

University of California
Office of the President

Guidance for Integrated
Safeguards and Security Management
Gap Analysis

INTRODUCTION

The University of California (UC) has agreed to accomplish certain goals set forth in Appendix O, Paragraph 2.2 of the Management and Operating contracts with the Department of Energy (DOE) concerning the establishment of an Integrated Safeguards and Security Management (ISSM) system.¹ UC's methodology for achieving this goal is set forth in this document.

The purpose of the Gap Analysis and the methodology described herein is to determine the status of the progress that has been achieved by each Laboratory in the course of creating a fully implemented ISSM system. As noted in Element 2 of the ISSM document "Minimum ISSM Framework Elements to Declare ISSM is In Place, (SSMIT)," the desired end state is one in which "DOE and contractor organizations have self-assessed their ISSM system using ISSM expectations and attributes to determine the status of implementation. Implementation gaps are identified and addressed." The Gap Analysis will lead to an Action Plan for each Laboratory in sufficient detail to identify the required actions, establish anticipated resource requirements and validation techniques, and determine completion dates for each of the identified actions in ISSM implementation.

UC's ISSM VISION

UC's vision for ISSM is that it is an overarching system framework within UC and at LANL and LLNL based upon ISSM's objective and guiding principles. We expect the ISSM framework to promote employee "ownership" and management leadership, commitment and accountability for security while fostering scientific excellence.

UC has no greater responsibility to the Nation than ensuring the protection of critical and sensitive national security assets in the possession of its Laboratories. It is equally important that this objective is achieved in a manner that recognizes the University's commitment to maintaining the principles of intellectual freedom and due process. The fundamentals of ISSM represent a means of accomplishing this.

¹ References to "ISSM," "S&S Program" or "security" used herein are intended to include all security related elements, e.g., cyber, personnel, physical, MC&A, counterintelligence, etc.

UC will ensure that the ISSM framework is integrated with the Laboratories' missions in a manner that maximizes scientific inquiry and gains broad-based support from its employees.

APPROACH

In response to the requirements of Appendix O, UC management convened a workshop with representatives from UC, LANL, LLNL and Aegis Research Corporation to establish the process, schedule, and responsibilities of the parties. Consistent with Appendix O, it was agreed that the seven guiding principles for ISSM, enumerated in DOE P 470.1 (Component 2), best describe the mature status of an "in-place" ISSM system (*i.e.*, the end state). Taken together, these seven guiding principles characterize a management system that will systematically integrate S&S into management and work practices at all levels so that missions are accomplished securely. Criteria intended to guide the Labs in better defining desired ISSM "end state" qualities were developed. The criteria are linked to one or more guiding principles with at least one criterion identified for every guiding principle.

The status of Laboratory implementation of ISSM relative to the criteria will identify the gaps. The gaps should be analyzed and described in sufficient detail to provide the scope and effort of the work to be done toward achieving Element 2 of the SSMIT "In Place" criteria, and they will form the basis of the Lab-specific Action Plans.

The seven guiding principles that correspond to the numbers in the matrix, below, are:

1. **Individual Responsibility and Participation**: Each individual is directly responsible for following security requirements and contributing to secure missions and workplaces.
2. **Line Management Responsibility for Safeguards and Security**: Line management is directly responsible for the protection of the DOE assets. Appropriate risk analysis is performed prior to work being authorized. Residual risk must be accepted by line management and controls must be in place and verified prior to authorization of operations.
3. **Clear Roles and Responsibilities**: Clear and unambiguous lines of authority and responsibility for ensuring S&S must be established and maintained at all organizational levels within the contractor's organization.
4. **Competence Commensurate with Responsibilities**: Individuals must possess the experience, knowledge, skills and abilities necessary to fulfill their responsibilities.

5. **Balanced Priorities**: Resources must be effectively allocated to address safeguards and security, programmatic, and operational considerations, realizing that achieving programmatic goals is a significant component of achieving safeguards and security. Protecting the DOE assets must be a priority whenever activities are planned and performed.

6. **Identification of S&S Standards and Requirements**: Before work is performed, the associated risk must be evaluated, and an agreed-upon set of safeguards and security standards and requirements shall be established that, if properly implemented, will provide appropriate assurance that DOE assets, the worker, the public, and the environment are protected from adverse consequences.

7. **Tailoring of Protection Strategies to Work Being Performed**: Administrative and engineering controls to prevent and mitigate risk must be tailored to the work being performed.

The matrix below lists the criteria and identifies the guiding principles to which the criteria apply.

Matrix of Criteria to Guiding Principles

		Guiding Principles						
	Criterion	1	2	3	4	5	6	7
A	Each worker understands and accepts responsibility for performing work securely.	X		X	X			
B	Workers are actively involved in providing feedback and improving the security of their work and workplace.	X		X				
C	Managers understand and accept their S&S responsibilities.	X	X	X	X			
D	Managers ensure that only appropriately competent staff is authorized to perform specific work assignments, identify additional training and education needed to maintain competence, and hold staff accountable.		X	X	X			
E	Managers ensure necessary and sufficient controls are in place to reduce security risks to acceptable levels.		X				X	X
F	Managers understand and accept residual risk and authorize work to be performed.		X				X	
G	Senior managers ensure that their managers receive S&S training consistent with their security responsibilities and appropriately execute their S&S responsibilities.	X	X	X	X		X	X
H	Senior managers optimize the Laboratory-wide allocation of S&S resources for the most effective protection of DOE assets.		X			X	X	
I	S&S Program develops and provides S&S training and other mechanisms that provide appropriate skills, knowledge, and abilities to meet security requirements.	X			X		X	
J	S&S Program interprets the DOE S&S requirements, promotes worker involvement in developing site-specific requirements and implementing tailored controls, and assists managers and workers in assessing and reducing S&S risks to acceptable levels.	X	X				X	X
K	S&S Program assists senior management in S&S oversight by providing program assessments, incident analyses, and lessons learned.	X	X	X			X	

