Contents

SECTION II – PROTECTION PLANNING

1.0 INTRODUCTION

A. Security assets must be protected from theft or diversion, sabotage, espionage, or loss, and other hostile acts which could cause unacceptable adverse impacts on national security, program and mission continuity, or harm to the health and safety of employees, public, or the environment. [Requirement 9-2001]

B. DP-PO Program Office, DP-PO-PA Planning and Analysis, SO-SS Security Systems and Physical Security will introduce relevant Site Security Plan (SSP) criteria during project design/planning which may require integration of other Safeguards and Security (S&S) groups in defining additional requirements for ensuring compliance with established S&S protection strategies.

2.0 PLANNING

A. Protection planning can be more economically integrated within buildings and structures during the early planning and design phases. Design basis threat may change over the life of a project, which could increase or decrease the scope of the project necessitating the implementation of appropriate change controls.

B. A graded approach is used to establish levels of protection in accordance with the potential risks to national security and the health and safety of employees and the public.

C. Protection planning must be based on the adversary capabilities outlined in the design basis threat (DBT) and the results of security risk assessments (SRA) and vulnerability assessments (VA), as applicable. [Requirement 9-2002]

D. DP-PO-PA Planning and Analysis performs VAs and SRAs to identify facility assets; threats; threat capabilities; facility and operational protection characteristics; and provides risk analyses in report form to offer recommendations for further risk mitigation.

E. SO-SS Security Systems will define the requirements for the design and installation of PACS and other security system requirements.

F. SO-SS Physical Security will define the requirements for physical protection strategies and measures to be integrated into the design.

G. For projects such as General Plant Projects (GPP), Major Item of Equipment (MIE), Capital Equipment, and Expense (not an inclusive list) seek security input at the earliest possible time in the design process.

1. DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security, and other security subject matter experts (SMEs) are involved in the development of scope definition and requirements document (SDRD), requirements and criteria document (RCD), risk analysis, cost estimates and schedules (list not inclusive).

2. DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security, and other security subject matter experts (SME) are involved in the conceptual design, design reviews, construction of projects and commissioning.

3. A formal security review of the design must be performed before actual construction or modification begins.

H. For line-item projects, seek security involvement prior to CD-1. [Requirement 9-2003]

1. S&S requirements for the recommended alternative and preliminary identification of alternatives (including facility design and the incorporation of S&S technologies) must be made and evaluated with respect to their impact on mission needs, satisfaction of other requirements (such as safety requirements) and other cost considerations.

2. A preliminary SRA must be conducted that accounts for the set of applicable safeguards and security requirements, evaluates the methods selected to satisfy those requirements and address any potential risk acceptance issues.

3. The project execution plan (PEP) and performance baseline (PB) must be reviewed to ensure that cost, schedule, and integration aspects of S&S are addressed, all feasible risk mitigation has been identified and concerns for which explicit line management risk acceptance will be required are appropriately supported.

4. Prior to CD-3, a final SRA report should be issued addressing all the S&S requirements of the project. The project requirements should be satisfied by the facility design or the proposed operational features.

Guidance: Contact DP-PO-PA Planning and Analysis in determination if SRA and/or VA are necessary. E-mail: va-team@lanl.gov

3.0 PROJECT INITIATION

A. The project is responsible for initiating review of the project for S&S requirements.

B. The project should also submit a SECURITY PROJECT REQUEST FORM, link located on the Defense Protection organization home page. This starts the process of walk downs and meetings to understand the project and assign appropriate S&S SMEs.

C. Project Activity and Review submissions will also notify S&S, but often the PAR is generated later than recommended to ensure S&S requirements are integrated during the early planning phases.

4.0 UPGRADING AND DOWNGRADING SECURITY AREAS

A. Refer to LANL Policy P202-1 *Security Areas and General Access Areas* section 5.3.1 Upgrading and Downgrading Security Areas.

B. Retrofits of existing facilities pose a greater challenge because building systems must be able to accommodate increased requirements and may not have the additional space or compatibility to upgrade systems capabilities. Designs should include the ability to increase security in response to a heightened threat, as well as to reduce security if changes in risk warrant it.

5.0 VULNERABILITY/SECURITY RISK ASSESSMENT

A. SRAs and VAs are executed to support the development of the LANL site security plan (SSP) and upgrades, and downgrades of the security posture in accordance with all applicable driving documents, including but not limited to DOE O 473.3C, Design Basis Threat (DBT), DOE O 470.4C, Safeguards and Security Planning, and NNSA Supplemental Directive (SD) 470.4-2 Implementation Instructions.

B. DOE O 470.3C, Design Basis Threat (DBT) defines the physical protection strategies for departmental assets at LANL by establishing procedures for implementation of DOE O 470.4C Safeguards and Security Planning. DBT prescribes the performance metrics for protection of nuclear weapon components (SNM Cat II or higher quantities) and provides adversary capabilities for planning purposes used in security risk analysis for other departmental assets (including classified mater, radiological material, chemicals, biological agents, select agents and toxins, critical infrastructures, government property, and personnel from malevolent acts).

C. LANL uses the DBT-established performance criteria for equivalencies and exemptions from current DOE polices.

D. The results of the completed analyses are documented in the vulnerability analysis report (VAR), material roll-up analysis, and security risk analysis. Risk analyses are submitted to NNSA to ensure risk-accepting officials are informed of security risk and to use as a risk-management foundation for security planning at LANL.

E. The security plan and supporting analysis must be reviewed and the following changes must be incorporated into the security plan. The ODFSA must approve these changes prior to implementation. [Requirement 9-2004]

1. Changes in risk or authorization basis
2. Planned changes to the security program at the facility or site
3. Changes in operations to include (but not limited to) addition of assets, modification of assets, or asset removal not covered by security plans at a facility or site that require modification to approved security measures.

6.0 PROJECT EXECUTION

A. During the project execution phase security SMEs (e.g., DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security; not an all-inclusive list) shall participate in the following project phases:

1. Planning or Project Initiation

   Support development of goal, objective, design, development of capability gaps, high-level project parameter, rough order of magnitude (ROM) cost range and schedule estimates for security attributes as needed.

2. Conceptual Design

   Support development of engineering studies, pre-conceptual designs, SDRD, Functional Requirements Document (FRD), RCD and Design Criteria for ensuring that the appropriate physical protection measures are integrated into the project documents.

3. Design

   Support development of preliminary, conceptual and/or detailed design of required physical security features. Participate in design reviews (30/60/90/100) including project drawings, project specifications and other contract documents which may be developed for the project.

Security SMEs must review project drawings to ensure requirements are incorporated into design and project specifications to ensure intent is maintained in revision of LANL master specifications.

4. Start-up and commissioning planning

   For any security system the project must coordinate with DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security in development of the Test and Acceptance Plans and/or any Commissioning Plan developed for the project to assure that passive and active security systems will be inspected, tested, and accepted in an appropriate and thorough manner.

   (Note, ESM Ch. 15, Commissioning Rev. 1 excludes security scope)

5. Construction Phase

   Support any design change forms (DCFs) and request for information (RFIs). Conduct intermediate and final inspections of physical security features and general construction during construction of the facility. Coordinate with DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security for appropriate SME input and participation in the inspections of security systems or components being installed.

6. Project Closeout

   Support development of lessons learned, project documentation, and other activities as appropriate.

7.0 COMMISSIONING, READINESS, AND VALIDATION OF SECURITY SYSTEMS

A. Commissioning

Conduct or witness any tests of passive and active physical security features or systems required by the Commissioning Plan. Coordinate testing with involvement of DP-PO, DP-PO-PA, SO-SS Security Systems and Physical Security.

B. Acceptance Testing (Activation Validation and Cutover (AVCO)/Site Acceptance Test (SAT)):

Acceptance testing for all physical protection systems, in conformance with the manufacturer's specification must be performed prior to acceptance of the installed system and include the following: [Requirement 9-2005]

1. Must include all sensors, equipment and devices
2. Verify the system was installed as designed
3. Verify the alarm station(s) or CAS/SAS receive alarms as designed
4. Verify assessment is accomplished as designed
5. Verify response is initiated as designed

AVCO/SAT plans are used to authenticate the acceptance criteria for the verification of security systems. Acceptance criteria are organized in tabular form and uniquely identified as steps. Each step is performed and results compared against system operability requirements. Successful completion of the steps concludes the verification process and serves as ground for acceptance of the security system(s). Development and execution of the AVCO/SAT plan is supported by DP-PO, SO-SS Security Systems and Physical Security.

C. Readiness Activities

Participate upon request from the project manager of the project, as the Project Security Representative and SMEs in any Readiness Review or Assessment required for project closure, acceptance for safe startup of operations, and facility turnover.

8.0 RECORD OF REVISIONS

Rev	Date	Description	POC	Resp. Mgr.
6	05/06/2026	Split chapter into three main documents and standalone design/construction tables with Section III. See Section I for complete chapter history.	Tina Vigil, *SO-SS*	Michael Richardson, *ES-DO*