[DOE Order 475.1, Counterintelligence Program (12/10/2004)](#)
Site Compliance Plan, (Rev 0, 2/06/2017)

Contents

Introduction

This Site Compliance Plan (SCP):

a) corresponds with the version of the DOE Order on Counterintelligence Program listed in the Prime Contract,

b) states how the Laboratory complies with applicable requirements as tailored to the risks at the Laboratory,

c) identifies CRD sections that do not apply, and

d) documents DOE-approved methods of compliance for applicable requirements and that there are no recurring deliverables*.

Impact on the Contract:

Under the SCP, sections of the CRD are incorporated into the Contract as-is, unless the SCP indicates that a section or portion thereof is inapplicable, or the section has been changed. Thus, for example, if "in compliance" is listed next to a CRD section, that section is incorporated into the Contract as-is. However, where an SCP indicates that a section or portion thereof is inapplicable, the section or portion thereof is excluded from the Contract. In addition, where a section or portion thereof is applicable, but changes to the section have been agreed by the Parties, the section, as modified by the Parties, shall be incorporated into the Contract. The SCP also memorializes the Parties' agreement on how SLAC will comply with sections of the CRD (whether or not modified).

Attachment 2 - Contractor Requirements Document (CRD)

1. Background.

The Director of the DOE Office of Counterintelligence (OCI) or the Chief of the NNSA Office of Defense Nuclear Counterintelligence (ODNCI) consults with appropriate DOE field site/facility management within their respective jurisdictions to establish local CI offices with full-time Federal and contractor CI personnel who implement the CI Program.[1] In addition, determinations are made concerning each local CI office as to whether it will act as a servicing CI office for facilities that do not have local CI offices. A CI office may service more than one

---

[1] In fiscal year 2007 legislation, Congress consolidated the DOE Office of Counterintelligence (OCI) and the NNSA Office of Defense Nuclear Counterintelligence (ODNCI). Counterintelligence responsibilities for the DOE and NNSA are now overseen by the DOE Office of Intelligence and Counterintelligence."

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

field office or site. The OCI Director/ODNCI Chief, to support CI Program requirements, may change the scope of responsibility for each local CI office. For managing and operating contractors, when it is determined that no local CI office is required, a servicing CI office for that contract will be designated and the contractor will be required to support the requirements of the site-specific CI plan developed for that contract in coordination with the servicing CI office and the OCI Director or the ODNCI Chief, as appropriate. At facilities not requiring a local CI office, a servicing CI office will be designated. For facilities supported by a servicing CI office an individual at the serviced site will be designated by site/facility management as the on-site contractor CI Representative. This selection should be coordinated with the servicing CI office Federal or contractor SCIO and the OCI Director or the ODNCI Chief as appropriate. All contractor CI personnel are required to work in close cooperation with field and Headquarters Federal CI personnel. The contractor must ensure that the senior CI officer (SCIO) reports directly to both site/facility senior management and either the OCI Director or the ODNCI Chief. The contractor CI Representative reports to the SCIO for CI matters only.

2. Program Dimensions.

Contractor CI Programs will be evaluated in accordance with performance assessments covering, but not limited to, the following program dimensions and functional activities:

a. quality, quantity, and timeliness of investigations, including actions recommended in accordance with such overriding requirements as referrals to the Federal Bureau of Investigation (FBI) [see Title 50 United States Code (U.S.C.) 402a];

b. quality and effectiveness of the CI program management process (planning, organizing, directing/executing, budgeting, coordinating, communicating, evaluating, and quality assurance activities conducted in relation to CI resources, personnel, and operations);

c. quality and effectiveness of program components such as unclassified foreign visits and assignments (UFVA), CI awareness/briefing and debriefing/reporting, investigations, information and special technologies, CI analysis, information management, financial management, liaison, training, CI Evaluations Program support, and administration of unique and/or high-risk personnel;

d. compatibility of performance results with OCI/ODNCI policies, procedures, program directives, strategic planning, and other administrative requirements;

e. quality of data gathered, evaluated, recorded, and reported through CI briefings and debriefings of those individuals having professional, substantive personal, enduring, or financial contact with sensitive country foreign nationals;

f. ability of the program to define and counter any CI risks and concerns incurred as a result of DOE activities, especially those that involve interaction with foreign nationals for official and unofficial reasons;

g. quality, accuracy, and timeliness of CI work products submitted in response to requirements, assignments, and/or requests for support issued by the OCI Director/ODNCI Chief;

h. quality of the local CI program's liaison and interaction with local FBI, United States intelligence community (USIC), and law enforcement personnel; and

i. measures taken to identify and resolve matters of CI concern, and promote proactive interaction, communications, and liaison with the site/facility manager, contract manager, and/or other operational elements (e.g., security, personnel administrators, export control, technology transfer, classified and unclassified computer security, foreign travel, and foreign visits and assignments).
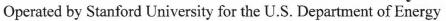
3. Contractor Requirements

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
-	Regardless of the performer of the work, the contractor is responsible for compliance with the requirements of this Contractor Requirements	In compliance	SLAC flows the requirements of this SCP to all subcontractors whose subcontract involves SLAC's provision of information or performance of work involving issues of national security.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)

DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	Document (CRD). The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor will not unnecessarily or imprudently flow down requirements to subcontracts. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD to the extent necessary to ensure the contractor's compliance and only incur costs that would be incurred by a prudent person in the conduct of competitive business.		SLAC's onsite subcontractors are made aware of their responsibility to operate in compliance with the UFVA program at SLAC.				
3.a.	Contractors and subcontractors under their purview must support, adhere to, and implement all DOE CI Program requirements at their sites.	In compliance	SLAC has determined that the SLAC Site Security Plan (SSP) satisfies all applicable DOE CI Program requirements. In addition, SLAC cooperates with and coordinates all CI activities through the Livermore CI Office.	n/a	n/a	n/a	n/a
3.b.	The contractor must ensure implementation of the following DOE CI Program requirements.	In compliance	Outlined in sections below.	n/a	n/a	n/a	n/a
3.b(1)	Support the local assigned servicing CI office in the development and implementation of site/facility specific CI support plans in accordance with paragraph 3c(2) of this CRD.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(2)	At sites where a local CI office is co-located, implement the CI Program directly through the local office.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(3)	At sites that use a servicing CI office at another location, contractors will coordinate implementation with the assigned servicing CI office.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(4)	Site/facility management contractors at sites assigned to act as servicing CI offices for other contractor facilities	n/a	Not applicable to SLAC; SLAC is not a servicing CI office for other contractor facilities.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
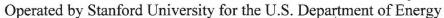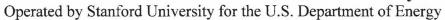
SLAC National Accelerator Laboratory

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

DOE Order 475.1, Counterintelligence Program (12/10/2004)

Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	will be responsible for developing site-specific CI support plans and overall CI Program implementation through the Federal or contractor servicing SCIO in coordination with those assigned sites and the OCI Director/ODNCI Chief.						
3.b(5)	Support the Director and or Chief in identifying and selecting individuals to serve as contractor SCIOs or CI Representatives.	In compliance	SLAC has a designated CI Representative. See 3.a.	n/a	n/a	n/a	n/a
3.b(6)	Maintain effective coordination with the OCI Director and the ODNCI Chief on matters of CI interest.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(7)	Provide the Federal or contractor SCIO, local or servicing CI office personnel, and the contractor CI Representative with direct access to senior management.	In compliance	SLAC's CI Representative is a Senior Manager. SLAC cooperates with and coordinates all CI activates through the Livermore CI Office.	n/a	n/a	n/a	n/a
3.b(8)	Ensure that the local or servicing CI office has appropriate access to all records, facilities, operational activities, security information, IT systems, and databases necessary to perform its official duties.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(9)	Coordinate with the OCI Director and the ODNCI Chief to ensure the implementation of CI plans for each DOE special access program (SAP) and SAP CI threat assessments.	n/a	Not applicable; SLAC does not have any SAPs. If SLAC anticipates having an SAP in the future, it will revisit this requirement.	n/a	n/a	n/a	n/a
3.b(10)	Provide support and assistance for CI eligibility evaluations and CI scope polygraphs for designated DOE high-risk personnel pursuant to current statutes and the regulatory requirements [Title 10 Code of Federal Regulations (CFR) Part 709, Polygraph Examination Regulations].	n/a	Not applicable; SLAC does not have any SAPs or high-risk personnel. If SLAC anticipates having an SAP or high-risk personnel in the future, it will revisit this requirement.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
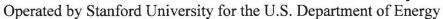
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
3.b(11)	Ensure that the implementation of an effective CI awareness program for contractor employees includes the following. (a) Initial, comprehensive briefings on CI. Briefing topics include but are not limited to overview of the foreign intelligence collection and international terrorist threat, espionage indicators, and reporting requirements. (b) Annual refresher briefing. Refresher briefings should reinforce and update awareness of CI issues and their responsibilities, regardless of whether the employee holds clearances or not. (c) Additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans. NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.	In compliance	See 3.a. In addition, annually, the DOE Servicing CI Officer from Livermore Office conducts a briefing to the Laboratory. SLAC distributes CI orientation information during the new hire onboarding process.	n/a	n/a	n/a	n/a
3.b(12)	Institute and maintain a process for coordinating adverse personnel actions with the responsible local or servicing CI office (including such actions as disciplinary suspensions, terminations, involuntary separations, and revocations/ reinstatements of access authorizations/security clearances).	In compliance	SLAC interprets this requirement to mean it shall coordinate such actions with the servicing CI Office (LLNL) only when they involve persons with security clearances or relate to national security interests, including issues related to assignees from Sensitive Countries or State Sponsors of Terrorism.	n/a	n/a	n/a	n/a
3.b(13)	Ensure that CI resources are used to protect and preserve classified and/or sensitive programs and operations.	n/a	Not applicable to SLAC: SLAC does not possess any classified information and there are no sensitive programs or operations.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
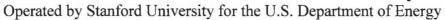
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
3.b(14)	Maintain accountability to both the Secretary and the Administrator for the performance of CI program functions and requirements at their locations.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(15)	Provide timely and thorough support to Headquarters CI Program Directors, CI taskings, and requests for information.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(16)	Support the CI role in assessing risks associated with sensitive country foreign visits and assignments and or when sensitive subjects will be discussed or security areas will be used at DOE facilities by— (a) supporting the effective implementation of the local UFVA program, (b) providing recommendations for approval/disapproval of specific visits, (c) supporting the conduct of indices checks by the CI Program, and (d) supporting the conduct of briefings and debriefings by the CI Program.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(17)	Ensure that all contractor employees are aware of the requirement to report the following to the local or servicing CI office.	See below	Outlined in sections below.	n/a	n/a	n/a	n/a
3.b(17)	(a) Official foreign travel to sensitive countries regardless of whether the traveler possesses a security clearance.	In Compliance	SLAC coordinates with the DOE Servicing CI Officer on all travel to sensitive and State Sponsors of Terrorism countries.	n/a	n/a	n/a	n/a
3.b(17)	(b) Travel to any country where they intend to have or have had discussions with sensitive	In Compliance	SLAC does not have any information pertaining to sensitive subjects, however, SLAC coordinates with the DOE Servicing CI Officer to provide	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
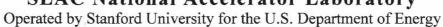
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2		Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
					Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
		country foreign nationals regarding sensitive subjects. This would include travel which they know in advance will involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.		training on these issues in briefings with employees who have or have had clearances.				
3.b(17)	(c)	All travel to any country when areas determined to be sensitive subjects will be discussed.	In Compliance	SLAC does not have any information pertaining to sensitive subjects, however, SLAC coordinates with the DOE Servicing CI Officer to provide training on these issues in briefings with employees who have or have had clearances.	n/a	n/a	n/a	n/a
3.b(17)	(d)	Any substantive professional, personal, or enduring financial relationship [one that has existed, or is expected to exist, for a substantial period of time (months or years)] with foreign nationals affiliated with sensitive countries.	In compliance with approved changes	SLAC coordinates with the DOE Servicing CI Officer to only train employees with active clearances issued by DOE to report such information to the DOE Service CI Officer.	n/a	n/a	n/a	n/a
3.b(17)	(e)	Any contacts with foreign nationals who make requests that could be attempts at exploitation or elicitation. Examples are— 1 requests for documents or information that is viewed by the traveler as unexpected or unrelated to the purpose of the interaction; 2 requests for the traveler to transport back to the U.S. any package(s) or letter(s) for mailing in the U.S.; 3 requests of any kind that cause the traveler to feel uncomfortable or call into	In compliance	See 3.b(11)	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	question the purpose of the request; 4 professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad; and 5 any foreign travel for which foreign monetary support is provided, whether to a sensitive or a non-sensitive country.						
3.b(17)	(f) Requests for unauthorized access to classified or otherwise sensitive information.	In compliance	SLAC does not possess Classified or sensitive information. Nonetheless, to the extent SLAC becomes aware of unauthorized attempts to gain access to classified or otherwise sensitive information, SLAC will report such attempts. In addition, SLAC trains those personnel with clearances or those that possess national security information to report all requests for unauthorized access to classified or otherwise sensitive information.	n/a	n/a	n/a	n/a
3.b(18)	At the discretion of the local or servicing CI office, support the briefing and debriefing of contractor employees when warranted to support the CI Program, including contractor employees who are— (a) traveling to sensitive foreign countries when required regardless of whether they hold a security clearance or (b) hosting sensitive and non-sensitive country foreign visitors and assignees that are going to be given access to sensitive subjects or sites. NOTE: Other circumstances may arise which could warrant the briefing and debriefing of certain employees to support the CI Program.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(19)	Support the proactive integration and use of information security and intrusion detection resources and	In compliance	SLAC's IT infrastructure incorporates information security and intrusion detection and reports breaches as appropriate	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	capabilities to protect the DOE information architecture and detect and deter technical attacks and intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements.						
3.b(20)	Support analyses of the threats posed by foreign intelligence services and international terrorist activities for CI purposes and provide threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.b(21)	Support the conduct of investigations and inquiries about incidents of CI concern.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.	The contractor must ensure that the assigned SCIO performs the following functions at the local site and for assigned sites which they service. For sites not assigned a local SCIO, the assigned servicing CI office SCIO will be responsible for performing these same functions in coordination with the local contractor site contractor CI Representative.	n/a	Does not apply to SLAC; SLAC does not have its own SCIO.	n/a	n/a	n/a	n/a
3.c.(1)	Implement CI Program policies, standards, and guidelines pursuant to legal and regulatory mandates, provisions of this Order, and other relevant DOE CI directives and requirements.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(2)	Ensure the development of a site-specific CI support plan for each site/facility for which the local/servicing CI office is responsible. These plans are to be developed in coordination with OCI/ODNCI, as appropriate. Site	In compliance	See 3.a. and 3(b)(11).	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
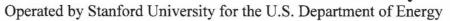
STANFORD UNIVERSITY
SLAC National Accelerator Laboratory
Operated by Stanford University for the U.S. Department of Energy

DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

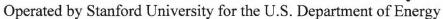| CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	specific CI support plans should address the following areas at a minimum. (a) Threat Analysis. Conduct site-based counterintelligence threat assessments based on a variety of sources, including foreign intelligence and international terrorist information. Conduct ongoing analysis of the threat to support prioritization of local and national CI Program activities. (b) Information Technology. Develop specific actions to be taken to counter the threat to information systems posed by foreign intelligence collection and international terrorist activities. (c) Awareness. Ensure site personnel are aware of their responsibilities to support the CI Program. (d) Briefing and Debriefing. Brief and debrief specific personnel whose activities require foreign travel, hosting foreign visitors or assignees, working in high risk positions or special access programs or who otherwise need focused CI program support. (e) Investigations and Inquiries. Conduct investigations and inquiries on matters of CI concern. (f) Liaison. Conduct liaison with local law enforcement and the USIC in support of the site CI Program.						

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)

DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	(g) UFVA support. Coordinate the UFVA matters. (h) Security support. Coordinate with security on matters related to the site CI Program. (i) Support to the CI Evaluation Program. Conduct activities in support of CI evaluations of high risk personnel as required by law and DOE regulations (10 CFR 709). (j) Foreign Travel. Coordinate on foreign travel matters in support of the site CI Program. (k) Training. Address training needs of the CI staff, CI Representatives, and site staff on CI issues, as appropriate.						
3.c.(3)	Serve as the primary CI advisor and provide CI support to DOE site/facility management in accordance with established local/servicing CI office areas of responsibility while maintaining concurrent accountability to the OCI Director/ODNCI Chief for fulfilling CI Program requirements.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(4)	Immediately forward to the OCI Director/ODNCI Chief for referral by the OCI Director to the FBI, any information, regardless of origin, which indicates that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power (see 50 U.S.C. 402a).	In compliance	SLAC does not possess or maintain classified information, but does cooperate with and coordinates all CI activates through the Livermore CI Office. To the extent SLAC becomes aware of unauthorized attempts to gain access to classified information, SLAC will report such attempts.	n/a	n/a	n/a	n/a
3.c.(5)	Establish and/or maintain an approved records management system to support the local/servicing CI office,	In compliance	See 3.a.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
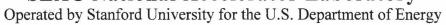
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	in coordination with the OCI Director/ODNCI Chief.						
3.c.(6)	Notify OCI/ODNCI of all incidents of CI concern involving suspected or identified hostile foreign intelligence or international terrorism activities and suspected or identified technical penetrations affecting persons or facilities under their jurisdiction and document these in appropriate CI information systems, as applicable.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(7)	Implement a CI briefing/debriefing program for contractor personnel who travel to a sensitive country or interact or have contact with foreign nationals, pursuant to CI Program policy and under the direction of the OCI Director/Chief ODNCI.	In compliance	See 3.b.(11).	n/a	n/a	n/a	n/a
3.c.(8)	Conduct analyses to assess the threats posed by foreign intelligence services and international terrorist activities to sites/facilities for CI purposes and provide relevant threat information to CI investigative, training and awareness, and Information and Special Technology Program (ISTP) personnel and outside offices such as those involved in foreign visits and assignments and other national security–related duties.	In compliance	SLAC's Serving CI Rep performs this function.	n/a	n/a	n/a	n/a
3.c.(9)	Ensure the proactive integration and use of information security and intrusion detection capabilities to protect the DOE information architecture and to detect and deter technical attacks and intelligence gathering activities directed against DOE by foreign intelligence and international terrorist elements.	In compliance	See 3.a.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
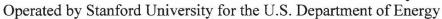
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
3.c.(10)	Ensure entry of all CI-relevant data into existing CI-Net applications, (or successor systems), including the results of investigations, debriefings, analysis, cyber, liaison, incident reports, and other lead information supplied by the DOE CI community.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(11)	Conduct liaison with site counterparts (including security, intelligence, export control, technology transfer, technical surveillance countermeasures, operations security, and nonproliferation personnel) on national security matters.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(12)	Conduct liaison with appropriate local, state, and Federal intelligence and law enforcement agencies, as appropriate, concerning CI/ counterterrorism matters and maintain a complete record of these interactions.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(13)	Execute OCI/ODNCI mission and related strategic plan requirements to deter, detect, and prevent foreign powers and other unauthorized personnel from compromising DOE assets (e.g., information or classified and unclassified computers).	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(14)	Support Headquarters OCI/ODNCI, including Program Directors, requests for information and assistance for other CI activities as required and deemed appropriate by the OCI Director or the ODNCI Chief.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(15)	Support and assist the CI Evaluation Program covering designated DOE high risk personnel, as required (10 CFR Part 709).	In compliance	See 3.a.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)
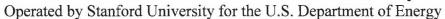
DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
3.c.(16)	Ensure the implementation of an effective CI awareness program for contractor employees that includes the following. (a) Initial briefings on CI. Briefing topics include but are not limited to overview of the foreign intelligence collection and international terrorist threat, espionage indicators, and reporting requirements. (b) Annual refresher briefings. Refresher briefings should reinforce and update awareness of CI issues and employees' responsibilities, regardless of whether they hold clearances or not. (c) Additional awareness briefings and training for specific employee groups as identified in site-specific awareness plans. NOTE: Portions of the awareness program may be coordinated with the security awareness program at the discretion of local site officials.	In compliance	See 3.a. and 3.b.(11).	n/a	n/a	n/a	n/a
3.c.(17)	Ensure that subordinate CI contractor personnel, including CI Representatives, receive the professional training and development necessary to execute their particular duties in support of the overall CI mission and OCI/ODNCI Strategic Plan.	In compliance	SLAC's CI Representative coordinates with the LLNL CI Office to ensure training requirements are met for the CI Representative role.	n/a	n/a	n/a	n/a
3.c.(18)	Ensure coordination with the local supporting security, human resources, or other organizational entity to institute and maintain a process for coordinating adverse personnel actions (including such actions as	In compliance	See 3.b.(12).	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)

DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	disciplinary suspensions, terminations, involuntary separations, and revocations/ reinstatements of access authorizations/security clearances).						
3.c.(19)	Implement local programs to assess CI implications of foreign visitors and assignees and foreign travel.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(20)	Ensure that CI resources are actively used to protect and preserve classified and/or sensitive programs and operations. Focus will be prioritized on programs with subject matter, personnel, or activities believed to be of interest to hostile foreign intelligence or international terrorist entities, where the possible loss of classified or sensitive information and materials imposes substantive national security concerns, and where there is significant interaction with sensitive country foreign nationals.	n/a	See 3.b.(13).	n/a	n/a	n/a	n/a
3.c.(21)	Support the evaluation of sensitive foreign country foreign visits and assignments to DOE facilities, including recommendations for approval/disapproval, the conduct of indices checks, and the conduct of host CI briefings and debriefings.	In compliance with approved changes.	See 3.a.; SLAC has a DOE-approved program for review of visitors or assignees from sensitive foreign countries. See the Site Compliance Plan for DOE O 142.3A in the prime contract.	n/a	n/a	n/a	n/a
3.c.(22)	Require contractor personnel to work in close cooperation with Federal CI personnel.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(23)	Support the UFVA program. (a) Review requests for foreign national access approval, including visits involving information and technologies that are releasable to the public,	In compliance	SLAC has implemented an effective risk-based UFVA program and coordinates and communicates with the Livermore CI office as appropriate.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	and requests for designation of optional areas within property protection areas for CI and Counterterrorism implications. This includes attendance in offsite conferences and other functions when foreign national access approval is required. (b) At the request of the local hosting site, provide CI consultations to the approval authority and his or her designees to evaluate foreign national access in the absence of a required, completed indices check, and document that the consultation was conducted in the Foreign Access Central Tracking System. (c) Conduct briefings and debriefings of foreign visitors' and assignees' hosts/sponsors/escorts and develop and provide CI awareness modules for local UFVA training. (d) Coordinate the external indices check process for local sites. (e) Document foreign interaction at the local site in applicable databases. (f) Support as required the approval process for nationals of state sponsors of terrorism visits in coordination with the OCI Director.						
3.c.(24)	Support the conduct of information technology CI activities to protect the DOE information architecture; to detect and deter technical attacks and	In compliance	SLACs IT infrastructure incorporates information security and intrusion detection and reports breaches as appropriate	n/a	n/a	n/a	n/a

Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (e.g., recurring reporting, external database entries)

DOE Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	intelligence collection directed against DOE by hostile foreign intelligence and international terrorist elements; and to develop and acquire information systems and other technology-based tools for the CI program.						
3.c.(25)	Support analyses of the threat posed by foreign intelligence and international terrorist activities for CI purposes and provide threat information to DOE management to support the protection of DOE personnel, information, facilities, and assets.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(26)	Support investigations and inquiries on incidents of CI concern.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.c.(27)	Develop criteria and establish a process to identify and document site-specific unique access programs, positions and individuals.	In compliance	See 3.a.	n/a	n/a	n/a	n/a
3.d.	Contractor CI Representatives will be appointed by site/facility managers, in coordination with the servicing SCIO and the OCI Director/ODNCI Chief for sites supported by a servicing CI office. For CI purposes only, contractor CI Representatives will report directly to their servicing CI office Federal or contractor SCIO. The contractor CI Representative position is not intended to be a full time responsibility.	In compliance	SLAC has appointed a CI Representative and cooperates with and coordinates all CI activates through the Livermore CI Office.	n/a	n/a	n/a	n/a
3.d.(1)	Contractor CI Representatives will coordinate with the assigned servicing CI office Federal or contractor SCIO and local site management on the implementation of the local CI Program. This will include at a minimum assistance to the servicing	In compliance	See 3.a.	n/a	n/a	n/a	n/a

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/06/2017)

CRD §	Requirements from CRD, Attachment 2	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	CI office for the development of a site-specific CI support plan.						
3.d.(2)	Contractor CI Representatives will support the servicing CI office in the conduct of investigations. NOTE: The CI Representative will not conduct CI investigations independent of the servicing CI office. The servicing CI office will conduct investigations and may request the support of the local contractor CI Representative, as appropriate.	In compliance	See 3.a.	n/a	n/a	n/a	n/a

(end CRD)

*Deliverables: Data delivered to DOE or other external agency as required by the text of the CRD (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 Order 475.1, Counterintelligence Program (12/10/2004)
Site Compliance Plan, (Rev 0, 2/07/2017)

4. Definitions.

a. Counterintelligence (CI)—the information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs.

b. CI Employee—any full-time or part-time Federal or contractor employee who is designated by the OCI Director or the ODNCI Chief as having CI Program responsibilities that require participation in and/or access to sensitive CI matters, databases, and/or records.

c. CI Evaluation—the process, including a CI scope polygraph examination, employed by the Office of Counterintelligence to determine whether DOE Federal and contractor employees, other individuals assigned or detailed to Federal positions at DOE, or applicants for employment will be recommended for initial or continued access to high-risk positions, pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

d. CI Indicator—information that reflects possible foreign intelligence or international terrorist motives/involvement/activity.

e. CI Investigation—administrative fact-finding and information gathering conducted by the DOE Office of Counterintelligence/NNSA Office of Defense Nuclear Counterintelligence to determine whether national security is being threatened and/or damaged by activities perpetrated against DOE personnel, information, activities, facilities, and technologies or systems by or on behalf of foreign powers, organizations or persons, or international terrorist organizations.

f. CI Officer (CIO)—a Federal or contractor employee appointed by the OCI Director/ODNCI Chief to conduct investigative matters and various additional duties in support of the CI Program. CIOs normally report to a senior CIO who is responsible for a specific CI Program field office.

g. CI Polygraph Program—engagement in activities and processes for administering CI scope polygraph examinations pursuant to required statutory provisions and related regulatory requirements embodied in DOE regulations at 10 CFR Part 709.

h. CI Representative—an employee who is formally appointed by local site management to serve in a coordination role with the CI Program. CI Representatives will normally be appointed when there are no on-site CI program personnel and where a servicing CI office covers the facility. The CI Representative acts as the interface between a servicing CI office and the local site to support CI Program implementation at the site.

i. Elicitation— subtle extraction of information during an apparently normal and innocent conversation

j. Emotional Bonds—feelings of affection or emotional attachment in a relationship.

k. Enduring Relationship—one that has existed or is expected to exist for a substantial period of time (months or years).

l. Exploitation—the harmful, merely instrumental utilization or unfair advantage of an individual or his capabilities for one's own gain.

m. Foreign Intelligence—information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons but not including counterintelligence other than information on international terrorist activities.

n. Foreign Interest—any of the following:
(1) a foreign government or foreign government agency;
(2) any form of business enterprise organized under the laws of any country other than the United States or its possessions;
(3) any form of business enterprise organized or incorporated under the laws of the United States or a State or other jurisdiction within the United States that is owned, controlled, or influenced by a foreign government, agency, firm, corporation, or person; or
(4) any person who is not a U.S. citizen.

o. Foreign National—anyone who is not a U.S. citizen by birth or naturalization.

p. Foreign Nexus—specific indications that a DOE employee or contractor employee is or may be engaged in clandestine or unreported relationships with foreign powers, organizations or persons, or international terrorists, contacts with foreign intelligence services; or other hostile activities directed against DOE facilities, property, personnel, programs, or contractors by or on behalf of foreign powers, organizations or persons, or international terrorists.

q. High-Risk—programs, offices, and positions subject to the counterintelligence evaluation and polygraph examination provisions specified in DOE regulations at 10 CFR 709.

r. Insider—anyone with authorized, unescorted access to any part of DOE facilities and programs.

s.   International Terrorism—the unlawful use of force or violence by a group or individual who has some connection to a foreign power or whose activities transcend national boundaries against persons or property, for purposes of intimidating or coercing a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

t.   Local CI Office—the location where the CI Program has established a full-time presence for the conduct of CI Program activities staffed by personnel assigned to the CI program.

u.   National Nuclear Security Administration (NNSA) Facilities—the laboratories and facilities covered by NNSA: Los Alamos, Lawrence Livermore, and Sandia national laboratories; the Kansas City, Pantex, and Y-12 plants; tritium operation facilities at the Savannah River Site; the Nevada Test Site; and any other sites or facilities as designated by the Secretary in consultation with the NNSA Administrator (see P.L. 106-65).

v.   Senior CI Officer (SCIO)—a Federal or contractor employee serving full-time in support of the CI program and responsible for the management of a specific CI program field office located within a specific facility or housed in a location that services a number of facilities. SCIOs are appointed by the OCI Director or the ODNCI Chief directly or in consultation with local management.

w.   Servicing CI Office—local DOE CI offices staffed with full-time personnel and assigned responsibility for providing CI services to additional designated DOE facilities including those without full-time personnel and ensuring that all Departmental activities receive necessary CI services.

x.   Substantive Relationship—one that is enduring and involves substantive sharing of personal information and/or the formation of emotional bonds.

y.   Substantive Sharing (of personal information)—discussion of private information about oneself that one would not routinely share with strangers.

Approvals

Name	Title		Date
Steven L. Porter	Legal Counsel, SLAC		2/7/2017
Thomas Rizzi	Subject Matter Expert, SSO		2/7/2017
Paul Golan	DOE SLAC Site Office Manager		2/9/17

Please return signed document to: Contract Management, MS 75

Revision History

Revision	Revision Date	Summary of Change(s)
R0	02/07/2017	Original Release.