DRAFT

RESEARCH SUPPORT BUILDING AND INFRASTRUCTURE MODERNIZATION

PRELIMINARY SECURITY VULNERABILITY ASSESSMENT REPORT

SLAC
NATIONAL ACCELERATOR LABORATORY

April 2009
SLAC-I-050-07010-002

Contents

Revision History

Rev. No.	Date	Revision Description	Pages Modified
Rev. 0	04.15.09	Initial Issue; Preliminary Security Vulnerability Report for CD-1	Not Applicable

1.0 Introduction

SLAC National Accelerator Laboratory (SLAC) proposes the construction of a new energy efficient and environmentally sustainable research support building, the renovation of existing space and the demolition of substandard buildings. This project is designed to provide progressive and adjustable space for furthering the scientific mission at SLAC. The design will use efficient space planning benchmarks as the basis for determining the size and configuration of space types. The design of the new facility will also emphasize open, collaborative environments, with flexibility to respond to future mission changes. The facilities will include office spaces for researchers, small group collaboration spaces, equipment areas, restrooms, circulation space, and supporting infrastructure. These facilities will permit the collocation of accelerator scientists and staff, enabling interaction among researchers and graduate students with complementary interests. These proposed facilites further the support of the accelerator based research programs at the Laboratory and optimize cross program collaborations. The proposed renovations to the existing buildings (i.e., 003, 024, 041) will group like mission critical support functions together, improve the work spaces within those structures and provide an efficient and reliable working environment

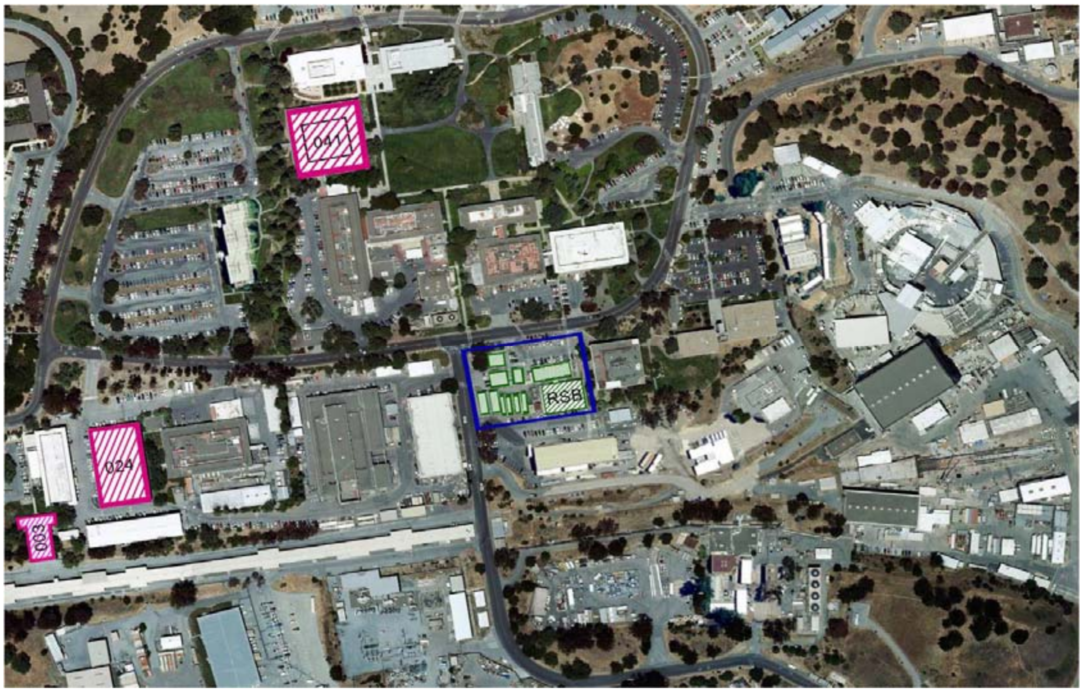


Figure 1 – Project Site

1.1 Purpose

The purpose of this Preliminary Security Vulnerability Assessment Report (PSVAR) is to identify the safeguards and security requirements and integrate these requirements into the Research Support Building and Infrastructure Modernization (RSB) Project at the early conceptual design phase of the project's life cycle. In addition those requirements implementation is assessed throughout the project.

The Project Preliminary Security Vulnerability Assessment Report is developed using DOE G 413.3-3 Safeguards and Security for Program and Project Management as the guidance document for this effort.

1.2 Scope

The Preliminary Security Vulnerability Assessment Report (PSVAR) evaluates the potential risk to employees, the public, and the environment at SLAC during the design, construction, and operational phases of the RSB project. The PSVAR also develops the effective protection strategies that will be implemented during the project's different phases. Future activites planned for the RSB, B003, B024, and B041 will also be evaluated in the PSVAR.

The successful protection of security interests requires that effective protection strategies and procedures be developed and implemented. The Protection strategy for an asset will include consideration of the threat to the asset as a fundamental part of the design process. Establishing and integrating safeguards and security requirements early in the projects lifecycle is necessary for project planning, cost estimating, facilities requirements, and to prevent project impacts that can arise when safeguards and security requirements are identified late into the design process, construction, or as part of the operational readiness review. Additionally, due to potential conflicts in meeting safeguards and security requirements and the requirements of other critical disciplines (e.g. safety), the integration of all requirements is critical to developing the best overall cost effective solution for the project.

1.3 Ojectives

The objective of the PSVAR is as following:

a. To provide safeguards and security advice to Federal project directors and federal program/site office managers (contractors and subcontractors as applicable) in identifying and implementing key safeguards and security components of their projects an integrating safeguards and security consideration into each acquisition management phase (initiation, definition, execution and transition/closeout).

b. To define security project's features and functions as developed or required by the security program or security policy which minimizes impact on operations.

c. To identify the function of the federal site security program representative who serves as security design point of contact for security features and is a member of the integrated project team as appropriate during the entire project cycle.

d. To facilitate communication and interaction between the site security professionals, other integrated project teams and the members of the project design team.

2.0 Target Identification and Description

The Security Vulnerability Assessment of RSB project is developed to evaluate the potential risk to employees, the public, and the environment at SLAC during project design, construction and operation phases.

The project will not change the safeguards and security requirements at SLAC. The site is categorized as a Class C, Security Protection Level (SPL) IV facility. No sensitive or classified research is conducted by SLAC. Currently the entry gates provide perimeter access and basic visitor services and traffic management.

The RSB Project adopts the SLAC Site Security Plan SLAC-I-730-0A86M-002-R000 as the guidance document for security protection during design, construction, and operation phases. See Appendix A. The Hazard Analysis Report (HAR) will identify the types of threats and potential targets for the Project.

2.1 Facilities

2.1.1 Research Support Building

The new Research Support Building design includes typical private and open office spaces, library area, small group collaboration spaces, restrooms, circulation space, etc. The potential security threats found in the design, construction and operation phases of the building are the same as the threats indicated in the SLAC Site Security Plan.

2.1.2 Building 003

The renovation of Building 003 design includes typical private office spaces, Training Center, restrooms, circulation space, etc. The potential security threats found in the design, construction and operation phases of the building is the same as the threats indicated SLAC Site Security Plan. Refer to Appendix A for SLAC Site Security Plan; table 1 for the types of threats that might be expected and their potential targets.

2.1.3 Building 041

The renovation of Building 041 design includes typical private and open office spaces, small group collaboration spaces, SLAC medical facility, restrooms, circulation space, etc. The potential security threats found in the design, construction and operation phases of the building is the same as the thread indicated SLAC Site Security Plan. Refer to Appendix A – SLAC Site Security Plan: table 1 for the types of threats that might be expected and their potential targets

2.1.4 Building 024

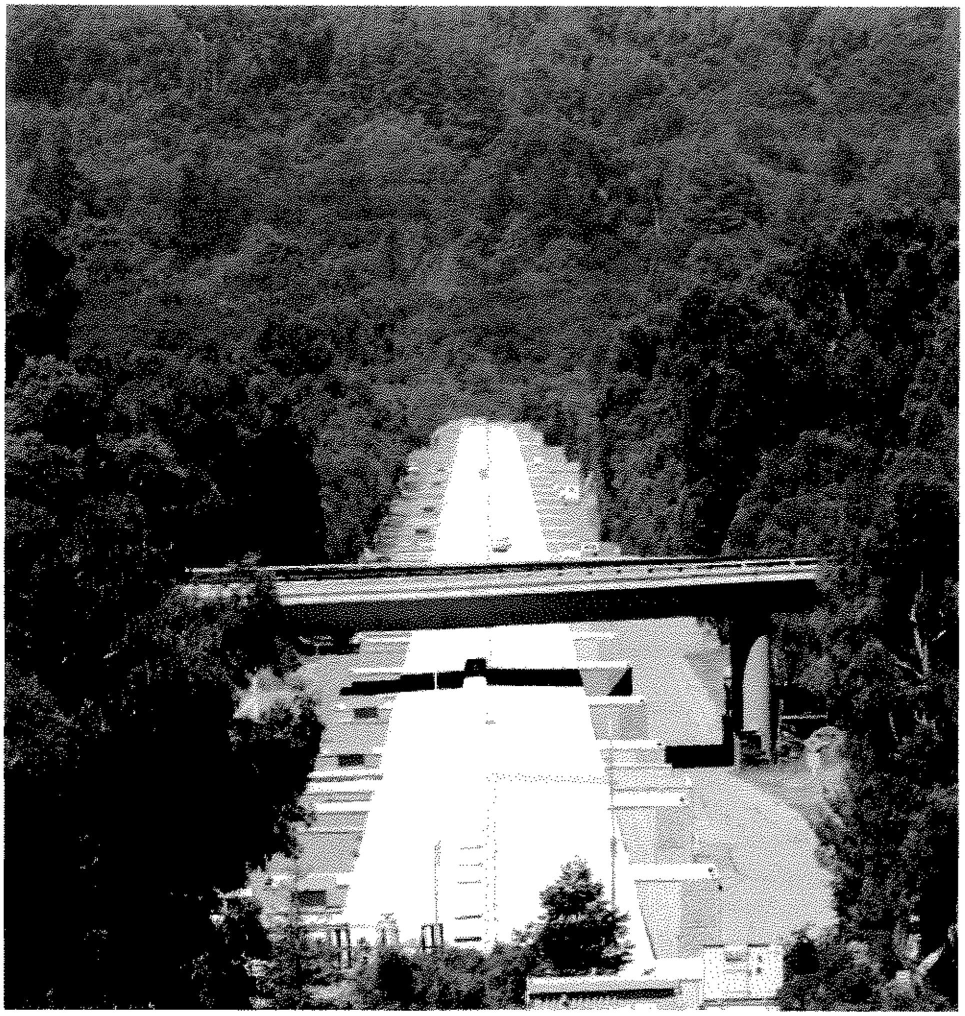
The renovation of Building 024 includes spaces identified in the renovation of B003 and B041. In addition the renovation will include light manufacturing and assembley areas, chemical labs and hoods, and a radioactive emission source. The evaluation of the renovation’s security threats for this building by the Project Team has been performed with the assistance of the Radiation Protection Department. They have determined that the renovation will not increase the potential security threats beyond the existing ones as indicated in SLAC Site Security Plan.

2.2 Safeguards and Security

Safeguards and Securities requirements are coordinated with SLAC Security and addressed in the Preliminary Securities Vulnerability Assessment Document SLAC-I-050-07050-002. Access requirements and procedures are written into project contract documents and will be followed by all project subcontractors accessing the site. SLAC is not a classified DOE facility; therefore, no Q or L clearances will be required. The contractor will be required to provide fencing to isolate the project areas for safety as well as security considerations.

Appendix A: SLAC Site Security Plan

SLAC National Accelerator Laboratory
Stanford University
Menlo Park, California



Site Security Plan
December 2008

Site Security Plan
SLAC National Accelerator Laboratory

Effective Date
8 December 2008

Prepared By: ________________________________ Date: __________
Simon Ovrahim
Manager, SLAC Site Security
Environment, Safety, and Health Division

Approved By: ________________________________ Date: __________
Brian Sherin
Deputy Division Director
Environment, Safety, and Health Division

Approved By: ________________________________ Date: __________
Craig Ferguson
Division Director and Chief Safety Officer
Environment, Safety, and Health Division

Approved By: ________________________________ Date: __________
Alexander Merola
Chief Operations Officer
SLAC National Accelerator Laboratory

TABLE OF CONTENTS

INTRODUCTION

The SLAC National Accelerator Laboratory (SLAC) is a federally funded research and development center (FFRDC) and a national user facility. SLAC serves a large community of users from both the United States and numerous foreign nations. Consistent with the terms of the contract with Stanford University, no sensitive or classified research is conducted by SLAC or allowed on-site.

SLAC is a Class C, Security Protection Level (SPL) IV facility, with emphasis on prevention of unaccountable property loss from the site. The SLAC *Property Management Plan* is used as the reference for property protection. From a site security point of view, property protection is accomplished by implementation of the strategy described in Section 1.2.

FACILITY OVERVIEW

Type of Facility	Facility Importance Rating	Material Type/Classification	Facility Threat Level
Property Protection	Class C	Category IV/Unclassified	SPL IV

MISSION

The mission of the SLAC National Accelerator Laboratory is

- **Photon Science Discoveries.** To make discoveries in photon science at the frontiers of the ultrasmall and ultrafast in a wide spectrum of physical and life sciences
- **Particle and Particle Astrophysics Discoveries.** To make discoveries in particle and astroparticle physics to redefine humanity's understanding of what the universe is made of and the forces that control it
- **Operate Safely; Train the Best.** To operate a safe and secure laboratory that employs and trains the best and brightest, helping to ensure the future economic strength and security of the nation

DESCRIPTION

The SLAC site consists of approximately 426 acres of land leased from Stanford University by the US Department of Energy (DOE). The site is located in southern San Mateo County at the base of the foothills of the San Francisco peninsula. The site has been developed as a physics research laboratory and is operated by Stanford University under contract with the DOE. (Exhibit 4 shows an aerial photo of the SLAC site.)

Site Security Interests

Identification of Site Security Interests

There is a limited scope of security interests that are protected in designated property protection areas. The remainder of the site is an open extension of the Stanford University campus. The entry gates provide perimeter access and basic visitor services and traffic management. Formal access controls and enhanced security are accomplished at the designated (property protection areas) PPAs.

Location of Property Protection Areas

PPAs have been established to protect government-owned property against damage destruction, or theft. Designated PPAs within the lab that may be at risk from groups or individuals identified in the risk assessment have higher levels of physical protection and access controls. These areas include the following:

- Hazardous Waste Storage Facility, Building 245
- Radiological Calibration Facility, Building 24, Room 167

1.0 PROGRAM MANAGEMENT AND SUPPORT

1.1 PROTECTION PROGRAM MANAGEMENT

1.1.1 Program Management and Administration

References

- DOE P 470.1, "Integrated Safeguards and Security Management (ISSM) Policy"
- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 1, Section A, "Safeguards and Security Program Planning"

Integrated management at SLAC includes both integrated safeguards and security management (ISSM) and integrated safety and environmental management (ISEM). Every member of the SLAC community is expected to contribute to the furtherance of safety and security at SLAC and to the protection of government assets. The SLAC community is expected to understand and carry out applicable safety practices, physical and/or computer security practices, and procedures.

The IM principles are to be integrated into every task. This includes reviewing every new task or project for any safety or security concern and ensuring these concerns are addressed and/or corrected before beginning the work. Everyone is expected to promptly speak with his/her supervisor or project lead about any safety or security concern and to report irregularities.

The DOE undersecretary for science is responsible for the management and implementation of site security programs administered by the Office of Science (SC) and serves as the cognizant security authority. The SC SLAC Site Office (SSO) is the lead responsible office (LRO) for SLAC and is the local DOE authority that approves the site security plan (SSP). The SC Oak Ridge Service Center is the designated surveying office.

The SLAC Site Security Office is assigned to the Environment, Safety, and Health Division (ES&H). ES&H reports to the SLAC director of operations. Property protection and site surveillance operations are conducted under a subcontract with a commercial security services company, Securitas. This subcontract (515-PS-42965, Supplemental Agreement, Modification No. 3) is dated 22 September 2005 and executed under the Prime Contract Number DE-AC02-76-SFO0515, between the United States Department of Energy and Stanford University. It comports with the Stanford University Board of Trustees Resolution Number 13 and SLAC National Accelerator Laboratory Business Services Division Procedure Number 40-0. General law enforcement services to SLAC are provided by the San Mateo County Sheriff's Department, located in Redwood City, California. Administration and management of the subcontract is the direct responsibility of the SLAC Site Security manager, who also fills the role of facility security officer (FSO). (Figure 1 shows the overall SLAC organization chart.)

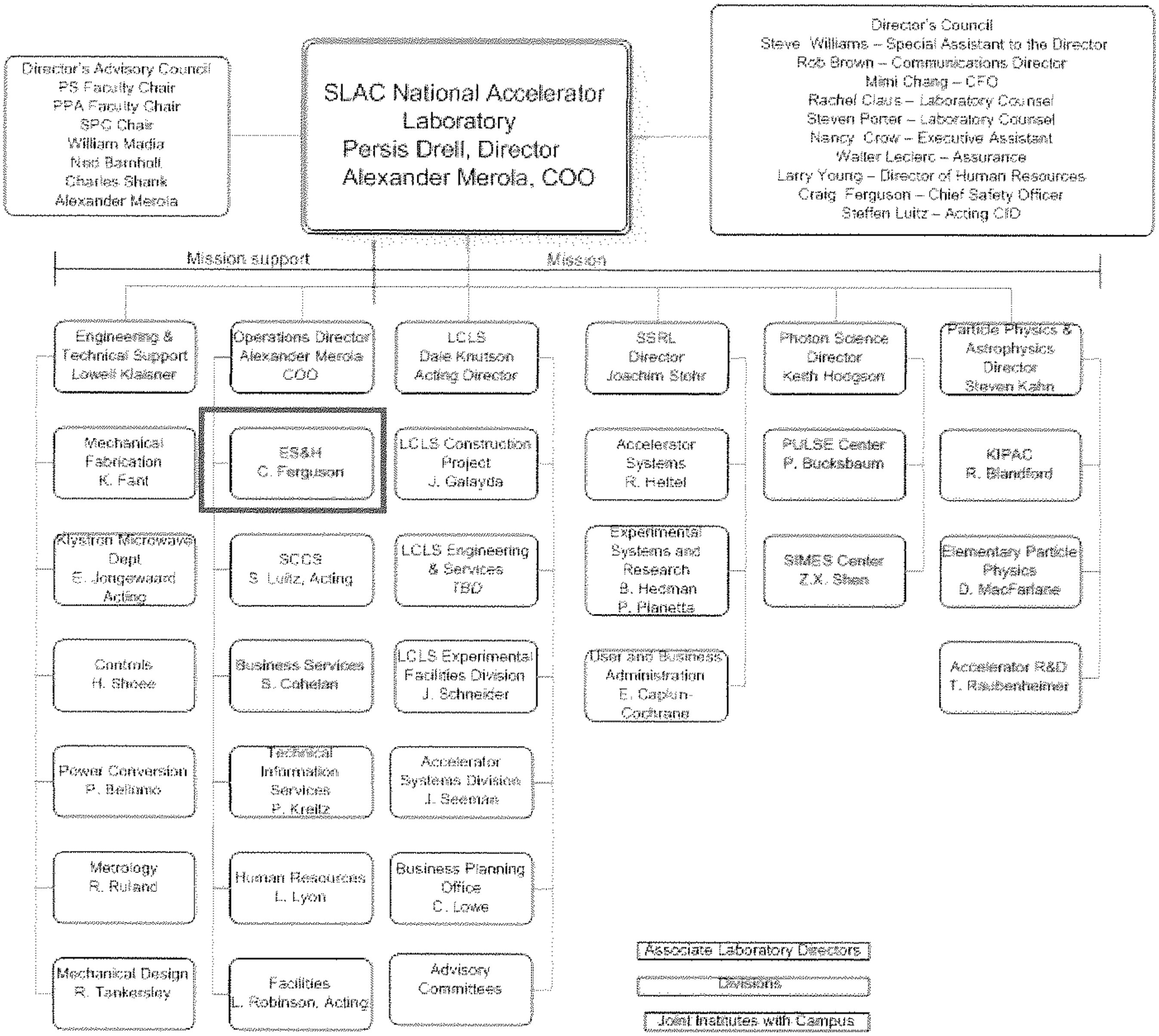

Director's Advisory Council
PS Faculty Chair
PPA Faculty Chair
SPC Chair
William Madia
Ned Barnholt
Charles Shank
Alexander Merola
SLAC National Accelerator Laboratory
Persis Drell, Director
Alexander Merola, COO
Director's Council
Steve Williams – Special Assistant to the Director
Rob Brown – Communications Director
Mimi Chang – CFO
Rachel Claus – Laboratory Counsel
Steven Porter – Laboratory Counsel
Nancy Crow – Executive Assistant
Walter Leclerc – Assurance
Larry Young – Director of Human Resources
Craig Ferguson – Chief Safety Officer
Steffen Luitz – Acting CIO
Mission support
Mission
Engineering & Technical Support Lowell Klaisner
Operations Director Alexander Merola COO
LCLS Dale Knutson Acting Director
SSRL Director Joachim Stohr
Photon Science Director Keith Hodgson
Particle Physics & Astrophysics Director Steven Kahn
Mechanical Fabrication K. Fant
ES&H C. Ferguson
LCLS Construction Project J. Galayda
Accelerator Systems R. Hettel
PULSE Center P. Bucksbaum
KIPAC R. Blandford
Klystron Microwave Dept E. Jongewaard Acting
SCCS S. Luitz, Acting
LCLS Engineering & Services TBD
Experimental Systems and Research B. Hedman P. Pianetta
SIMES Center Z.X. Shen
Elementary Particle Physics D. MacFarlane
Controls H. Shoee
Business Services S. Cohelan
LCLS Experimental Facilities Division J. Schneider
User and Business Administration E. Caplun-Cochrane
Accelerator R&D T. Raubenheimer
Power Conversion P. Bellomo
Technical Information Services P. Kreitz
Accelerator Systems Division J. Seeman
Metrology R. Ruland
Human Resources L. Lyon
Business Planning Office C. Lowe
Mechanical Design R. Tankersley
Facilities L. Robinson, Acting
Advisory Committees
Associate Laboratory Directors
Divisions
Joint Institutes with Campus

Figure 1

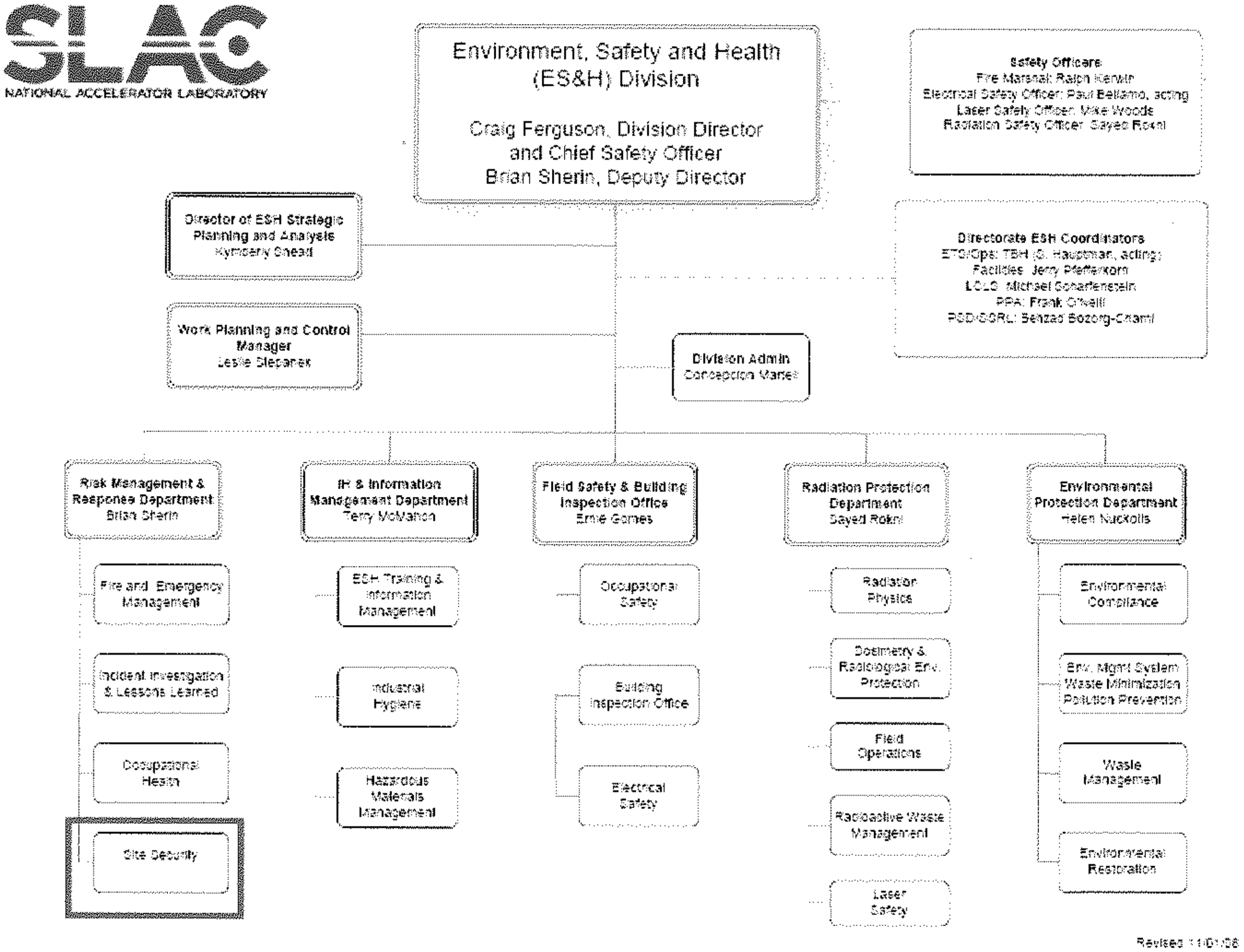

SLAC NATIONAL ACCELERATOR LABORATORY
Environment, Safety and Health (ES&H) Division
Craig Ferguson, Division Director and Chief Safety Officer
Brian Sherin, Deputy Director
Safety Officers
Fire Marshal: Ralph Kerwin
Electrical Safety Officer: Paul Bellamo, acting
Laser Safety Officer: Mike Woods
Radiation Safety Officer: Sayed Rokni
Director of ESH Strategic Planning and Analysis
Kymberly Snead
Directorate ESH Coordinators
ETO/Ops: TBH (G. Hauptman, acting)
Facilities: Jerry Pfefferkorn
LCLS: Michael Scharfenstein
PPA: Frank O'Neill
PSD/SSRL: Behzad Bozorg-Chami
Work Planning and Control Manager
Leslie Stepanek
Division Admin
Concepcion Manes
Risk Management & Response Department
Brian Sherin
IH & Information Management Department
Terry McMahon
Field Safety & Building Inspection Office
Ernie Gomes
Radiation Protection Department
Sayed Rokni
Environmental Protection Department
Helen Nuckolls
Fire and Emergency Management
Incident Investigation & Lessons Learned
Occupational Health
Site Security
ESH Training & Information Management
Industrial Hygiene
Hazardous Materials Management
Occupational Safety
Building Inspection Office
Electrical Safety
Radiation Physics
Dosimetry & Radiological Env. Protection
Field Operations
Radioactive Waste Management
Laser Safety
Environmental Compliance
Env. Mgmt System Waste Minimization Pollution Prevention
Waste Management
Environmental Restoration
Revised 11/01/08

Figure 2

1.1.2 Resources and Budgeting

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 1, Section A, "Safeguards and Security Program Planning"

See Exhibit 5, line item FS1009-1 and FS1009-7. In FY09, 90 percent of the Site Security manager's time is associated with activities related to Site Security operations, the remaining 10 percent are currently associated with management and oversight of activities supporting safety-related issues. In addition, 0.25 FTE of ES&H Division management time (includes department head and IT support to Site Security) is associated with the management and oversight of security operations. In FY10 and FY11, this will also be 90 percent of the Site Security manager, and 100 percent of a to-be-hired deputy, associated with activities related to Site Security operations. Division management time in FY'10-11is estimated to be 0.25 FTE.

1.1.3 Personnel Development and Training

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 1, Section J, "Safeguards and Security Training Program"

Training and development of SLAC's Security professional staff will be accomplished through available:

- Career development
- Professional counseling
- Environmental, Health, and Safety training to safely carry out the security mission
- On-the-job training
- DOE National Training Center
- Workshops
- Conferences
- Forums

For related budget expenses, see Exhibit 5, line item FS 1001-8 and FS1009-2.

1.2 Site Security Planning and Procedures

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management"
  - Part 1, Section A, "Safeguards and Security Program Planning"
  - Part 2, Section M, "Deviations"

SLAC is a university-based science laboratory. Only unclassified, non-sensitive research is undertaken at SLAC. SLAC's work falls within the "fundamental research" exclusion from export control regulations of the Commerce Department, 15 CFR 734.8, based on the nature of the research and on the wide dissemination and public availability of its research results.

SLAC's policies and procedures reflect compliance with this DOE order. Among these are counterintelligence, computer security, and unclassified visits and assignments by foreign nationals.

SLAC computer related security management is primarily directed at ensuring the integrity of the computer system from unauthorized intrusion ("hacking") by citizens of any nationality (including US), especially with regard to ensuring the viability of research and business operations and safeguarding personnel data protected under various privacy statutes.

Threats to SLAC may arise from those who oppose research and development activities of the laboratory, Stanford University, or the U S Department of Energy or the policies of the US Government. Additional threats may come from those who oppose the handling of hazardous materials associated with research. The following table summarizes the types of threats that might be expected and their potential targets.

Threat	Definition	Target
Terrorists	Persons or groups who will use violence to further political objectives	SLAC personnel and property
Criminals	White- or Blue-Collar, nonviolent, usually one person; insider, contractor, or visitor. Usually no prior criminal record. Not motivated by political or personal ideals; not willing to go to jail; not willing to get caught; act done for personal monetary gain. May be connected to narcotics activity. May damage or destroy equipment. May steal tools, equipment (including computers) and raw materials.	SLAC property
Organized Crime	Person or persons who conspire with others or perpetrate acts for financial gain to support narcotics or other illegal acts.	SLAC personnel and property
Mentally Ill	Mentally disturbed individuals. Capable of causing records or property destruction; may cause personal harm to others or self up to and including death.	SLAC personnel and property
Disgruntled Employees	One person, acting alone, capable of doing damage to records, equipment; can cause death or injury to others.	SLAC personnel and property
Violent Activists	Person or group in opposition to programs: ecological, political, economic, or ideological.	SLAC personnel and property

Three strategies are utilized in the protection of personnel and property at SLAC in a graded approach that includes designated property protection areas (PPAs), surveillance, and intervention. The degree to which these strategies are employed is risk-based and may change in level of deployment depending upon the identified security condition and/or threat level. Facilities within the designated PPAs, which may be targets of groups identified in the risk assessment, have higher levels of security.

Site Security Plan and Procedures

The following table shows the responsible SLAC organization for the various Site Security management plans and procedures.

Plan/Procedure Title	Responsible Organization
Site Security Plan	Site Security Office, ES&H Division
SLAC Incident Reporting Procedure	Site Security Office, ES&H Division
SLAC Site Access and Identification Badges Procedure	Site Security Office, ES&H Division
Traffic Control Program	Site Security Office, ES&H Division
Assets Protection Officer Procedure Manual	Business Services Division
Lock and Key procedure	Site Security Office, ES&H Division
Lost and Found Procedure	Site Security Office, ES&H Division
Protective Force Training and Qualification Plan	Site Security Office, ES&H Division
SLAC Security Condition (SECON) levels.	Site Security Office, ES&H Division
Site Surveillance, ES&H Training, and Radiation Dosimetry Policies and Procedures	Site Security Office, ES&H Division
Nuclear Material Control and Accountability Plan	Radiation Protection Department, ES&H Division
Cyber Security Program Plan (CSPP)	SLAC Scientific Computing and Computing Services (SCCS)

Security Condition Levels

Five security-condition levels apply to SLAC and align with the Homeland Security Threat Advisory System.

They are described briefly below.

- **SECON-1. (Red – Severe)** This most serious condition is declared in the immediate area where a terrorist attack has occurred that may affect the site or when an attack is initiated on the site. This condition significantly increases protective measures and may require additional protective elements, along with those required in SECON-2.
- **SECON-2. (Orange – High)** This condition is set when a terrorist incident occurs or intelligence information is received indicating that some form of terrorist action is imminent, and requires specific protection measures to be put in place.
- **SECON-3. (Yellow – Elevated)** This condition is used when an increased and more predictable threat of terrorist activity exists and may increase access controls to include additional personnel and vehicle barriers.
- **SECON-4. (Blue – Guarded)** This condition applies to a possible threat of terrorist activities and generally enhances security awareness responsibilities.
- **SECON-5. (Green – Low)** This condition exists when a general threat of possible terrorist activity exists, but warrants only routine security measures associated with daily operations.

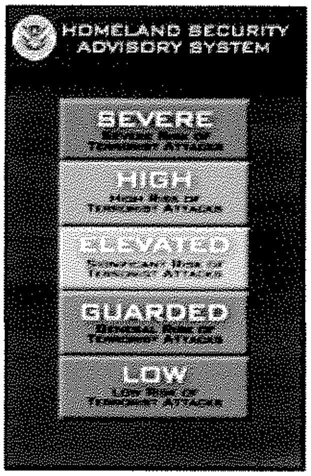

HOMELAND SECURITY
ADVISORY SYSTEM
SEVERE
Severe Risk of Terrorist Attacks
HIGH
High Risk of Terrorist Attacks
ELEVATED
Significant Risk of Terrorist Attacks
GUARDED
General Risk of Terrorist Attacks
LOW
Low Risk of Terrorist Attacks

Figure 3

SLAC has developed a local procedure for specific implementation of the various security condition levels.

1.3 Management Control

1.3.1 Surveys and Self-assessment Program

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 1, Section G, "Survey, Review, and Self-assessment Programs"

Self-assessment

SLAC Site Security participates in an annual functional area self-assessment, which is an ongoing process begun as part of the Business Management Oversight Pilot established by DOE in March 1995 and continued by executive order as part of DOE performance-based management. The assessment materials are collected from data collected over the previous year, followed by a process of validation of findings, analysis, and report writing. The Site Security functional area self-assessment is based on and measured against performance measures agreed to between

SLAC and the DOE SLAC Site Office (SSO) in order to address customer satisfaction, cost efficiency, and contract compliance.

SLAC currently benefits from its separate location from the main Stanford University campus. The existing exterior barriers, including fencing, uniformed protective force, DOE Office of Science common badge use, DOE NO TRESPASSING signs, and other protective measures contribute to a visible deterrent factor. However, substantial additional development is occurring adjacent to the site (major hotel and spa currently under construction and likely additional Stanford University construction) that will require improvements to SLAC's perimeter fencing. The terrain adjacent to SLAC Accelerator, which is also fenced, creates multiple barriers to unrestricted entry by the general public and to any person or persons with other than honorable intentions.

To date, violent crime has not been a problem on the site; however, some workplace violence issues have arisen and have been dealt with through the university administrative procedures by the SLAC Human Resources Department. No assaults have been associated with workplace violence cases. Theft of high-dollar items and some raw materials theft (mostly copper cable) occur periodically, with computers being the most frequently stolen high dollar item.

There has been no major violent crime at SLAC for last 12 years

For related budget expenses, see Exhibit 5, line item FS1009-3.

1.3.2 Performance Assurance Program

Not applicable

1.3.3 Resolution of Findings

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 1, Section G, "Survey, Review, and Self-Assessment Programs"

The purpose of the SLAC's Corrective Action Tracking System (CATS) is to track corrective actions generated from SLAC incidents, SLAC assessments, both internal and external, and at times lessons learned.

Before corrective actions can be developed and entered into CATS, a thorough understanding of causal factors that led to an incident or assessment issue is required. Without knowing the cause of an incident or assessment issue, it is impractical to develop effective corrective action.

In the case of an incident, as described in the ES&H Manual Chapter 28, "Incident Investigation", a competent investigator from the line organization experiencing the incident is to assess causal factors and develop effective corrective actions which are then entered into CATS. When the incident meets DOE occurrence reporting thresholds, causal analysis and corrective action must be in accordance with Occurrence Reporting and Processing System (ORPS) program. Once corrective actions are developed, they are entered into CATS as well as the DOE Occurrence Report and Processing System.

In the case of issues arising from assessment activities, the authority conducting the assessment will decide if causal analysis is warranted prior to entering deficiencies into CATS. Where causal analysis is warranted, the advice and counsel of a competent investigator as defined in the ES&H Manual Chapter 28, "Incident Investigation" will be sought.

The closure of a corrective action will be validated by the SLAC Office of Assurance, which will also make an assessment of the corrective action's effectiveness. CATS data quality will be monitored by staff in the Knowledge Management Group of the ES&H Division who also will respond to a line organization's request to facilitate data entry. However, the line may undertake data entry independent of the ES&H Division.

Dates for completing corrective actions are generally set by the assessment owner. Changes to the completion dates can be submitted by task owners but are not accepted until approved by the assessment owner.

1.3.4 Incident Reporting and Management

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 2, Section N, "Incidents of Security Concern"
- DOE O 226.1A, "Department of Energy Oversight Board"
- DOE O 221.1A, "Reporting Fraud, Waste, and Abuse to the Office of Inspector General"

Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the SLAC facility security officer. This is accomplished through SLAC's incident notification system, which all employees receive in the form of a badge card.

The internal SLAC emergency notification number (Ext. 5555) is managed by SLAC Site Security from the main gate. Security officers have posted instructions to notify appropriate management personnel and emergency authorities, depending upon the type of incident. When the need arises, everyone is expected to cooperate in any security inquiry or investigation in accordance with local incident reporting procedures.

Any person discovering actual or suspected fraud, waste, or abuse of government resources must ensure such incidents are reported to the Office of the Inspector General in accordance with DOE O 221.1A, "Reporting Fraud, Waste, and Abuse to the Office of Inspector General", dated 22 March 2001. Such incidents shall be reported to the Security Manager and the on-call Facility Manager Designee (FMD) as soon as possible, but no later than 24 hours after discovery. In months where there have been no reportable incidents, SLAC provides confirmation that there has been nothing reported (negative reporting) to the local IG office and SSO.

SLAC is subject to DOE O 226.1A, "Department of Energy Oversight Board". By effectively implementing the DOE 470-series directives SLAC satisfy the requirements of DOE 226.1A.

These oversight activities ensure continue cost-effective implementation of DOE requirements, related contract provisions, approved site security plans, approved management programs, work controls and procedures, and mission objectives.

Investigations and incidents are recorded in a database that allows sorting by type of incident. Fields are dedicated to theft, missing property, suspicious activity, vehicle accidents, injuries, traffic violations, vandalism and harassment. Semi-annual and annual reports are provided to the SLAC Director's Office. Theft and missing property reports are forwarded to SLAC Property Control as they occur. Upon receipt of a report of a theft, it is reported to the US Department of Energy Inspector General and to the DOE SLAC Site Office.

1.4 PROGRAM-WIDE SUPPORT

1.4.1 Facility Approval and Registration of Activities

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 2, Section I, "Facility Clearances and Registration of Safeguards and Security Activities"

The SLAC facility security officer provides updates to the facility registration to the SLAC Site Office.

1.4.2 Foreign Ownership, Control or Influence

Not applicable

1.4.3 Security Management in Contracting

References

- DEAR (48 CFR) § 904.404(d), "Solicitation Provision and Contract Clause"
- DEAR (48 CFR) § 970.5204-2, "Laws, Regulations, and DOE Directives"

Applicability of DOE Safeguards and Security Orders to the DOE-Stanford University Contract

The SLAC National Accelerator Laboratory (SLAC) handles unclassified information and DOE property. The need to protect that information and property in a graded fashion in accordance with DOE policy and guidance and federal law is understood. SLAC is in compliance with DOE policy and guidance that has been agreed upon between the DOE and Stanford University.

Specific elements of the graded implementation of applicable DOE safeguards and security directives are contained in this SSP and associated local procedures. Any change to an existing, accepted DOE order or manual, or any addition of any existing or new DOE order or manual to the contract, will be accomplished in accordance with the appropriate article(s) of the contract and included in a revision to the SSP and subsequently approved by SSO.

2.0 PROTECTIVE FORCE

2.1 MANAGEMENT

2.1.1 First Line of Protection

The first line of protection of personnel and property is provided by the contract security force. Should higher-level law enforcement services be required, SLAC notifies and requests assistance from the San Mateo County Sheriff's Department in Redwood City. The Sheriff's Department provides general and special law enforcement services to SLAC as a recognized law enforcement agency under the laws and regulations of the state of California. Services available and rendered are theft investigations, automobile investigations, burglary investigations, interdiction, vandalism investigations, bomb-squad services, and other special investigations as may be required. In addition, the San Mateo County Sheriff's Department provides booking for persons arrested on SLAC property, as well as input capacity to the California Criminal History computer database for police matters associated with SLAC. Special circumstances involving certain types of criminal activity may involve notification of the San Francisco Office of the Federal Bureau of Investigation.

2.1.2 Organization, Mission, and Capabilities

The site protective force is organized into three shifts of contractor-supplied personnel reporting to the SLAC Site Security manager for line management services. The three shifts are the day from 0600 to 1400, the swing from 1400 to 2200, and the graveyard from 2200 to 0600.

The day shift consists of a contract site supervisor, three senior patrol officers, two gate officers at the Sand Hill Road Gate, one gate officer at Sector 30, one gate officer at Gate 17, one gate officer at Alpine gate, and two administrative officers handling DOE common badge, special ID card and dosimeter issue, key issuance, vehicle registration, and traffic violation research.

The swing shift consists of three senior patrol officers, two gate officers at the Sand Hill Road Gate, one gate officer at Sector 30, and one gate officer at Gate 17. One additional gate officer is utilized in a part-time or overtime capacity for the Alpine Road Gate from 1400 to 1800.

The graveyard shift consists of two senior patrol officers, two gate officers at the Sand Hill Road Gate, and one gate officer[1] at the Sector 30 Gate and one gate officer at Gate 17. Those officers working at the Sector 30 Gate and Gate 17 provide safety access control to accelerator areas. Alterations to automate these safety access gates will reduce the security officers providing safety-related services to one officer on the Monday through Friday day shift, thereby allowing the patrol officers to shift more of their time to security and protective service activities.

[1] SLAC employee, title: SLAC Radiation Gate Guard

San Mateo County Sheriff's Department

All violations of state law are investigated by the San Mateo County Sheriff's Department and arrests are made as appropriate. A complete criminal investigative case file is maintained on all criminal matters involving SLAC interests. As a police agency, the San Mateo County Sheriff's Department is fully trained and qualified in all aspects of law enforcement and emergency services response. Additional resources may be requested if required through mutual aid agreements with the California Highway Patrol, from the cities of Menlo Park or Palo Alto, or other law enforcement agencies in the Bay Area. Request and coordination of mutual aid assistance from agencies, other than the San Mateo County Sheriff's Department, is provided by the Office of the Sheriff of the County of San Mateo.

For related budget expenses, see exhibit 5, line item FS1001-1.

2.2 TRAINING

2.2.1 Qualifications and Training

Contract Security Force

The Security Services Contractor provides formal classroom training, some with available undergraduate credits in addition to the fact that all members receive basic assets protection training from the contractor. The basic training includes techniques of observation and report writing, verbal reporting, radio procedures, vehicular and foot patrolling, basic first aid, CPR, telephone procedures and courtesies, bomb threat recording, violence in the workplace identification and training, various personal interaction courses) and basic self-defense tactics. The training is in accordance with the California Bureau of Security and Investigative Services (BSIS) requirements for contract security officers. The applicable California regulation is:

> ***Division 7 of Title 16 of the California Code of Regulations***
>
> ***ARTICLE 9. SKILLS TRAINING COURSE FOR SECURITY GUARDS***
>
> ***643. SKILLS TRAINING COURSE FOR SECURITY GUARDS***
>
> *(a) The course of skills training for registered security guards shall follow the standards prescribed by section 7583.6(b) of the Business and Professions Code. The attached Appendix sets forth the subjects that shall be taught and the maximum number of hours that shall be allowed towards meeting required training.*
>
> *(b) For each course, or series of courses, the institution or company providing the training shall issue a Certificate of Completion to the individual completing the course. The certificate shall identify the course(s) taken, the number of hours of training provided, identification of the issuing entity, name of the individual and instructor and a date, and state that the course(s) comply with the Department of Consumer Affairs.*

The supervisory personnel and senior patrol officers have had advanced classes in all areas plus additional classes in supervisory techniques, identification of safety hazards, hazardous materials response activities, earthquake safety, violence in the workplace, illegal narcotics use and indicators, sexual harassment, physical and mental abuse indicators, burglary and theft indicators, identification and evaluation of suspicious behavior, and basic computer techniques.

Ongoing training in all areas is provided via online course at the SLAC Site Security Operations Office and during monthly meetings hosted by the SLAC Site Security manager

Qualification and training in weapons use is not required in order to meet statement-of-work minimum qualification requirements at SLAC, nor are they required by the US Department of Energy for at a Class C Energy Research Facility.

For related budget expenses, see exhibit 5, line item FS1001-8.

2.3 Duties

The primary mission of the protective personnel is to provide physical protection against theft, misappropriation, vandalism to, or misuse of, US Department of Energy and Stanford University owned or leased materials and equipment through the judicious use of foot and vehicular patrols and electronic recording of site physical security status. Secondary missions of the protective force include

- Preparation and issue of the DOE common badges, SLAC special IDs, and radiation protection dosimeters
- Investigation, preparation, and submission of vehicle accident and theft or missing property reports
- Issuance and recordkeeping for all door keys for the site
- Fence line, site lighting, and building and roadway surveillance and reporting
- First responder assistance to incidents
- Traffic control and enforcement including vehicle registration
- Employee assistance in building and office unlocks
- Lost-and-found item recording and storage
- Employee escort service
- Special event support, including assistance to US Secret Service during US or foreign dignitary visits or tours

Intervention by SLAC Site Security protective personnel or sworn law enforcement agency personnel comes at the request of a building manager, office manager, employee, scientific visitor, or contractor who has been victimized through a call to 911, or to SLAC Site Security Incident Notification system via the site telephone system or a personal visit to any security location

Intervention may be initiated by visual observation or detection of an incident by a patrol officer during the conduct of a patrol tour since patrol officers monitor the entire site through random vehicle and foot patrols and building security checks 24 hours per day, 365 days per year. These checks are recorded electronically and downloaded to computer disk for review and storage. After normal work hours and on weekends and holidays, open offices and buildings are checked, secured, and reports of out of normal activity or unlocked facilities are provided to the specific building manager, project manager, and/or office occupant(s) the next work day. Written reports of incidents are provided to the SLAC Site Security manager for evaluation, further action, or other disposition. Non-security safety, fire, and equipment alarms are monitored and maintenance or emergency services are dispatched, as required, 24 hours per day, 365 days per year.

"For cause" searches of private vehicles leaving the laboratory are authorized by the laboratory director when sufficient reason exists to believe that SLAC/DOE property is being transported from the premises without approval.

In the event formal law enforcement intervention is required in response to an incident or activity, the San Mateo County Sheriff's Department, Redwood City, California, is notified by the SLAC Site Security manager and assistance is requested. The San Mateo County Sheriff's Department provides the full range of services of a sworn police department, which includes typical law enforcement, response to emergencies and criminal investigations as required.

2.4 Facilities And Equipment

References

DOE M 470.4-2, PHYSICAL PROTECTION, Chapter XII, Communications

Routine personal protective equipment is checked at the beginning of each shift.

3.0 PHYSICAL SECURITY

3.1 ACCESS CONTROLS

References

- DOE M 470.4-2, "Physical Protection"
  - Chapter II, "Protection of Nuclear Weapons, Components, Special Nuclear Materials, and Classified Information and Matter"
  - Chapter IV, "Security Areas"
  - Chapter XIV, "Posting Notices"
  - Chapter XV, "DOE Badge Program"

The SLAC perimeter boundary is defined by a chain-link fence or a multi-strand barbed wire fence. The lab perimeter has two vehicle entry points, the primary entrance to the laboratory located at 2575 Sand Hill Road, Menlo Park, and a secondary entry point on Alpine Road is designated for staff entry during commute hours.

The Stanford Guest House was opened in June 2003. This facility has 112 guest rooms available to members of the Stanford University community. SLAC is a part of the Stanford campus and those with proper identification are granted access upon checking in at the main gate. The overall site access procedures have not been impacted by this increase in non-SLAC visitors. The majority of the guesthouse occupants are SLAC scientific visitors, users, and collaborators, with an especially high population occurring during major conferences, meetings, reviews, and symposia. Other guests include individuals associated with other departments of Stanford University, families of patients being treated at Stanford Medical Center and Children's Hospital, and a variety of other Stanford-associated guests. Doors throughout the main campus are locked by Security Patrols between the hours of 1800 and 0600, which should prevent unauthorized access by Guest House residents.

The Accelerator Area (AA), which is similar to a working industrial site, is located within the laboratory boundaries and is protected with a 6-foot high chain link fence with barbed wire outriggers, which encompasses the entire area. A number of service gates are located in the AA fence line and are chained, locked, and patrolled on a daily basis by random vehicular patrols conducted by SLAC protective personnel.

Two internal gates provide vehicle entry points to the AA. The primary internal gate is currently staffed 24 hours per day, 365 days per year, and provides an entry point to the AA from the main campus area. The second SLAC AA gate is staffed Monday through Friday from 0600 to 1800 and also provides an entry point to the AA from the main campus area. Entrance into the AA requires the display upon entrance of the DOE common badge issued by Site Security, which reflects the individual's specific ES&H training level and status, that is, employee, scientific user, or contractor. SLAC is currently evaluating the installation of automated gates at the AA access points to reduce the amount of time that security officers and patrols will have to spend on safety access. These gates would be remotely controlled from the main Sand Hill Road Gate.

Visitors are issued a distinctive SLAC visitor badge indicating ESCORT REQUIRED while in the AA. All visitors require escort by a trained and badged SLAC employee, scientific user, or contractor. The surrounding terrain consists of rolling hills with minimal brush coverage and contains several main and secondary improved and unimproved roads. While penetration of the fence line would not be difficult, entry would require crossing several adjacent property areas that are also protected by fencing, all of which are open land making any crossing easily visible to adjacent property owners and mobile SLAC protective personnel.

SLAC's 2009 Security Risk Assessment has identified that additional improvements are needed to improve perimeter fencing and access in several areas. For related budget expenses to complete these improvements in FY'10 and FY'11, see Exhibit 5, line item FS1002-3.

3.1.1 Site Entry

Entry into the SLAC site is through one of two gates. The Sand Hill Road Gate is staffed 24 hours daily, 365 days per year, and entry requirements are contained in the gate procedures. The other gate, located on Alpine Road, is unlocked and staffed during morning and afternoon commute hours (0600-1000 and 1500-1800 Monday through Friday).

Stanford University operates a commercial bus shuttle service Monday through Friday between the Stanford campus and SLAC. This is a contract service and DOE common badge presentation is not required to board a shuttle bus or to enter the SLAC Main Gate location at Sand Hill Road. The pick-up and drop-off location is limited to the open areas in SLAC. Random visual screening of passengers is conducted by SLAC protective personnel. The shuttle operates from 0830 to 1800, Monday through Friday.

Individuals who enter or attempt to enter the SLAC main campus property without appropriate ID, sponsorship, or prior approval, after hours or on weekends or holidays are escorted off-site. Individuals who enter or who attempt to enter the controlled Accelerator Area without appropriate ID are refused entry and placed in contact with a person who can assist in determining the need and arranging for authority for entry. If no need exists, they are escorted off the site. Individuals who attempt re-entry after proper admonishment are subject to arrest for trespass by the San Mateo County Sheriff's Department.

3.1.2 Summary of Site-Wide Physical Protection Systems

Entry Control Systems

Building entry control for areas within the laboratory perimeter is done by restricted key hardware, lock-and-key sets at critical doors, and by several electro-mechanical locking systems coded with individual codes to permit entry to those areas protected by the system to authorized code holders only.

Metallic security keys are prepared using the Schlage master-key system with a restricted keyway. The SLAC Site Security manager administers the site key system. Records are maintained of all keys issued using the serialized key number and the key recipient's name, employment location, and department authorization signature. The key system is composed of five levels of access, from individual lock entry to the great grand master. The key system is maintained by a contract locksmith who installs and maintains the security key system.

For areas requiring a higher level of entry control, SLAC has installed OMNILOCK combination locks. Persons requiring entry into areas controlled by the OMNILOCK system require department approval. The SLAC Site Security manager installs, maintains, and audits the system, and installs and deletes all combination codes for authorized persons. A computer-based log system is used to monitor the use and assignment of codes.

3.2 INTRUSION DETECTION AND ASSESSMENT SYSTEMS

References

- DOE M 470.4-2, "Physical Protection"

3.2.1 Lighting

The focus of lighting on SLAC property is established to ensure safe operations. The lighting around the designated property protection areas has the added feature to enable assessment of unauthorized activities and/or persons at pedestrian and vehicular entrances. When required lights are found inoperative the protective force submits a Facilities Department service request. If the lighting is critical to safety or security the service request receives priority attention.

3.2.2 Video Cameras

Several locations on the site have been identified as having the need for higher than normal surveillance. Those areas have video camera protection connected to time-lapse video recorders. Live video camera coverage is also in place at the three pedestrian turnstile gates where DOE common badge photo ID cards and the person's face requesting entrance are compared by the Sector 30 gate officer prior to pressing the gate release switch for entry into the AA.

Areas where video cameras are in operation are posted. Below is sample of one of the signs.

Figure 3

SLAC's 2009 Security Risk Assessment has identified that additional improvements are needed to improve intrusion detection and monitoring through the use of CCTV and recording devices.

For related budget expenses to complete these improvements in FY10 and FY11, see Exhibit 5, line item FS1002-2.

3.3 Barriers and Delay Mechanisms

References

- DOE M 470.4-2, "Physical Protection"
  - Chapter II, "Protection of Nuclear Weapons, Components, Special Nuclear Materials, and Classified Information and Matter"
  - Chapter X, "Locks and Keys"
- DOE M 470.4-7, "Safeguards and Security Program References"

3.3.1 Physical Barriers

Physical barriers include not only the laboratory perimeter fence, but also areas inside the fence that are protected by walls, fences, or other restraints from unauthorized entry. The SLAC site has multiple protection levels based on a graded approach. Specific access requirements are located in the *SLAC Site Access and Identification Badges Policies and Procedures*. The areas are as follows.

- **Open Area.** Areas that are an extension of the Stanford University and are open to faculty, students and the public. These areas include
  - SLAC Guest House
  - Kavli Institute for Particle Astrophysics and Cosmology (KIPAC)
  - Panofsky Auditorium
- **Administrative Area.** Areas where access controls are established to protect the confidentiality, integrity, and availability of information that is primarily protected by the Privacy Act. These areas include
  - Business Services
  - Computer Center
- **Safety Areas**. Areas containing potentially hazardous equipment and materials that can pose a danger to an individual who has not had the proper training. These areas include
  - Industrial areas (e.g., manufacturing and testing facilities)
  - Accelerator Area
  - Radiologically controlled areas (RCAs)
  - Radiological areas within a RCA that is defined in 10 CFR 835
- **Property Protection Areas.** PPAs are established to protect government-owned property against damage destruction, or theft. Designated PPAs within the laboratory that may be at risk from groups or individuals identified in Chapter 2 have higher levels of physical protection and access controls. These areas include

- The Hazardous Waste Storage Facility
- The Radiological Calibration Facility, Building 24, Room 167

SLAC's 2009 Security Risk Assessment has identified that additional improvements are needed to improve barrier and delay mechanisms through the use of improved door access systems, such as badge readers for critical buildings. This includes 11 buildings on the main campus and the Main Control Center for the accelerator in the Accelerator Area.

For related budget expenses to complete these improvements in FY10 and FY11, see Exhibit 5, line item FS1002-4. This line item also includes the expenses of running the badging office.

3.4 TESTING AND MAINTENANCE

References

- DOE M 470.4-2, "Physical Protection", Chapter XIII, "Maintenance"

3.4.1 Testing and Maintenance

SLAC Site Security radio communications are checked three times per day at the beginning of each shift, plus a monthly site-wide test is conducted by the SLAC Network Operations / Wireless Department. The emergency telephone number is tested each morning. The lab public address system (not located in all buildings) is tested at least once a month by the responsible building manager and more often if maintenance is required. Deficiencies are reported to SLAC Network Operations / Wireless Department, or to SLAC Telephone Services for emergency telephone repair.

Fire alarms are tested on a random basis by the SLAC fire alarm technicians in the Facilities Department in conjunction with the Palo Alto Fire Department Engine 7 located on the site. The Controls and Power Electronics Department tests the system and equipment alarms. Deficiencies are detected through employee reports by monitoring daily alarm printouts provided to the SLAC Site Security manager. Repair and maintenance is performed by the Facilities Department.

Security and site lighting is inspected daily by the Assets Protection patrol officers, and defective lighting is reported to the Facilities Department three times weekly for repair or replacement as necessary.

The SLAC Main Gate backup generator is scheduled and tested periodically by technicians from the Facilities Department. Repair, if required, is done by a commercial company.

The electronically supported protective personnel tours of the SLAC site are conducted daily during all three shifts, and are recorded and downloaded into a database, which is transferred to a disk for storage and printed and reviewed by the contract site supervisor and the SLAC Site Security manager.

3.5 COMMUNICATIONS

The primary means of communications from all areas / facilities of the laboratory consists of a lab controlled and operated telephone switch connected to a local and long distance commercial telephone company. Supporting the primary system is a SLAC owned and operated mobile and hand-held radio communications system maintained by the SLAC Wireless Communications Office, SLAC Operations Directorate.

Continuous radio communications 24 hours per day, 365 days per year, is maintained between the Site Security fixed and mobile elements site-wide. Telephone calls from SLAC employees requesting non-emergency site security or law enforcement services are routed through non-emergency telephone connections to the Sand Hill Main Gate or the appropriate law enforcement agency.

All emergency 911 calls not dialed directly by the requester are routed via the SLAC emergency at the Main Gate by protective personnel to the Palo Alto Emergency Dispatch Center. This center then dispatches fire, ambulance, and law enforcement support as required. The radio frequency of the Palo Alto Emergency Dispatch Center is monitored by the Sand Hill Main Gate and the Site Security Operations Office for dispatch of SLAC patrol officers to escort emergency vehicles as required.

Additional emergency radio communications are maintained by the SLAC Main Control Center during active beam line operations, and the SLAC Maintenance Mechanics, both of which are monitored by the Sand Hill and Sector 30 gate officers. Service and maintenance of Site Security communications is the responsibility of the SLAC Network Operations / Radio Wireless Department, SLAC Operations Directorate. Frequencies are assigned by the US Government Frequency Management Agency and installed in SLAC radios by the SLAC Wireless Communications Department.

4.0 INFORMATION PROTECTION

4.1 Basic Requirements

References

- DOE M 471.3-1, "Manual for Identifying and Protecting Official Use Only Information"

4.1.1 Stanford Openness in Research Policy

This policy expresses Stanford's commitment to openness in research; defines and prohibits secrecy, including limitations on publishability of results; and specifies certain circumstances that are acceptable under this policy.

The principle of openness in research is one of overriding importance to Stanford University. Accordingly, no program of research that requires secrecy may be conducted, unless it meets one of the exceptions set out in the university's Openness in Research policy.

The openness checklist is used when reviewing all research conducted at SLAC:

- Requests for proposals or project solicitations
- Program award notices
- Non-disclosure agreements (NDAs)
- Any other documents related to research proposals, contracts, cooperative agreements, and other arrangements for sponsored research projects to assure that they do not require secrecy or impose unacceptable restrictions

In any proposals for research funding, Stanford will include standard language in its cover letter indicating the University's commitment to openness in research, and its intention to adhere to its policy in this regard. This policy provides a proactive approach to preclude sensitive unclassified or classified work from being conducted at SLAC.

Questions on the openness checklist include

- Does this project or agreement:
  - Contain language referring to or mandating compliance with export laws or regulations?
  - Restrict researcher participation (faculty, student, others) based on country of origin or citizenship?
  - Require researcher participation in US-citizen-only meetings?
  - Prohibit the hiring of non-US citizens to be involved in the proposed research?
  - Grant the sponsor a right of prepublication review for matters other than the inclusion of patent and/or proprietary sponsor information?
  - Provide that any part of the sponsoring, granting, or establishing documents may not be disclosed?

- Limit access to confidential data so centrally related to the research that a member of the research group who was not privy to the confidential data would be unable to participate fully in all of the intellectually significant portions of the project?

4.1.2 Sensitive Unclassified Information

Personnel Files and Data

SLAC employees who are entrusted with business confidential information pertaining to SLAC and Stanford University personnel and operations are required to protect it in accordance with federal and state privacy laws. This information includes personal, medical, and financial data. It is essential that this information be kept private or legally protected and that care is taken so that it is not accidentally or intentionally disclosed.

Handling and disposal of business confidential and private information is done in ways that ensures that it is not inappropriately or inadvertently disclosed. Business confidential information is not to be left in public view on desks or in other similar places. Hard copies of business confidential information should be shredded when one is finished working with them.

Employees are expected to review Stanford / SLAC policies on the use and handling of business confidential information and to maintain current knowledge of them. These include

- Administrative Guide Memo 15, *University Code of Conduct* (Section 8 and Section 13 in particular)
- Administrative Guide Memo 15.2, Section 2

Employees who are responsible for business confidential information are required to sign a confidentiality expectations and agreement memorandum.

Official Use Only

In general, SLAC does not generate any government official use only (OUO) information; however, from time to time DOE entities do provide OUO documents to SLAC staff. Once these OUO documents are received they are to be protected in accordance with DOE requirements.

These requirements include the following:

- Ensure that access to (a) documents marked as containing OUO information or (b) OUO information from such documents is only provided to those persons who need to know the information to perform their jobs or other DOE-authorized activities.
- Ensure that documents marked as containing OUO information are protected.
- Ensure that documents determined to no longer warrant protection as OUO have their markings removed.

Export Control

United States export controls exist to protect the national security and foreign policy interests of this country. Export controls govern the shipment, transmission, or transfer of certain sensitive items, information or software to foreign persons or entities. Where applicable, they may require authorization from the US Government in the form of an export license. Most of the items, information or software that Stanford ships or shares with its colleagues and research partners is not of a nature that would be restricted for these purposes, nor are they destined for countries or individuals subject to US embargoes or sanctions. Stanford however is required to exercise due diligence, and this decision tree has been crafted for the purpose of complying with US trade law while preserving one of Stanford's fundamental policies, openness in research.

A *foreign person* is anyone who is not a *US person*. A US person is a citizen of the United States, a lawful permanent resident alien of the US (a *green card holder*), a refugee, protected political asylee or someone granted temporary residency under amnesty or Special Agricultural Worker provisions. The word *person* includes organizations and entities, such as universities. The general rule is that only US persons are eligible to receive controlled items, information or software without first obtaining an export license from the appropriate agency.

To determine if an export control license is needed Stanford has developed an export control decision tree. Employees must follow this decision tree.

The questions in this decision tree use terminology derived from the regulations of the US Departments of State, Commerce, and Treasury. These questions ask about sharing, shipping, transmitting or transferring any items, information or software. Violations of these export control regulations can lead to significant civil and criminal penalties.

- *Items* refers to any *tangible things, equipment or hardware.*
- *Information* can include *technical data* such as models, formulae, engineering designs and specifications, or *technical assistance* such as training or instruction.
- *Software* refers to a collection of one or more *computer programs or microprograms* in either *source code* (programming statements) or *object code* (machine-readable instructions).

The conduct, products, and results of *fundamental research* are generally **excluded** from federal *deemed export* controls – that is, disclosure of information to foreign nationals on US soil – in accordance with National Security Decision Directive 189.

4.1.3 Site Security Records Management

The Site Security records management program for SLAC is composed of receipt and retention of all permanent log books prepared by each officer, daily reports of investigations and incidents, the tracking of incidents (including traffic violations) in a database, and maintenance of electronic access records on the entry system. SLAC does not have nor maintain any records regarding security clearances held by any SLAC person, scientific user, contractor, or visitor. Records management beyond that indicated here is deemed not appropriate for this facility.

4.2 Technical Surveillance Countermeasures

Not applicable

4.3 Operations Security

Applies to information regarding shipments of Nuclear Material and travel itineraries of SLAC senior management and dignitaries including Heads of State to and from the SLAC Site apply. Review of such events on a case-by-case basis in concert with SLAC's DOE Site Security representative will insure that necessary levels of OPSEC will be applied to such information and will be coordinated with other Federal, State, and International Agencies if appropriate.

4.4 Classification Guidance

Not applicable

4.5 Classified Matter Protection and Control

Not applicable

5.0 CYBER SECURITY

5.1 Classified Cyber Security

Not applicable

5.2 Telecommunications Security

Not applicable

5.3 Unclassified Cyber Security

References

- DOE O 205.1A, "Department of Energy Cyber Security Management"

The certification and accreditation (C&A) process as defined in the Guide for the Security Certification and Accreditation of Federal Information Systems (NIST 800-37) certifies that SLAC's information systems meet documented security requirements. The C&A documents are continually updated to ensure that everyone understands the current operational risks.

Authority To Operate (ATO) for the Certification and Accreditation (C&A) packaged was approved in January 2008.

Budget request for FY 2010 includes cyber security enhancements to close outstanding POA&Ms for network re-architecture. These items were requested in funding for FY 2009 and not funded, even though both the SAV and the SAR mentioned this as a weakness. One advantage for a delay in the implementation is the potential move of the Human Resource system, which contains contractor records with protected PII, to the direct purview of the contractor, Stanford University. Also included in the FY10 budget request is funding for increased effort in compliance and self-assessment, maintaining policies and procedures consistent with SLAC standards and closing POA&Ms relative to log analysis and host-based intrusion detection.

Budget request for FY 2011 includes cyber security enhancements to close POA&M for network based intrusion detection in a manner that allows for data transfers at maximum speeds so as to not interfere with the scientific mission of the lab. Additional staffing is required for forensics analysis of systems where the intrusion detection has raised suspicions of malicious activity.

For related budget expenses, see Exhibit 5, line item FS1005-3 through 5.

6.0 PERSONNEL SECURITY

6.1 ACCESS AUTHORIZATIONS

References

- DOE M 470.4-2, "Physical Protection", Chapter XV, "DOE Badge Program"
- DOE N 206.4, "Personal Identity Verification"

6.1.1 Site Access and Identification Badges

SLAC does not conduct classified research and does not maintain security clearances. SLAC is a Threat Level IV facility as defined in the 2004 Design Basis Threat (DBT) document. No classified information is generated under the Stanford contract or maintained on the SLAC site. SLAC does not issue the DOE standard security badge. SLAC was approved for the use of the Office of Science common badge. The primary purpose of the SC common badge is as a site access and identification badge for safety and administrative purposes and not for security access.

SLAC has many areas containing potentially hazardous equipment and materials that pose a danger to an individual who has not had the proper training to recognize those hazards. Therefore, access to certain areas at the laboratory is limited to those who have had the appropriate training, or are escorted by someone who has. The specifics details are contained in the Site Access and Identification Badges Policy and Procedures.

6.1.2 Security Clearances Sponsored by Others

A limited number of SLAC staff hold security clearances sponsored by another organization (DOE, DOD, DOS) for work performed by that staff member for that organization. Such work is not performed on the SLAC site and no classified documents are kept on the SLAC site. Any SLAC staff member holding a security clearance sponsored by another organization for work performed on behalf of that organization is subject to the requirements placed upon them by that organization and they are personally responsible for compliance therewith. The sponsoring organization is responsible for oversight of individuals and is responsible for ensuring that they are aware of and in compliance with the rules, regulations and procedures pertaining to their clearance and for obtaining any approvals required in conjunction with the security clearance.

6.2 HUMAN RELIABILITY PROGRAM

Not applicable

6.3 CONTROL OF CLASSIFIED VISITS

Not applicable

6.4 Safeguards and Security Awareness

References

- DOE M 470.4-1, "Safeguards and Security Program Planning and Management", Part 2, Section K, "Safeguards and Security Awareness Program"
- DOE O 475.1, "Counterintelligence Program"
- DOE O 551.1C, "Official Foreign Travel"

The rationale behind counterintelligence is that knowledgeable, aware employees are the key to identifying and preventing foreign intelligence and terrorist activities. Although SLAC does not conduct classified work or store classified information, the DOE Counterintelligence Office encourages employees and guests to report suspicious behavior that may involve foreign intelligence efforts or other inappropriate attempts to gather information.

SLAC conducts security education briefings as part of the new employee orientation and during the annual security and safety briefings.

The Security Manager maintains a close liaison with the DOE Counterintelligence Officer assigned to SLAC as well as other appropriate DOE, Federal, and State agencies. This ensures that any incidents or occurrences that may have counterintelligence implications are immediately addressed with the SLAC Directorate and SLAC Site Office.

Counterintelligence briefings are covered in the foreign visits and assignment section.

7.0 UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS

References

- DOE O 142.3, "Unclassified Foreign Visits and Assignments"

7.1 UFVA PERSONNEL RESPONSIBILITIES

The flowchart on the following page gives a detailed representation of the process followed at this facility for implementing DOE Order O 142.3.

The key individuals responsible for this process work in the following areas:

- FACTS Office – Business Systems and Laboratory Support Department
- Employment Office – Human Resources Department
- International Services – Human Resources Department
- Records Office – Human Resources Department
- SLAC Users' Office (SLUO) – Particle and Particle Astrophysics Directorate
- SSRL Users' Office – Photon Science Directorate

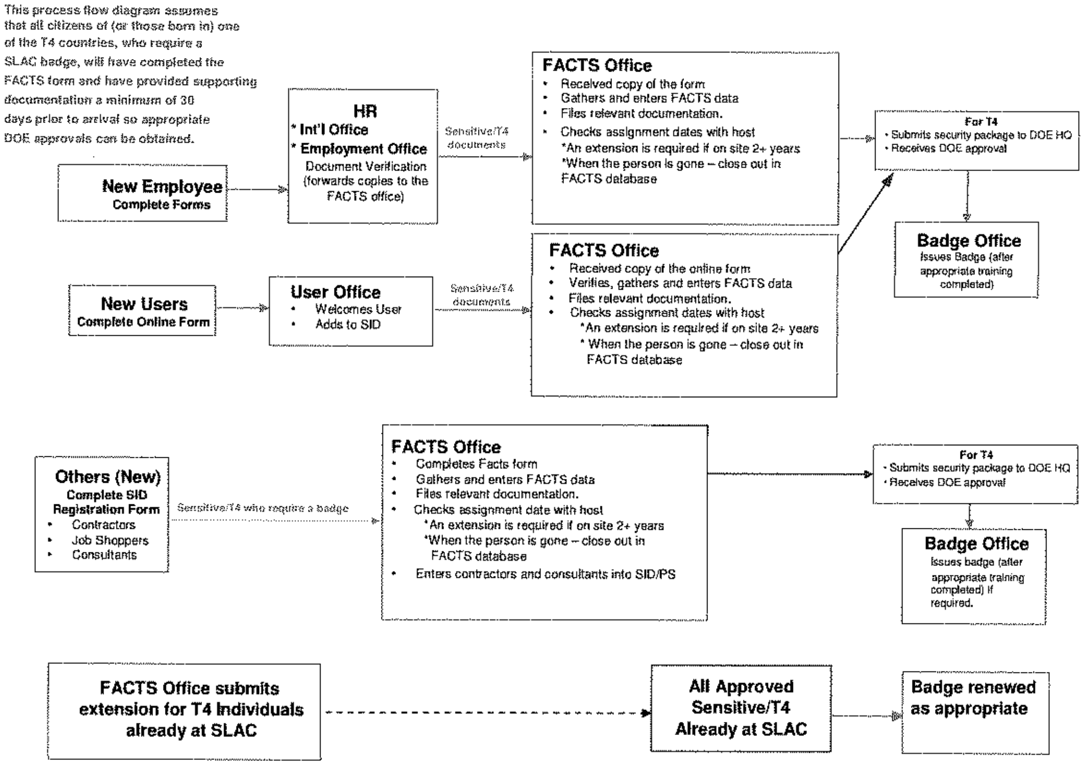

This process flow diagram assumes that all citizens of (or those born in) one of the T4 countries, who require a SLAC badge, will have completed the FACTS form and have provided supporting documentation a minimum of 30 days prior to arrival so appropriate DOE approvals can be obtained.
New Employee
Complete Forms
HR
* Int'l Office
* Employment Office
Document Verification (forwards copies to the FACTS office)
Sensitive/T4 documents
FACTS Office
• Received copy of the form
• Gathers and enters FACTS data
• Files relevant documentation.
• Checks assignment dates with host
*An extension is required if on site 2+ years
*When the person is gone – close out in FACTS database
For T4
• Submits security package to DOE HQ
• Receives DOE approval
Badge Office
Issues Badge (after appropriate training completed)
New Users
Complete Online Form
User Office
• Welcomes User
• Adds to SID
Sensitive/T4 documents
FACTS Office
• Received copy of the online form
• Verifies, gathers and enters FACTS data
• Files relevant documentation.
• Checks assignment dates with host
*An extension is required if on site 2+ years
* When the person is gone – close out in FACTS database
Others (New)
Complete SID Registration Form
• Contractors
• Job Shoppers
• Consultants
Sensitive/T4 who require a badge
FACTS Office
• Completes Facts form
• Gathers and enters FACTS data
• Files relevant documentation.
• Checks assignment date with host
*An extension is required if on site 2+ years
*When the person is gone – close out in FACTS database
• Enters contractors and consultants into SID/PS
For T4
• Submits security package to DOE HQ
• Receives DOE approval
Badge Office
Issues badge (after appropriate training completed) if required.
FACTS Office submits extension for T4 Individuals already at SLAC
All Approved Sensitive/T4 Already at SLAC
Badge renewed as appropriate

Figure 4.

7.2 The Stanford Synchrotron Radiation Lightsource (SSRL) Procedure

SSRL follows an identical process, with the exception that SSRL has a designated individual who manages the data input (while the rest of SLAC is handled by the Business Services Division).

7.3 Liaison with DOE Counterintelligence Representative

SLAC maintains a close liaison with the DOE counterintelligence representative assigned to SLAC and the DOE Safeguards and Security and other appropriate federal and state agencies. This ensures that concerns of the DOE regarding specific incidents or occurrences that may qualify as matters of counterintelligence interest will be addressed with the SLAC directorate and all others involved in this area.

The primary activity to support this program is conducted by personnel within the Business Services Division. For related budget expenses, see Exhibit 5, line item FS1006-5.

8.0 NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY

References

- DOE M 470.4-6, "Nuclear Material Control and Accountability"
- DOE O 5660.1B , "Management of Nuclear Materials" [note: not in current contract]

8.1 MATERIAL CONTROL AND ACCOUNTABILITY PROGRAM

SLAC's Material Control and Accountability (MC&A) program applies only to Category IV Special Nuclear Material (SNM). The Environment, Safety, and Health (ES&H) Division is responsible for management of that program. The SLAC *ES&H Manual* contains the MC&A program description. Within ES&H, health physicists and radiation technicians have the overall responsibility for control and monitoring of SNM. Authority is delegated as appropriate to the radioisotope monitors and others in ES&H, as required, to account for and safeguard SNM the details of which are disseminated by the appointed nuclear material representative.

8.2 NUCLEAR MATERIAL REPRESENTATIVE

This person is responsible for the control and accountability for nuclear materials, as prescribed in DOE Manual 470.4-6. The nuclear material representative tasks the SLAC protective force for the following support:

- Notifies the SLAC protective force through the SLAC Site Security manager of the arrival and placement into secure storage or secure experimental facility of each nuclear material shipment
- Provides a schedule of experimentation, including the commencement and termination dates of the experiment and the scheduled departure time of the nuclear material from SLAC via approved courier
- Provides additional information during the time the nuclear material is on the SLAC site regarding any movement, transfer, receipt of additional nuclear material, or shipment of the on-site nuclear material from SLAC

8.3 SLAC PROTECTIVE PERSONNEL

The SLAC protective personnel notifies the nuclear material representative of the arrival of the special courier, and provides a vehicle and a patrol officer for escort of the nuclear material courier from the Sand Hill Road Main Gate to SLAC Shipping and Receiving. The patrol officer remains with the vehicle and driver pending arrival of the SLAC nuclear material representative at Shipping and Receiving.

Escort to the designated secure storage area or to the secure experimental facility is provided. Once secure, an hourly check by a patrol officer is undertaken to confirm the integrity of the storage area or experimental facility. This check consists of a visual observation of the exterior of the facility for signs of unauthorized entry, and a physical facility check including door and window lock status.

Throughout the conduct of the experiment, any personnel inside the experimental facility are verified as authorized by the patrol officer conducting the check. The check is logged on a special check sheet provided by the nuclear material representative, and continues 24 hours a day, seven days a week until the nuclear material is removed from the SLAC site via authorized special courier.

Any deviation of physical security integrity will cause an immediate securing of the facility and the generation of an immediate report by the most expeditious means to the nuclear material representative. All logs and reports (if any) are turned over to the nuclear material representative for record purposes.

For related budget expenses, see Exhibit 5, line item FS1001-8.

Exhibit 1 Acronyms and Abbreviations

AA	Accelerator area
AFSO	Alternate facility security officer
Att.	Attachment
CH	Office of Science – Chicago
CSP	Cyber security plan
DOE	Department of Energy
ECI	Export controlled information
FCL	Facility clearance
FDAR	Facility data and approval record
FSO	Facility security officer
GSA	General services administration
GSP	Graded security protection
ISSM	Information systems security manager
ISSO	Information systems security officer
MBA	Material balance area
MC&A	Materials control and accountability
NMC&A	Nuclear materials control and accountability
NMMSS	Nuclear Materials Management and Safeguards System
OPSEC	Operations security
ORO	Oak Ridge Office
OUO	Official use only
PIN	Personal identification number
PPA	Property protection area
S&S	Safeguards and Security
SNM	Special nuclear material
SSIMS	Safeguards and Security Information Management System
SSP	Site security plan
UCI	Unclassified controlled information

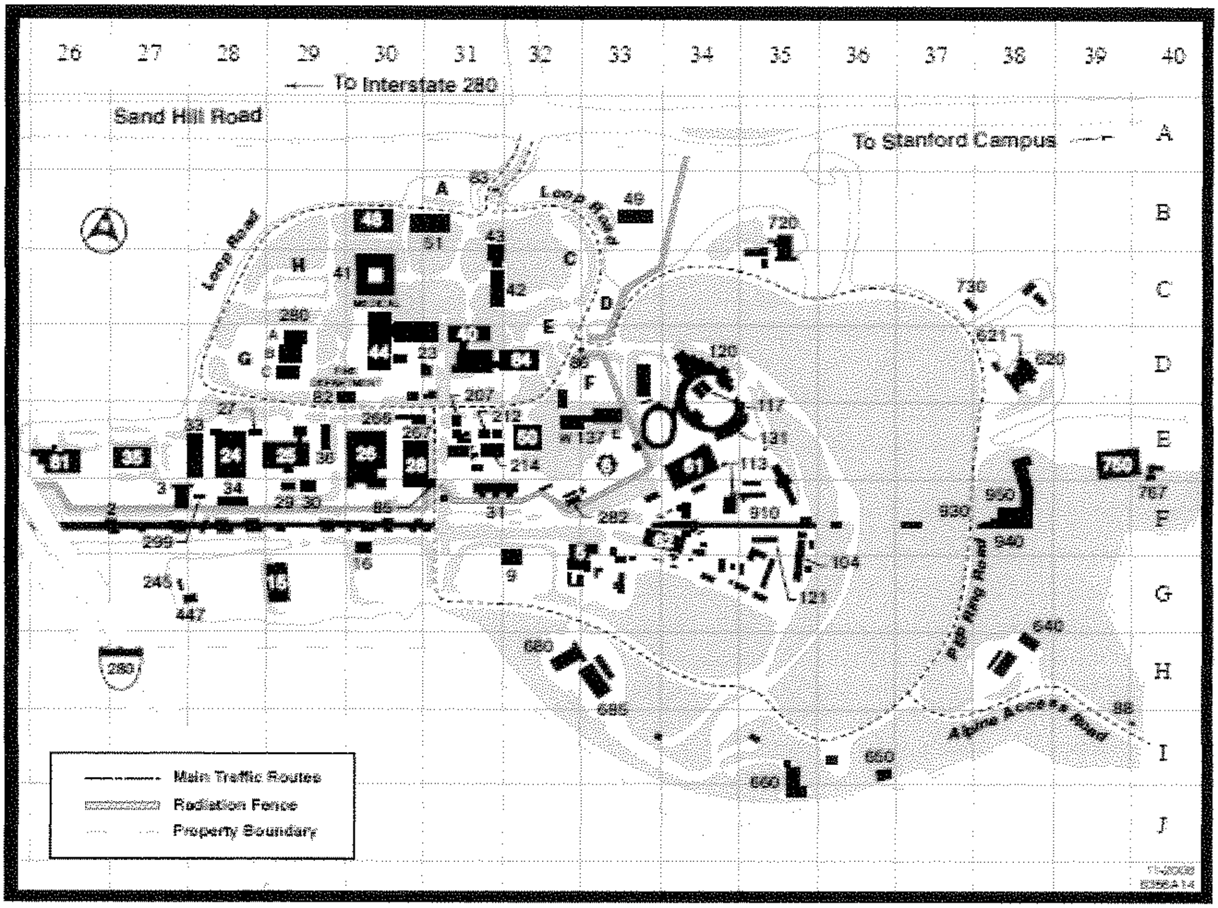
Exhibit 2 Site Security Program Responsibilities

Name	Position/Function(s)	Phone
Simon Ovrahim	FSO	650-926-2310
Simon Ovrahim	Inquiry Official	650-926-2310
Robert Cowles	ISSM	650-926-4965
Gary Buhrmaster	ISSO	650-926-4965
Marilyn Cariola		650-926-2820
Chris Mayfield		650-926-4598
Heather Larrieu		650-926-4127
Robert Cowles	CSM	650-926-4965
Jim Allen	NMCA Manager	650-926-4064
Brian Sherin	Deputy Director ES&H, Risk Assessment and Response Manager	650-926-5082
Craig Ferguson	Director ES&H	650-926-3106
Doug Kreitz	Foreign Visits and Assignments	650-926-2310
Robert Cowles	Cyber Security	650-926-4965
Sandy Merola	Associate Lab Director, Operations (COO)	650-926-4482

Exhibit 3 References

- DOE O 142.3, Chg 1, "Unclassified Foreign Visits and Assignments"
- DOE P 205.1, "Departmental Cyber Security Management Policy"
- DOE O 205.1A, "Department of Energy Cyber Security Management"
- DOE M 205.1-5, "Cyber Security Process Requirements Manual"
- DOE N 206.4, "Personal Identity Verification"
- DOE O 221.1, "Reporting Fraud, Waste and Abuse to the Inspector General"
- DOE O 221.2, "Cooperation with the Office of Inspector General"
- DOE O 226.1A, "Implementation of Department of Energy Oversight Policy"
- DOE 413.3A, "Program and Project Management for the Acquisition of Capital Assets"
- DOE G 413.3-2, "Safeguards and Security for Program and Project Management"
- DOE M 413.3-1, JDReilly@lbl.gov
- DOE P 470.1, "Integrated Safeguards and Security Management (ISSM) Policy"
- DOE M 470.4-1, Chg-1, "Safeguards and Security Program Planning and Management"
- DOE M 470.4-2, Chg 1, "Physical Protection"
- DOE M 470.4-6, Chg 1, "Nuclear Material Control and Accountability"
- DOE M 470.4-7, "Safeguards and Security Program References"
- DOE G 471.3-1, "Guide to Identifying and Protecting Official Use Only"
- DOE M 471.3-1, "Manual for Identifying and Protecting Official Use Only"
- DOE O 471.3, "Identifying and Protecting Official Use Only Information"
- DOE O 475.1, "Counterintelligence Program"
- DOE O 551.1C, "Official Foreign Travel"
- DOE O 5660.1B, "Management of Nuclear Materials"
- DEAR (48 CFR) § 952.204-73, "Facility Clearance (Solicitation) (2002)"
- DEAR (48 CFR) § 904.404(d), "Solicitation Provision and Contract Clause"

Exhibit 4 Facility Layout



SLAC Area Map

	Building Number	Grid Number
Administration and Engineering Building (A&E)	41	30-C
Alpine Gate Guard House	68	40-I
Auditorium and Visitor Center	43	31-C
Auxiliary Control Building	3	27-F
Beam Switch Yard Access	9	32-G
Cafeteria	42	31-C
Central Hazardous Waste Management Area	245	27-G
Central Laboratory	40	31-D
Central Laboratory Annex	84	32-D
Central Utility Building	23	31-D
Chemical Storage Building	38	29-E
Cleaning Facility Building	30	29-F
Collider Experimental Hall (CEH)	750	39-E
Communications Office	266, 267	30-E
Computer Building (SCS)	50	32-E
Controls Building	34	28-F
Cryogenics Laboratory	6	33-E
End Station A (ESA)	61	34-E
End Station B	62	34-F
Environmental Protection Restoration	299	28-F
Environmental Safety and Health (ES&H)	24	28-E
Exercise Room/Shops Dining Room	27	28-E
Experimental Facilities Department Shops (EFD)	104	35-F
Fire Station	82	30-D
Gate 17 Guard House	86	33-D
General Services Building (Shipping & Receiving)	81	28-E
Guest House	49	33-B
Hazardous Waste Storage Area	447	28-G
Heavy Fabrication Building	26	30-E
Kavli Building	51	31-B
Klystron Gallery (Visitors Alcove, Sector 27)	2	27-F
Laboratory Offices and Shops (LOS)	137	33-E
LCLS Beam Transport Hall	910	33/34/35-F
LCLS Far Hall Tunnel Entrance	757	40-E

	Building Number	Grid Number
LCLS Near Hall	930/940/950	37/38-F
Light Assembly Building	33	28-E
Light Fabrication Building	25	29-E
Main Control Center (MCC)	5	32-F
Main Gate (Information Booth)	83	31-B
Master Substation	16	30-F
Medical (A&E)	41	30-C
Metal Stores Shelter	29	29-F
Parking Lots	A and C to H	
PEP Beam Facility/SSRL	650	36-I
PEP Beam Facility/SSRL	730	37-C
PEP Control Room	685	33-H
PEP Interaction Region 2 (IR-2)	620	38-D
PEP Interaction Region 4 (IR-4)	640	38-H
PEP Interaction Region 6 (IR-6)	660	35-I
PEP Interaction Region 8 (IR-8)	680	32-H
PEP Interaction Region 12 (IR-12)	720	35-B
Physics and Engineering Building	280	29-D
Plant Maintenance and Utilities	35	27-E
Power Conversion	15	29-G
Research Office Building (ROB)	48	30-B
Safeguards and Security	267	31-E
Sector 30 Guard House	85	31-F
SLC Engr. Trailer South (Fort Apache)	282	32-F
SLC Offices	212/214	31-E
SPEAR Control Room	117	34-D
Stanford Synchrotron Radiation Lab (SSRL)	120	34-D
Stanford Synchrotron Radiation Lab (SSRL)	131	34-E
Test Beam Facility	121	35-F
Test Laboratory	44	30-D
User Offices/Warehouse	28	30-E
Vacuum Assembly Building	31	31-F
Visitor Center	43A	31-C
Warehouse/User Offices	28	30-E