STANFORD UNIVERSITY

SLAC National Accelerator Laboratory

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

DOE Order 200.1A, Information Technology Management, Chg. 1 (1/13/2017)

Site Compliance Plan (final rev., 09/20/2019)

Contents

Introduction

This Site Compliance Plan (SCP):

a) corresponds with the version of the DOE Order on Information Technology Management 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).

Contractor Requirements Document (CRD) – Attachment 1

CRD §	Requirements from CRD, Attachment 1	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
1.	Information Technology Strategic Planning. Maintain a strategic plan that coordinates IT planning and investment decisions and links contractor-specific missions and goals to the Departmental strategic plan, as well as:	In compliance	Outlined in sections below.	n/a	n/a	n/a	n/a
1a.	Implement an IT investment decision process that utilizes	In compliance	SLAC has ongoing investment decision processes that align projects and efforts to lab and OCIO strategies and principles & Enterprise Architecture principles. Additionally, there is alignment with PEMP goals, cybersecurity requirements, risk-	n/a	n/a	n/a	n/a

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

DOE Order 200.1A, Information Technology Management, Chg. 1 (1/13/2017)

Site Compliance Plan (final rev., 09/20/2019)

CRD §	Requirements from CRD, Attachment 1	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	Enterprise Architecture principles		reduction and operational lifecycle implications, Capital Asset Management Process (CAMP) scoring, and the DOE strategic plan. The level of these alignments is then weighed against the amount of required investment to drive appropriate decision-making.				
1b.	Implement and manage IT acquisition processes to achieve cost savings through appropriate IT hardware and software standards, negotiated buying arrangements, and refresh policies.	In compliance	**(I) IT Standards** SLAC has desktop, laptop, standard models and configuration requirements for Business, Scientific, and Engineering client computing that assure that sustainability goals are met. Additionally, we have standardized on specific OEM models for enterprise storage and servers. Standardized models are process through the IT service catalog. **(II) Negotiated buying arrangements** The Computing Division, via SCM, leverages DoE ICPT contracts where possible. We consolidate site wide software acquisitions and negotiate volume purchase pricing and enterprise wide agreements for centrally managed information technologies in accordance with the DOE approved SLAC standard procurement policy and process: https://slac.sharepoint.com/sites/scm/PD/Forms/AllItems.aspx https://internal.slac.stanford.edu/scm/training/job-aids **(III) Technology Refresh Policies** Based on this roadmap and IT standards, lifecycle and refresh programs for IT hardware (server infrastructure) are in place with appropriate policies. A refresh program for user (client) devices (e.g. desktops, laptops, tablets) will be developed and operated on an ongoing basis.	n/a	n/a	n/a	n/a
2.	Capital Planning and Investment Control. Develop, implement, and maintain a Capital Planning and Investment Control (CPIC) process, as well as:	In compliance	Outlined in sections below.	n/a	n/a	n/a	n/a

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

DOE Order 200.1A, Information Technology Management, Chg. 1 (1/13/2017)

Site Compliance Plan (final rev., 09/20/2019)

CRD §	Requirements from CRD, Attachment 1	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
2a.	Execute program and office specific processes that support Department-wide CPIC efforts by monitoring and demonstrating effective control of the cost, schedule, and performance of investments and corresponding projects;	In compliance	A Computing Project Office is in place to control the cost and the processes that support Department-wide schedule and performance of Centrally Managed IT Investments and CPIC efforts by monitoring corresponding projects. The Computing Project Office operates effective control of costs, guidance, assurance, and schedule according to standards.	n/a	n/a	n/a	n/a
2b.	Implement appropriate internal policies regarding the acceptable use of IT assets;	In compliance	SLAC abides by Stanford's computer and network usage policy for assets and has an internal policy for Acceptable Use of Information Technology Resources. Stanford Acceptable Use Policy (AUP): • https://adminguide.stanford.edu/chapter-6/subchapter-2/policy-6-2-1 SLAC Acceptable Use of Information Technology Resources: • https://policies.slac.stanford.edu/policy/acceptable-use-information-technology-resources	n/a	n/a	n/a	n/a
2c.	Prioritizing and selecting investments, based upon performance and results, as part of the budget development process.	In compliance	SLAC has an ongoing effort and project prioritization process that supports decision-making on appropriate investments. This prioritization process is improved on an ongoing basis.	n/a	n/a	n/a	n/a
3.	Enterprise Architecture. Maintain an Enterprise Architecture for the life-cycle management of information resources and related IT investments funded by or operated for DOE.	In compliance	Information Technology roadmaps capture the cost, value and life-cycle of the various information resources. This is part of the enterprise architecture roadmap. Based on this roadmap and IT standards, an infrastructure, server lifecycle program is underway and is replacing aging, at-risk infrastructure. The remaining infrastructure requiring a formal lifecycle program to maintain its ongoing refresh (business systems, user devices, core infrastructure) has been developed and is implemented.	n/a	n/a	n/a	n/a
4.	Hardware and Software Acquisition. Ensure the acquisition, use, and management of IT hardware and software funded by or operated for DOE meet program and mission goals to	In compliance	Outlined in sections below.	n/a	n/a	n/a	n/a

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

CRD §	Requirements from CRD, Attachment 1	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	promote sound resource management, specifically to:						
4a.	Promote consolidation of software acquisition, volume purchasing arrangements, enterprise wide agreements and best practices in software implementation, consistent with the Program Evaluation Management Plan and/or the SmartBuy program.	In compliance	Lab-wide software requests route through computing for usage and compliancy review. Predominately, SLAC's software agreements are for software installed on DoE assets (which are verified via our Property Control database); a few titles include one home use licenses (such as Mathematica and MATLAB) for active FTE's. Software license requirements are combined to leverage volume discounting and establish enterprise agreements. Additionally, ongoing Support agreements are centrally managed by computing to assure appropriate discount levels are obtained and true-ups/renewals are transacted within the proper period of performance thus minimizing risk of compliancy concerns/audits. Client device procurements route through computing for standardization and configuration review. The majority of all client resources are centrally purchased using DoE funds and are centrally supported and comply with security and central management procedures/policies.	n/a	n/a	n/a	n/a
4b.	Implement a Software Quality Assurance (SQA) program that applies a graded, risk-based approach.	In compliance	SLAC has a defined Software Development Lifecycle, with security considerations taken into account throughout the lifecycle. Vulnerability scanning has been incorporated into the SDLC, so that vulnerabilities may be found and addressed before the application is moved into production • Internal and external SLAC websites and web-based applications are scanned on a regular basis to identify vulnerabilities, and if found, remediation plans are developed and implemented ○ This program has already identified and helped remediate over 600 vulnerabilities ○ More information: https://confluence.slac.stanford.edu/display/CSOP/Web+Application+Security+Scanning+Service • SLAC provides specialized training to application developers: CS-203 Cyber Security for Application Developers	n/a	n/a	n/a	n/a
4c.	Ensure compliance with negotiated contract	In compliance	(1) See corresponding implementation element in lb (II). (2) See corresponding implementation element in lb (I)	n/a	n/a	n/a	n/a

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

CRD §	Requirements from CRD, Attachment 1	Compliance Status	Method of Compliance	Deliverables* (managed through SLACTrak)			
				Item	Frequency	Due Date(s)	Recipient (e.g., SSO)
	procurement requirements for IT procurements. (1) Deploy acquisition strategies for IT hardware designed to take advantage of volume discount savings. (2) Promote use of common hardware and software configurations, where appropriate. (3) Adopt standard replacement policies to make the best use of existing resources.		(3) See corresponding implementation element in lb (III)				
5.	IT Operations and Use. Implement and manage IT operations and processes to ensure that information published to Federal service-to-citizens public websites are appropriate, timely, and accessible to the public and individuals with disabilities.	Not applicable to SLAC; SLAC does not have federal service-to-citizens public websites at this point.					

(end CRD)

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

Definitions

1. Architecture Review Board (ARB). The principal body charged with coordinating, reviewing and evaluating the implementation of the DOE EA.
2. Business Owners. Departmental entities that have an interest in IT management to support business needs.
3. Capital Planning and Investment Control (CPIC). A systematic approach to managing the risk and returns of IT investments for a given mission.
4. Computer Software Piracy. The use and or distribution of copyrighted computer software in violation of the copyright laws or applicable license restrictions. Common forms include end user piracy, counterfeiting, and hard-disk loading. End-user piracy occurs when an individual or organization reproduces and/or uses unlicensed copies of software for its operations by making more copies of the software than it is licensed for. Counterfeiting is the illegal duplication or distribution of software. Hard-disk loading occurs when a computer hardware reseller loads unauthorized copies of software into the machines it sells.
5. Departmental Element. A Departmental element is defined as a first-tier organization at Headquarters and in the Field. First-tier at Headquarters is the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier in the Field is Managers of the eight Operations Offices, Managers of the three Field Offices, and the Administrators of the Power Marketing Administrations. Headquarters and field elements are described as follows: (1) Headquarters elements are DOE organizations located in the Washington Metropolitan Area; and (2) "field elements" is a general term for all DOE sites (excluding individual duty stations) located outside of the Washington, DC, Metropolitan Area.
6. Enterprise Architecture (EA). A business-driven plan that describes the current state, future vision, and transitional states of an operation. This is presented in terms of: strategy and performance; business; applications and services; technology; data; and security, all at the end of a two-to-five year planning horizon.
7. Enterprise Architecture Working Group (EAWG). The principal body for DOE and Program Secretarial Office Enterprise Architecture integration initiatives.
8. Electronic Government. Electronic systems and networks that provide the public with access to or interaction with Government entities, services, information, and products without preference in a manner that acknowledges constitutional intent for privacy, security, and, if warranted, anonymity.
9. Hardware. Physical computer and other equipment used to process, store, or transmit computer programs or data.

STANFORD UNIVERSITY

SLAC National Accelerator Laboratory

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

DOE Order 200.1A, Information Technology Management, Chg. 1 (1/13/2017)

Site Compliance Plan (final rev., 09/20/2019)

Approvals

Name:	Title:	Signature:	Date:
Theresa Bamrick	Chief Information Officer, SLAC		30 Sep 2019
Scott Wenholz	Physical Scientist		9/24/2019
Paul Golan	Head of Field Element	ESM	9/30/19

Please return signed document to: Contract Management, MS 75

Revision History

Revision	Revision Date	Summary of Changes
R0	12/21/2008	Original Release
R1	09/20/2019	Updated to Chg. 1; Minor edits to links in document and methods of compliance