STANFORD UNIVERSITY

SLAC National Accelerator Laboratory

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

DOE Order 470.5 – Insider Threat Program (Jun 2, 2014)

Site Compliance Plan (2/11/2021)

Contents

Introduction 1
Attachment 1 – Contractor Requirements Document 1
Approvals 5
Revision History 5

Introduction

This Site Compliance Plan (SCP):

a) corresponds with the version of the DOE Order on Insider Threat Program 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).

Attachment 1 – Contractor Requirements Document

Regardless of the performer of the work, the contractors must comply with the requirements of this contractor requirement document and with National Nuclear Security Administration (NNSA) and other Department of Energy (DOE) program office direction approved by the DOE Insider Threat Program executive Steering Committee and provided through contract. Each contractor is responsible for disseminating the requirements and NNSA or other DOE program office direction to subcontractors at any tier to the extent necessary to ensure the contractor's and subcontractor's compliance with the requirements.

Contractors must provide data, information, systems, and any other support to the DOE Insider Threat Program in accordance with applicable laws, regulations, policies, directives and other requirements as directed through contract by the NNSA or other DOE program office(s).

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

DOE Order 470.5 – Insider Threat Program (Jun 2, 2014)

Site Compliance Plan (2/11/2021)

A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. & 2282b) The procedure for the assessment of civil penalties are set forth in 10 CFR Part 824, Procedural Rules of the Assessment of Civil Penalties for Classified Information Security Violations.

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., BASO)
4	REQUIREMENTS						
4.a	An Insider Threat Program (ITP) must be developed and maintained to deter, detect, mitigate, analyze and respond to insider threats.	6/31/201	SLAC will develop an insider threat program.	N/A	N/A	N/A	N/A
4.b	The ITP must:						
4.b.1	Fulfill and maintain consistency with the National Insider Threat Policy and Minimum Standard for Executive Branch Insider Threat Programs;	In progress 6/31/2021	SLAC has a working group, consisting of HR, Security, COO Office, evaluates all issues/threats. In addition, SLAC can request a threat assessment from the Stanford University Threat Assessment team. The DOE Site Office and CI are briefed on all related issues.	N/A	N/A	N/A	N/A
4.b.2	Identify insider threat and take appropriate actions to deter them from causing damage to DOE personnel, resources, capabilities and national security, commensurate with the potential consequences of the insider threats access, intent and ability;	In progress 6/31/2021	See 4.b.1	N/A	N/A	N/A	N/A
4.b.3	Ensure legal, civil and privacy rights and civil liberties are preserved and protected;	In progress 6/31/2021	See 4.b.1	N/A	N/A	N/A	N/A
4.b.4	Integrate inside threat related policies, procedures and resources across DOE, that include counterintelligence, security, human capital, legal counsel, information management and other DOE elements that can contribute to deterring, identifying and managing insider	In progress 6/31/2021	See 4.b.1	N/A	N/A	N/A	N/A

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

DOE Order 470.5 – Insider Threat Program (Jun 2, 2014)

Site Compliance Plan (2/11/2021)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., BASO)
	threats;						
4.b.5	Identify, collet and process data required to identify and address insider threats;	In progress 6/31/2021	See 4.b.1	N/A	N/A	N/A	N/A
4.b.6	Coordinate insider threat analysis, response and mitigation actions with appropriate law enforcement agencies, DOE intelligence, security, legal counsel, inspector general, human capital and other cognizant organizations;	In progress 6/31/2021	Same as above	N/A	N/A	N/A	N/A
4.b.7	Establish, maintain and conduct training or awareness activities to ensure all cleared federal and contactor employees are informed of their responsibilities and provided required information related to the ITP; and	In progress 6/31/2021	SLAC covers all safety, security training or awareness in ES&H training and SLAC conducts a safety training for all employees on site.	N/A	N/A	N/A	N/A
4.b.8	Monitor user activity on classified networks.	N/A	SLAC does not have a classified network.	N/A	N/A	N/A	N/A
4.c	DOE sites, facilities, programs and personnel must provide or provide access to data as required for ITP to successfully execute its mission.	N/A	SLAC has a working group, consisting of HR, Security, COO Office, evaluates all issues/threats. In addition, SLAC can request a threat assessment from the Stanford University Threat Assessment team. The DOE Site Office and CI are briefed on all related issues.	N/A	N/A	N/A	N/A
4.d	DOE programs must identify the resources to support the ITP and provide this information to the ITP Working Group (ITPWG)	N/A	See.4.c.	N/A	N/A	N/A	N/A
4.e	Annual progress/status reports must be prepared for the Secretary of Energy through the ITPWG and the Senior Information Sharing and Safeguarding Steering Committee (SISSSC) established by E.O. 13587 to document and report the progress/status of the	N/A	See.4.c.	N/A	N/A	N/A	N/A

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

DOE Order 470.5 – Insider Threat Program (Jun 2, 2014)

Site Compliance Plan (2/11/2021)

§	Requirement from Attachment 1 – CRD	Compliance Status	Method of Compliance	Deliverables*			
				Item	Frequency	Due Date(s)	Recipient (e.g., BASO)
	ITP.						
4.f	DOE Information system usage banners, policies and user agreements must be approved according to Designated Senior Official (DSO) direction and in consultation with the Office of General Counsel.	N/A	SLAC does not use DOE Information system usage banners.	N/A	N/A	N/A	N/A
4.g	Senior Counterintelligence Officers must ensure that Local Insider Threat Working Groups (LITWG) are established.	N/A	SLAC complies through the O 475.1 SCP.	N/A	N/A	N/A	N/A
4.h	Documentation pursuant to the ITP must be reviewed for classified and controlled unclassified information and handled accordingly	In compliance	SLAC complies through the O 475.1 SCP.	N/A	N/A	N/A	N/A
4.i	DSO-approved inside threat detection, assessment and referral criteria and procedures must be documented.	N/A	SLAC has a working group, consisting of HR, Security, COO Office, evaluates all issues/threats. In addition, SLAC can request a threat assessment from the Stanford University Threat Assessment team. The DOE Site Office and CI are briefed on all related issues.	N/A	N/A	N/A	N/A
4.j	Data sources and format(S) needed to support the centralized analytic operations must be documented.	N/A	SLAC has a working group, consisting of HR, Security, COO Office, evaluates all issues/threats. In addition, SLAC can request a threat assessment from the Stanford University Threat Assessment team. The DOE Site Office and CI are briefed on all related issues.	N/A	N/A	N/A	N/A

(end CRD)

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

DOE Order 470.5 – Insider Threat Program (Jun 2, 2014)

Site Compliance Plan (2/11/2021)

Approvals

Name	Title	Signature	Date
Brian Sherin	Deputy Director for Operations, SLAC		2/12 /2021
Thomas V. Rizzi	Division Director of Operations, BASO	Thomas V. Rizzi	02/16/2021
Paul Golan	Head of Field Element, BASO		2/18/2021

Please return signed document to Contract Management.

Revision History

Revision	Revision Date	Summary of Change(s)
R0	2/11/2021	Original release.