingerprint check. (3) Approvals for Temporary Access to Top Secret and Q require: (a) Favorable review of a completed SF-86 by the authorized adjudicative agency; (b) Citizenship verification; and (c) Completion and favorable review of a Federal Bureau of Investigation (FBI) fingerprint check. (a) Favorable review of a completed SF-86 by the authorized adjudicative agency; (b) Citizenship verification; and (c) Completion and favorable review of the following: 1 FBI fingerprint check; 2 FBI name check; and 3 National Crime Information Center (NCIC) check.		Service Provider (ISP) (2) Approvals for Temporary Access to Confidential, Secret, and L require: (a)Favorable review of a completed SF-86 by the authorized adjudicative agency; (b)Citizenship verification; and (c)Completion and favorable review of a Federal Bureau of Investigation (FBI) fingerprint check. (3) Approvals for Temporary Access to Top Secret and Q require: (a)Favorable review of a completed SF-86 by the authorized adjudicative agency; (b)Citizenship verification; and (c)Completion and favorable review of the following: (1) FBI fingerprint check; (2) FBI name check; and (3) National Crime Information Center (NCIC) check.				

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
2.f	Supporting rationale for all temporary access to classified information will be recorded in the individual's PSF/ePSF. All temporary access to classified information will be noted as such wherever security clearances are recorded, both internally within DOE and in all DOE submissions to national security clearance databases.	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC is aware that all Supporting rationale for all temporary access to classified information will be recorded in the individual's PSF/ePSF. All temporary access to classified information will be noted as such wherever security clearances are recorded, both internally within the DOE and in all DOE submissions to national security Clearance Databases.</p>	n/a	n/a	n/a	n/a
2.g	All individuals who are issued temporary access to classified information must be notified in writing that their continued security clearance is conditional upon favorable completion of the pending investigation, and may be canceled at any point where information of a security concern arises. Cancellations cannot be appealed and adjudication of the individual's eligibility for a security clearance will continue upon receipt of the completed investigation.		<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC ensure that all individuals who are issued temporary access to classified information are notified in writing that their continued security clearance is conditional upon favorable completion of the pending investigation and may be canceled at any point where information of a security concern arises. Also, that cancellations cannot be appealed and adjudication of the individual's eligibility for a security clearance will continue upon receipt of the completed</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			investigation.				
2.h	If DOE cancels an individual's temporary access to classified information, the individual's employer must ensure that the individual is precluded from access to classified information and/or SNM.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that if the DOE cancels an Individual's temporary access to classified information, SLAC will ensure that the individual is precluded from access to classified information and/or SNM.	n/a	n/a	n/a	n/a
2.i	Access to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to classified information will be granted or denied at the sole discretion of the office with authority for such access.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that access to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to classified information will be granted or denied at the sole discretion of the office with authority for such access.	n/a	n/a	n/a	n/a
3	Temporary Access to a Higher level of Classified Information						
3.a	CPSOs may approve temporary access to a higher level of classified information and/or SNM for a covered individual granted access to a	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	lower level when determined necessary to meet operational or contractual exigencies not expected to be of a recurring nature pursuant to EO 12968, as amended. Access approvals will remain valid until the exigency has abated or the access is terminated. In any case, access must not exceed 180 days. When access is expected to exceed 180 calendar days, the sponsor will request Temporary Access to Classified information in accordance with paragraph 1., above.		Security Program. SLAC is aware that CPSOs may approve temporary access to a higher level of classified information and/or SNM for a covered individual granted access to a lower level when determined necessary to meet operational or contractual exigencies not expected to be of a recurring nature pursuant to EO 12968, as amended. Access approvals will remain valid until the exigency has abated or the access is terminated. In any case, access must not exceed 180 days. When access is expected to exceed 180 calendar days, the sponsor will request Temporary Access to Classified information in accordance with paragraph 1., above.				
3.b	Temporary access to a higher level of classified information must be necessary to meet operational or contractual exigencies not expected to be of a recurring nature. (1) Such higher level of access will be limited to specific, identifiable information and information access records must be maintained. The nature of this information must be referenced on the request for access. (2) Acceptable temporary access to	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that temporary access to a higher level of classified information must be necessary to meet operational or contractual exigencies not expected to be of a recurring nature. And that such higher level of access will be limited to specific, identifiable information	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	higher level of classified information is: L to Q or TS; S to Q or TS; and any C to L or S.		and information access records must be maintained. Also, that the nature of this information must be referenced on the request for access. Acceptable temporary access to higher level of classified information is; L to Q or TS; S to Q or TS; and C to L or S.				
3.c	Requests for temporary access must include a justification and must be forwarded by the appropriate official (i.e., contractor, Federal site manager) with the request to the appropriate CPSO. This submission must set forth the expected duration of the higher level of access, identify the information to which the individual will be afforded access, and describe the exigent circumstances prompting the request.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that requests for temporary access include a justification and will be forwarded by the appropriate official (I.e., contractor, site manager) with the request to the appropriate CPSO. The submission will set forth the expected duration of the higher level of access, identify the information to which the individual will be afforded access, and will describe the exigent circumstances prompting the request.	n/a	n/a	n/a	n/a
3.d	If the CPSO is satisfied that exigent circumstances exist, that routine processing of the individual for the higher level of access to classified information would adversely impact mission needs, is not in possession of information indicating that access at the higher level of access to classified	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that if the CPSO is satisfied that exigent circumstances exist, that routine	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	information would jeopardize Departmental interests or the national security, and that the request is not an attempt to circumvent normal security clearance processing requirements, the CPSO must grant the higher level of access. Otherwise, the request must be denied and returned to the requester with an explanation as to the reason(s) for the denial.		processing of the individual for the higher level of access to classified information would adversely impact mission needs, is not in possession of information indicating that access at the higher level of access to classified information would jeopardize Departmental interests or the national security, and that the request is not an attempt to circumvent normal security clearance processing requirements, the CPSO must grant the higher level of access. Otherwise, the request must be denied and returned to the requester with an explanation as to the reason(s) for the denial.				
3.e	Recipients of temporary access to a higher level of information must possess a current security clearance and the access required will be limited to classified information or SNM one level higher than the recipient's current security clearance.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that recipients of temporary access to a higher level of information possess a current security clearance and the access required will be limited to classified information or SNM one level higher than the recipient's current security clearance.	n/a	n/a	n/a	n/a
3.f	Temporary access to higher level of classified information must be recorded in the recipient's PSF/ePSF and in the CPCI, but will not be included in submissions to	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	inter-agency databases. Such security clearances are not subject to reciprocity.		SLAC will record temporary access to a higher level of classified information in the recipient's PSF/ePSF and in the CPCI, but it will not be included in submissions to inter-agency databases. SLAC is aware such security clearances are not subject to reciprocity.				
3.g	Access at the higher level will be facilitated under the general supervision of a fully-cleared individual. The individual charged with providing such supervision will be responsible for the general custody of the information provided.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that access at the higher level will be facilitated under the general supervision of a fully-cleared individual. SLAC is aware that the individual charged with providing such supervision will be responsible for the general custody of the information provided.	n/a	n/a	n/a	n/a
3.h	Such higher level access must be canceled and associated access terminated promptly when no longer required, at the conclusion of the authorized period of access, upon notification from the granting authority, or after 180 calendar days from when access was granted, whichever comes first.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure higher level access is canceled and that associated access is terminated promptly when no longer required, at the conclusion of the authorized period of access, upon notification from the	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			granting authority, or after 180 calendar days from when access was granted, whichever comes first.				
3.i	If, during the period of temporary higher level access, information of a security concern arises which indicates that suspension or revocation of the individual's permanent security clearance may be warranted, the temporary higher level access will be canceled and action will be taken under 10 CFR 710 regarding the permanent clearance. No due process or other procedural rights exist regarding temporary access to a higher level of classified information.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that if, during the period of temporary higher level access, information of a security concern arises which indicates that suspension or revocation of the individual's permanent security clearance may be warranted, the temporary higher level access will be taken under 10 CFR 710 regarding the permanent clearance. SLAC is aware no due process or other procedural rights exist regarding temporary access to a higher level of classified information.	n/a	n/a	n/a	n/a
3.j	Temporary access to a higher level of classified information to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to a higher level classified information will be granted or denied at the sole discretion of the office with authority for such access.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that temporary access to a higher level of classified information to other programs or types of information (SAP, COMSEC, CRYPTO, SCI, NATO, or SIGMA) based upon temporary access to a higher level classified information will be	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			granted or denied at the sole discretion of the office with authority for such access.				
4	One-Time Access to Classified Information.						
4.a	a. During exceptional circumstances, CPSOs may approve one-time access to classified information when it is determined to be in the national security interest. One-time access must be limited to individuals whose expertise offers specialized and important benefit and value to the United States Government (USG), or to individuals to whom access to classified information needs to be provided in the interest of national security.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.b	b. One-time access must be limited to the period needed to accomplish the national security requirement and must not exceed one year. Where access is expected to last more than one year, the individual is required to be sponsored by a program office for a security clearance.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.c	c. One-time access must only be granted to U.S. citizens with a willingness and ability to abide by regulations governing the use, handling, and protection of classified information.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
4.d	d. A statement of compelling need must accompany a one-time access request, and must include the following elements: (1) The unique qualifications of the individual(s) and/or the unique circumstances that require access to classified information; (2) The expected benefit to the USG and national security; (3) The expected nature, extent, and level of access to classified information; and dates for which access is required.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.e	CPSOs must record, document, and maintain one-time access to classified information and the dates for which one-time access was granted locally in the Clearance Action Tracking System only.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.f	One-time access will not be active for multiple national security requirements unless specifically authorized by the Program Secretarial Officer.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.g	Investigative checks and required information identified below must be obtained, corroborated, and favorably adjudicated prior to granting one-time	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>access. CPSOs must also obtain all required SF-86 consent forms:</p> <p>(1) Confidential, Secret, and L Access. The following information, including PII, will be obtained from the individual and corroborated as required in the Federal Investigative Standards (FIS) prior to access authorization:</p> <p>(a) Full name;</p> <p>(b) Date and place of birth;</p> <p>(c) Social security number;</p> <p>(d) Other names used;</p> <p>(e) Citizenship to include dual/multiple citizenship;</p> <p>(f) Current address;</p> <p>(g) Current employment;</p> <p>(h) Police record; and</p> <p>(i) Prior investigations and clearance.</p> <p>2) The following records checks will be conducted and favorably</p>						

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	adjudicated prior to approving access: (a) Intelligence Community (IC) Scattered Castles (or successor); (b) Defense Information System for Security (DISS) or Central Verification System (CVS) (or successor); and (c) NCIC check. (3) Top Secret and Q Access. The following information, including PII, must be obtained from the individual and corroborated as required in the FIS prior to access authorization: (a) Full name; (b) Date and place of birth; (c) Social security number; (d) Other names used; (e) Citizenship to include dual/multiple citizenship; (f) Current address; (g) Current employment;						

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	(h) Foreign contacts, relatives, and travel; (i) Police record; and (j) Prior investigations and clearance. (4) The following records checks must be conducted and favorably adjudicated prior to approving access: (a) IC Scattered Castles (or successor); (b) DISS or CVS (or successor); (c) FBI name check; (d) NCIC check; and (e) Intelligence Indices.						
4.h	One-time access will be restricted to specific, identifiable classified information, and will be limited only to information needed to fulfill the national security requirement.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.i	Individuals approved for one-time access will not be permitted access to classified information technology systems, except under very limited conditions as approved by the Program Secretarial Officer. Such	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	conditions require restricted access and continuous oversight and monitoring.						
4.j	One-time access to SAP information requires the approval of the establishing authority or the designated program manager. Establishing authorities may implement policies and procedures for one-time access to their SAPs.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.k	Programs must ensure classified information with dissemination control markings that require originator consent for further dissemination (e.g., Dissemination and Extraction of Information Controlled by Originator [ORCON]) be approved by the originator to be shared with individuals who have a one-time access approval. Other control markings that restrict access to certain individuals (e.g., Caution-Proprietary Information Involved [PROPIN], ORCON-USGOV, etc.) must be adhered to.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.l	Individuals approved for one-time access will receive a security briefing and be required to sign an approved nondisclosure agreement prior to receiving classified information.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.m	Individuals will be debriefed	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirements from Attachment 4 – Temporary Eligibility	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	immediately when access is no longer required		do not foresee submitting requests for One-Time Access.				
4.n	One-time access approvals are valid only within the agency granting such access and may be terminated at any time without appeal. CPSOs may accept one-time access approvals from other agencies based on their own assessment of risk on known information about the individual.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.o	One-time access approvals are not to serve as the basis for a subsequent final security clearance; nor are they authorized for convenience or to fill positions that would otherwise require a security clearance.	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a
4.p	One-time access may not be used in lieu of granting temporary access to classified information (interim security clearance).	Non-Applicable	SLAC is a non-possessing facility as such we do not foresee submitting requests for One-Time Access.	n/a	n/a	n/a	n/a

Attachment 5 – Reporting Requirements

This attachment provides information and/or requirements associated with DOE O 472.2 and is applicable to contracts in which the associated CRD (Attachment 1) is included.

The reporting requirements set forth in this Attachment in accordance with 4.w. of the requirements section of the Order, and paragraph 7. of the CRD apply to all applicants for a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

security clearance and covered individuals who hold a security clearance or access authorization, and/or who occupy a national security position, as set forth in 5 CFR 1400 (collectively referred to herein as "covered individuals"). Specific details required when reporting this information, beyond those listed below, will be communicated to covered individuals by the responsible office. Covered individuals will submit reportable information using the appropriate DOE Security Executive Agent Directive (SEAD) 3 reporting form or system form to be developed.

Upon recognition that a covered individual's information may include potential counterintelligence indicators [as identified by the Office of Intelligence and Counterintelligence (IN)], Cognizant Personnel Security Offices (CPSO) will refer the information to the local counterintelligence office. In addition to SEAD 3 reporting requirements, SCI access holders are also subject to the reporting requirements set forth in Intelligence Community Standard 703-02, Reporting Requirements for Individuals with Access to Sensitive Compartmented Information, and DOE O 475.1, Counterintelligence Program, current version.

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1.	Unofficial Foreign Travel						
1.a	Covered individuals must report all unofficial (i.e., personal) foreign travel plans to the appropriate CPSO before the start of travel. If reporting does not occur before planned travel, the covered individuals must report travel to the CPSO as soon as possible after the travel occurs, and no longer than five working days. Reports of planned unofficial foreign travel must include, at a minimum, the following information as available and applicable: (1) Full itinerary;	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure all covered individuals report all unofficial (i.e., personal) foreign travel plans to the appropriate CPSO before the start of travel. If reporting does not occur before planned travel, the covered individuals must report travel to the CPSO as soon as possible after the travel occurs, and no longer than five working days. Reports of	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	(2) Dates of travel; (3) Mode(s) of transport, including identity of carriers; (4) Passport number; (5) Emergency point of contact; (6) Names and association of foreign national traveling companions, and (7) Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted).		planned unofficial foreign travel must include, at a minimum, the following information as available and applicable: (1) Full itinerary; (2) Dates of travel; (3) Mode(s) of transport, including identity of carriers; (4) Passport number; (5) Emergency point of contact; (6) Names and association of foreign national traveling companions, and (7) Planned interactions with foreign governments, companies or citizens during travel and reasons for contact (routine travel/tourism-related contacts excepted).				
1.b	When the need for emergency unofficial foreign travel precludes full compliance with the above requirements, the covered individual must, at a minimum, verbally notify their supervisor/management chain concerning the nature of the emergency. Full reporting must be	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that when the need for emergency unofficial foreign travel	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	accomplished within five (5) working days of return.		precludes full compliance with the above requirements, the covered individual must, at a minimum, verbally notify their supervisor/management chain concerning the nature of the emergency. Full reporting must be accomplished within five (5) working days of return.				
1.c	Covered individuals traveling to a sensitive country must receive an appropriate defensive counterintelligence briefing from the local counterintelligence office prior to travel. Covered individuals must also receive post-travel debriefings from IN for all unofficial foreign travel if applicable in accordance with paragraph 1.e., below. Deviations from sensitive country travel itineraries must be reported immediately upon return, but in no event greater than five (5) working days upon returning to work.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that covered individuals traveling to a sensitive country receive an appropriate defensive counterintelligence briefing from the local counterintelligence office prior to travel. Covered individuals will also receive post-travel debriefings from IN for all unofficial foreign travel if applicable in accordance with paragraph 1.e., below. Deviations from sensitive country travel itineraries will be reported immediately upon return, but in no event greater than five (5) working days upon returning to work.	n/a	n/a	n/a	n/a
1.d	Unplanned border crossings to Canada or Mexico must be reported within five (5) working days of the occurrence.	In Compliance	Section is addressed in SLAC Plan for Personnel Security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			<p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure all unplanned border crossings to Canada or Mexico are reported within five (5) working days of the occurrence.</p>				
1.e	<p>Upon return from any unofficial foreign travel, the covered individual must report the following information to their CPSO/Counterintelligence:</p> <p>(1) Unplanned interactions with foreign governments, companies or citizens, and the reasons for the interaction(s) (not including routine travel/tourism-related contacts);</p> <p>(2) Unusual or suspicious occurrences during travel, including those of a possible security or counterintelligence significance; and</p> <p>(3) Any foreign legal or customs incidents.</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that upon return from any unofficial foreign travel, the covered individual reports the following information to their CPSO/Counterintelligence:</p> <p>(1) Unplanned interactions with foreign governments, companies or citizens, and the reasons for the interaction(s) (not including routine travel/tourism-related contacts);</p> <p>(2) Unusual or suspicious occurrences during travel, including those of a possible security or counterintelligence significance; and</p> <p>(3) Any foreign legal or customs incidents.</p>	n/a	n/a	n/a	n/a
2.	<p>Contacts with Foreign Intelligence. Covered individuals must report all unofficial contacts with any known or</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>suspected foreign intelligence entity to counterintelligence. Reporting must occur immediately upon the covered individual's becoming aware of the contact, and in no event later than three (3) working days [upon returning to work]. Counterintelligence will ensure the information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting must occur immediately upon return to the covered individual's normal duty station, and in no event later than three (3) working days upon returning to work.</p>		<p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals report all unofficial contacts with any known or suspected foreign intelligence entity to counterintelligence. Reporting will occur immediately upon the covered individual's becoming aware of the contact, and in no event later than three (3) working days [upon returning to work]. Counterintelligence will ensure the information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting will occur immediately upon return to the covered individual's normal duty station, and in no event later than three (3) working days upon returning to work.</p>				
3.	<p>Elicitation. Attempted elicitation (to include by media sources), exploitation, blackmail, coercion, or enticement to obtain classified matter or other information or material specifically prohibited by law from disclosure, regardless of means, must be reported by covered individuals to counterintelligence immediately, and in no event later than three (3) working days upon returning to work. Reporting is required regardless of whether the attempt results in a disclosure. Counterintelligence will ensure the</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that attempted elicitation (to include by media sources), exploitation, blackmail, coercion, or enticement to obtain classified matter or other information or material specifically prohibited by law from disclosure, regardless of means, will be reported by covered individuals to counterintelligence immediately, and in no</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting must occur immediately upon return to the cover individual's normal duty station, and in no event later than three (3) working days.		event later than three (3) working days upon returning to work. Reporting is required regardless of whether the attempt results in a disclosure. Counterintelligence will ensure the information is passed to the appropriate CPSO. If this occurs while outside the U.S., reporting must occur immediately upon return to the cover individual's normal duty station, and in no event later than three (3) working days.				
4.	<p>Continuing Association with Foreign Nationals. Covered individuals must report to the appropriate CPSO any unofficial continuing association with known foreign nationals that involves bonds of affection, personal obligation, or intimate contact</p> <p>(Note: cohabitation with any foreign national for more than 30 days, regardless of the nature of the relationship, must be reported under this requirement).</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals report to the appropriate CPSO any unofficial continuing association with known foreign nationals that involves bonds of affection, personal obligation, or intimate contact</p> <p>(Note: cohabitation with any foreign national for more than 30 days, regardless of the nature of the relationship, must be reported under this requirement).</p>	n/a	n/a	n/a	n/a
4.a	This requirement is based on the nature of the relationship, regardless of how or where the contact was made or how the relationship is maintained (i.e., in	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	person, telephonic, mail, internet, etc.).		Security Program. SLAC is aware that this requirement is based on the nature of the relationship, regardless of how or where the contact was made or how the relationship is maintained (i.e., in person, telephonic, mail, internet, etc.).				
4.b	After initial reporting, updates must be provided when there is a significant change (e.g., enduring relationship that involves substantial sharing of personal information and/or the formation of emotional bonds; transitioning from cyber, postal, telephonic, etc. contact to face-to-face contact, establishing an intimate and/or monogamous relationship, and marriage proposals) in the nature of the contact.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure after initial reporting, updates will be provided when there is a significant change (e.g., enduring relationship that involves substantial sharing of personal information and/or the formation of emotional bonds; transitioning from cyber, postal, telephonic, etc. contact to face-to-face contact, establishing an intimate and/or monogamous relationship, and marriage proposals) in the nature of the contact.	n/a	n/a	n/a	n/a
4.c	"Continuing" contact is any contact which recurs, or which might reasonably be expected to recur, but does not include casual contact not based upon affection, obligation, or intimacy.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			SLAC is aware that “continuing” contact is any contact which recurs, or which might reasonably be expected to recur, but does not include casual contact not based upon affection, obligation, or intimacy.				
4.d	Covered individuals must report under this section immediately after it becomes apparent that contact is continuing, and in no event later than three (3) working days.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that covered individuals report under this section immediately after it becomes apparent that contact is continuing, and in no event later than three (3) working days.	n/a	n/a	n/a	n/a
5	Foreign Activities. The following foreign activities must be reported by covered individuals to the appropriate CPSO immediately, but in no event later than three (3) working days: a. Direct involvement in a foreign business; b. Opening of a foreign bank account; c. Purchase of a foreign property (whether located in a foreign country or not); d. Application for or receipt of foreign	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that the following foreign activities are reported by covered individuals to the appropriate CPSO immediately, but in no event later than three (3) working days: a. Direct involvement in a foreign business; b. Opening of a foreign bank account; c. Purchase of a foreign property (whether	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	citizenship; e. Application for, possession, or use of a foreign passport or identity card for travel; f. Voting in a foreign election; g. Adoption of a non-U.S. citizen child.		located in a foreign country or not); d. Application for or receipt of foreign citizenship; e. Application for, possession, or use of a foreign passport or identity card for travel; f. Voting in a foreign election; g. Adoption of a non-U.S. citizen child				
6	Other Reportable Information. The following occurrences/actions must be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure the following occurrences/actions are reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	n/a	n/a	n/a	n/a
6.a	Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, state, or other law enforcement authorities for violations of law within or outside the U.S. Traffic violations for which a fine of less than \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, state, or	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			other law enforcement authorities for violations of law within or outside the U.S. Traffic violations for which a fine of less than \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.				
6.b	Financial anomalies including, but not limited to: (1) Bankruptcy; (2) Wage garnishment; (3) Delinquency more than 120 days on any debt; (4) Unusual infusions of assets more than \$10,000 or greater, such as inheritance, winnings, or similar financial gain.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Financial anomalies including, but not limited to: (1) Bankruptcy; (2) Wage garnishment; (3) Delinquency more than 120 days on any debt; (4) Unusual infusions of assets more than \$10,000 or greater, such as inheritance, winnings, or similar financial gain Will be reported to the appropriate CPSO immediately, but in no event later than three	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			(3) working days after occurrence. This report must be in writing.				
6.c	Action to legally change one's name;	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Action to legally change one's name will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	n/a	n/a	n/a	n/a
6.d	Change in citizenship;	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Change in citizenship will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	n/a	n/a	n/a	n/a
6.e	The use of any Federally illegal drug (to include the abuse or misuse of any legal drug), and any drug- or alcohol-related treatment;	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. The use of any Federally illegal drug (to include the abuse or misuse of any legal	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			drug), and any drug- or alcohol-related treatment will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.				
6.f	An immediate family member assuming residence in a sensitive country, and	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. An immediate family member assuming residence in a sensitive country will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	n/a	n/a	n/a	n/a
6.g	Hospitalization for mental health reasons.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. Hospitalization for mental health reasons. will be reported to the appropriate CPSO immediately, but in no event later than three (3) working days after occurrence. This report must be in writing.	n/a	n/a	n/a	n/a
7	Marriage/Cohabitant(s). All cleared	In Compliance	Section is addressed in SLAC Plan for	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	individuals (including individuals with a suspended clearance) and applicants must provide a completed DOE F 5631.34, Data Report on Spouse / Cohabitant directly to the CPSO within forty-five (45) calendar days of marriage or cohabitation. Note: A cohabitant is a person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g., a roommate). A cohabitant does not include individuals such as a husband, wife, and children.		<p>Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure all cleared individuals (including individuals with a suspended clearance) and applicants provide a completed DOE F 5631.34, Data Report on Spouse / Cohabitant directly to the CPSO within forty-five (45) calendar days of marriage or cohabitation. Note: A cohabitant is a person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g., a roommate). A cohabitant does not include individuals such as a husband, wife, and children.</p>				
8	Reportable Actions by Others. Covered individuals must alert the appropriate CPSO to the following reportable activities/actions on the part of other covered individuals:	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals alert the appropriate CPSO to the following reportable activities/actions on the part of other covered individuals.</p>	n/a	n/a	n/a	n/a
8.a	An unwillingness to comply with rules	In Compliance	Section is addressed in SLAC Plan for	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	and/or regulations, or to cooperate with security requirements;		<p>Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO an unwillingness to comply with rules and/or regulations, or to cooperate with security requirements on the part of other covered individuals.</p>				
8.b	Unexplained affluence or excessive indebtedness;	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO unexplained affluence or excessive indebtedness on the part of other covered individuals.</p>	n/a	n/a	n/a	n/a
8.c	Alcohol abuse;	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO alcohol abuse on the part of other covered individuals.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
8.d	Illegal use or misuse of drugs or drug activity;	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO illegal use or misuse of drugs or drug activity on the part of other covered individuals.</p>	n/a	n/a	n/a	n/a
8.e	Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified matter or other materials specifically prohibited by law from disclosure;	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program.</p> <p>SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified matter or other materials specifically prohibited by law from disclosure on the part of other covered individuals.</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
8.f	Criminal conduct;	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO criminal conduct on the part of other covered individuals.	n/a	n/a	n/a	n/a
8.g	Any activity that raises doubts as to whether another covered individual's continued national security eligibility for access to classified matter or to hold a national security position is clearly consistent with the interests of national security; or	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO any activity that raises doubts as to whether another covered individual's continued national security eligibility for access to classified matter or to hold a national security position is clearly consistent with the interests of national security on the part of other covered individuals.	n/a	n/a	n/a	n/a
8.h	Misuse of U.S. government property or	In Compliance	Section is addressed in SLAC Plan for	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 4 – Reporting Requirements	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	information systems.		Personnel Security. SLAC will comply per our Personnel Security Program. SLAC will ensure that covered individuals are aware they must report to the appropriate CPSO Misuse of U.S. government property or information systems on the part of other covered individuals.				

Attachment 6 – Personnel Security Quality and Training

This attachment provides information and/or requirements associated with DOE O 472.2 and is applicable to contracts in which the associated CRD (Attachment 1) is included.

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1.	General. Quality and training are both essential to the success of the DOE personnel security program. This Attachment outlines the measures and processes in place to ensure that individuals involved in the personnel security process are trained and qualified to perform their assigned tasks and that personnel security products and services meet or exceed customers' expectations.	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program. SLAC is aware that quality and training are both essential to the success of the DOE personnel security program. This Attachment outlines the measures and processes in place to ensure that individuals involved in the personnel	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
			security process are trained and qualified to perform their assigned tasks and that personnel security products and services meet or exceed customers' expectations.				
2.	<p>Quality.</p> <p>a. Quality measures will be in place to determine:</p> <p>(1) The accuracy and consistency of investigations and adjudicative decisions;</p> <p>(2) Compliance with reciprocity of investigations and adjudicative decisions;</p> <p>(3) Whether the Cognizant Personnel Security Office (CPSO) has sufficient resources to fulfill its function in accordance with this Order;</p> <p>(4) The timeliness of personnel security actions; and</p> <p>(5) Whether individuals are afforded due process during the security clearance determination process.</p> <p>b. CPSOs are responsible for ensuring the quality of the personnel security operations under their purview. Such reviews should include a random sampling of cases and should be accomplished within the framework of DOE O 414.1, Quality Assurance,</p>	In Compliance	<p>Section is addressed in SLAC Plan for Personnel Security.</p> <p>SLAC will comply per our Personnel Security Program</p> <p>SLAC will ensure that:</p> <p>a. Quality measures will be in place to determine:</p> <p>(1) The accuracy and consistency of investigations and adjudicative decisions;</p> <p>(2) Compliance with reciprocity of investigations and adjudicative decisions;</p> <p>(3) Whether the Cognizant Personnel Security Office (CPSO) has sufficient resources to fulfill its function in accordance with this Order;</p> <p>(4) The timeliness of personnel security actions; and</p> <p>(5) Whether individuals are afforded due process during the security clearance determination process.</p> <p>b. CPSOs are responsible for ensuring the quality of the personnel security operations under their purview. Such</p>	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	current version. c. CPSOs are to ensure that adjudicators report quality of background investigations in accordance with Quality Assessment Standards via the Office of the Director of National Intelligence Quality Assessment Reporting Tool.		reviews should include a random sampling of cases and should be accomplished within the framework of DOE O 414.1, Quality Assurance, current version. c. CPSOs are to ensure that adjudicators report quality of background investigations in accordance with Quality Assessment Standards via the Office of the Director of National Intelligence Quality Assessment Reporting Tool.				
3.	Training. Employees must receive personnel security training in accordance with their duties and levels of responsibility to acquire and maintain job proficiency. Training requirements and certification standards will be jointly developed by the Office of Departmental Personnel Security and the National Training Center (NTC). The NTC will maintain the training records. a. Supervisors are responsible for ensuring that subordinate employees performing personnel security duties are trained in accordance with the requirements of this Order as developed by NTC. b. The NTC is responsible for the	In Compliance	Section is addressed in SLAC Plan for Personnel Security. SLAC will comply per our Personnel Security Program SLAC will ensure employees receive personnel security training in accordance with their duties and levels of responsibility to acquire and maintain job proficiency. Training requirements and certification standards will be jointly developed by the Office of Departmental Personnel Security and the National Training Center (NTC). The NTC will maintain the training records. a. Supervisors are responsible for ensuring that subordinate employees performing personnel security duties are	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>development and implementation of training courses and certification processes for the Personnel Security Program in accordance with national and Departmental policy.</p> <p>c. The NTC must ensure that the training modules sufficiently enable trainees to acquire the necessary knowledge and skills to perform their duties effectively.</p> <p>d. Training is required for all adjudicators, adjudicative support staff and other key officials. Adjudicative personnel are prohibited from making security clearance determinations until they have completed the NTC’s Adjudication Fundamentals Course or other nationally approved training and/or have received adequate initial on the job training, as determined by the CPSO.</p> <p>e. Adjudicator Training (specifics regarding sequential course titles and order will be determined by current NTC course guidelines).</p> <p>(1) Initial Training. All newly</p>		<p>trained in accordance with the requirements of this Order as developed by NTC.</p> <p>b. The NTC is responsible for the development and implementation of training courses and certification processes for the Personnel Security Program in accordance with national and Departmental policy.</p> <p>c. The NTC must ensure that the training modules sufficiently enable trainees to acquire the necessary knowledge and skills to perform their duties effectively.</p> <p>d. Training is required for all adjudicators, adjudicative support staff and other key officials. Adjudicative personnel are prohibited from making security clearance determinations until they have completed the NTC’s Adjudication Fundamentals Course or other nationally approved training and/or have received adequate initial on the job training, as determined by the CPSO.</p> <p>e. Adjudicator Training (specifics regarding sequential course titles and order will be determined by current NTC course guidelines).</p>				

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>appointed personnel security specialists performing adjudicative duties have one year to complete the NTC Adjudication Fundamentals Course.</p> <p>(2) Adjudicative Support Training. Employees who are involved in the initial screening of cases, but do not conduct consultations or perform second or third tier reviews (e.g., security assistants, screeners) need a basic understanding of the DOE personnel security process to perform their duties effectively. All personnel performing adjudicative support functions have one year from their date of appointment to adjudicative duties to complete NTC's Adjudication Fundamentals Course.</p> <p>(3) Adjudicators from other Federal Agencies. Adjudicators who are appropriately trained in accordance with the National Security Adjudicator Training Program will not have to complete NTC's Adjudication Fundamentals Course, as determined by the CPSO. The determination of the CPSO will be annotated with the NTC and a copy sent to the Office of</p>		<p>(1) Initial Training. All newly appointed personnel security specialists performing adjudicative duties have one year to complete the NTC Adjudication Fundamentals Course.</p> <p>(2) Adjudicative Support Training. Employees who are involved in the initial screening of cases, but do not conduct consultations or perform second or third tier reviews (e.g., security assistants, screeners) need a basic understanding of the DOE personnel security process to perform their duties effectively. All personnel performing adjudicative support functions have one year from their date of appointment to adjudicative duties to complete NTC's Adjudication Fundamentals Course.</p> <p>(3) Adjudicators from other Federal Agencies. Adjudicators who are appropriately trained in accordance with the National Security Adjudicator Training Program will not have to complete NTC's Adjudication Fundamentals Course, as determined by the CPSO. The determination of the CPSO will be annotated with the NTC and a copy sent to the Office of Departmental Personnel Security.</p>				

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

§	Requirement from Attachment 6 – Personnel Security Quality and Training	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	<p>Departmental Personnel Security.</p> <p>f. Key Officials. Other employees involved in the personnel security process who have no or limited personnel security program experience require a basic understanding of the policies and procedures related to their responsibilities. These key personnel are defined as managers, deputy managers, hearing officers and hearing counsel involved with administrative review hearings conducted under 10 CFR 710, as well as DOE-sponsored consultant psychologists/ psychiatrists and appeal panel members, but may also include human resource managers, Human Reliability Program certifying officials and other managers who are less directly involved in the personnel security process. The NTC-developed and computer-based Personnel Security Awareness Briefing (or successor course/training tool) meets this briefing requirement.</p>		<p>f. Key Officials. Other employees involved in the personnel security process who have no or limited personnel security program experience require a basic understanding of the policies and procedures related to their responsibilities. These key personnel are defined as managers, deputy managers, hearing officers and hearing counsel involved with administrative review hearings conducted under 10 CFR 710, as well as DOE-sponsored consultant psychologists/ psychiatrists and appeal panel members, but may also include human resource managers, Human Reliability Program certifying officials and other managers who are less directly involved in the personnel security process. The NTC-developed and computer-based Personnel Security Awareness Briefing (or successor course/training tool) meets this briefing requirement.</p>				

*Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

Attachment 7 – References

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

A List of references for this order can be found in attachment 7 of [DOE O 472.2A Personnel Security](#)

Attachment 8 – Definitions

[This attachment provides information and/or requirements associated with DOE O 472.2A and is applicable to contracts in which the associated CRD (Attachment 1) is included.]

1. **Access Authorizations.** An administrative determination under the Atomic Energy Act of 1954, Executive Order 12968, or 10 CFR part 710 that an individual is eligible for access to classified matter or is eligible for access to, or control over, special nuclear material.
2. **Active National Security Eligibility.** An individual who is currently cleared by another federal agency with the completion of an adjudicated background investigation and subsequently has access to classified information.
3. **Agency.** Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.
4. **Authorized Adjudicative Agency.** An agency authorized by law, executive order, or designation by the Security Executive Agent (SecEA) to determine eligibility for access to classified information in accordance with Executive Order (EO)12968, as amended, or eligibility to hold a sensitive position.
5. **Authorized Investigative Agency.** An agency authorized by law, EO, or designation by the SecEA to conduct a background investigation of individuals who are proposed for access to classified information or eligibility to hold a sensitive position or to ascertain whether such individuals continue to satisfy the criteria for retaining access to such information or eligibility to hold such positions.
6. **Classified National Security Information or Classified Information.** Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.
7. **Cognizant Personnel Security Office (CPSO).** A DOE personnel security office that is authorized to submit investigative requests to investigative service providers and to adjudicate security clearances.

**Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)*



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022

Site Compliance Plan (5/09/2023)

8. **Consultation (formerly, Personnel Security Interview).** A follow-up with the individual to obtain relevant information to resolve an issue(s) related to granting or continuing their eligibility for a security clearance.
9. **Continuous Evaluation.** Reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.
10. **Contractor.** An expert or consultant (not appointed under section 3109 of title 5, U.S.C.) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).
11. **Controlled Substance.** A drug or other substance, or their immediate precursors, included in schedule I, II, III, IV, or V of part B of 21 USC 802. This does not include distilled spirits, wine, malt beverages, or tobacco, as defined or used in subtitle E of the Internal Revenue Code of 1986.
12. **Covered Individual.**
 - a. A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive position; but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. 105 or 107, the Vice President, or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. 106 or annual legislative branch appropriations acts.
 - b. A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in EO 13549, who has been granted access to classified information, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law.
 - c. A person working in or for the legislative or judicial branches who has been granted access to classified information and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.
 - d. Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.
13. **Departmental Element.** A first-tier organization at Headquarters and in the field. First-tier at Headquarters encompasses heads of the major Headquarters line programs, e.g., Program Secretarial Officers. First-level field element refers to first-level organizations located outside the Washington Metropolitan area and encompasses Operations Offices, Site Offices, Field Offices, and Regional Offices.
14. **Director.** Director, Office of Departmental Personnel Security.

**Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)*



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

15. **Drug Test.** An examination of biologic material to detect the presence of specific drugs and determine prior drug usage, carried out in accordance with procedures, protocols and standards established at Title 10, Code of Federal Regulations, Part 707, Workplace Substance Abuse Programs at DOE Sites, or DOE O 343.1, Federal Substance Abuse Testing Program, current version, and other applicable DOE policies.
16. **Dual Citizen.** An individual who is a citizen of more than one country.
17. **Federal Head of Departmental Element.** The senior Federal official with cognizance over a Departmental Element, as identified in the most current edition of the Department's Executive Secretariat Style Guide.
18. **Federal Site Manager.** The senior Federal management official at any DOE facility.
19. **Foreign Intelligence Entity.** Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.
20. **Foreign National.** Any person who is not a U.S. citizen.
21. **Investigative Service Provider (ISP).** A federal agency authorized to conduct investigations utilizing federal staff and/or contractor personnel.
22. **Key Management Personnel.** An entity's senior management official (SMO), facility security officer (FSO), Insider Threat Program Senior Official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.
23. **Media.** Any person, organization, or entity, other than Federal, state, local, tribal, and territorial governments who are:
 - a. Primarily engaged in the collection, production, or dissemination of information in any form, which includes print, broadcast, film, and Internet to the public; or
 - b. Otherwise engaged in the collection, production, or dissemination of information to the public in any form related to topics of national security, which includes print, broadcast, film, and Internet.
24. **National Security.** Those activities directly concerned with the foreign relations of the U.S. or protection of the nation from internal subversion, foreign aggression, or terrorism.
25. **National Security Eligibility.** Eligibility (after background investigation was completed and adjudicated) for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information.

**Deliverables: Data delivered to DOE or other external agency (e.g., recurring reporting, external database entries)*



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

26. **Need-to-Know.** A determination made by a possessor of classified information or SNM that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the classified information or SNM to perform tasks or services essential to the fulfillment of an official U.S. Government program.
27. **Non-U.S. Citizen.** A person without U.S. citizenship or nationality (may include a stateless person). This term is synonymous with “alien” as defined in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)).
28. **Program Secretarial Officer.** The Federal head of a major DOE Headquarters line program, as identified in the most current edition of the Department's Executive Secretariat Style Guide.
29. **Reasonably Exhaustive Efforts.** The appropriate level of effort to resolve issues or corroborate discrepant information. This may include multiple attempts or techniques to satisfy the issue, attempts to corroborate the activity through references from the background investigation, and/or attempts to obtain and pursue additional leads through other aspects of the investigation.
30. **Security Clearance.** An administrative determination that an individual is eligible for access to classified matter and/or SNM. DOE grants Q and L clearances to individuals who require access to RD information at a classification level equal to or less than their security clearance level. DOE also grants Top Secret, Secret, or Confidential clearances to individuals approved for access to National Security Information or Formerly Restricted Data at classification levels equal to or less than their security clearance level.
31. **Sensitive Position.** Any position within or in support of an agency in which the occupant could bring about, by virtue of the nature of the position, a material adverse effect on national security regardless of whether the occupant has access to classified information and regardless of whether the occupant is an employee, military service member, or contractor.
32. **Unauthorized Disclosure.** A communication or physical transfer of classified information to include Special Nuclear Material to an unauthorized recipient.

(end CRD)



STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
 Operated by Stanford University for the U.S. Department of Energy



DOE O 472.2A, Personnel Security 6/10/2022
Site Compliance Plan (5/09/2023)

Name	Title	Signature and Date
Simon Ovrachim	Security Program Manager, SLAC	<i>Simon Ovrachim</i> 5-11-2023
John Connolly	Deputy Director for Operations, SLAC	<i>John Connolly</i> 5/15/2023
Thomas V. Rizzi	Division Director of Operations, DOE-SSO	
Hanley Lee	Head of Field Element, DOE-SSO	

Please return signed document to Burtnett@SLAC.Stanford.edu

Revision History

Revision	Revision Date	Summary of Change(s)
R0	5/09/2023	Original release.