

INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT PLAN (ISSM)

Environment, Health and Safety Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California
Berkeley, CA 94720



Ernest Orlando Lawrence Berkeley National Laboratory
Prepared for the U.S. Department of Energy under Contract Number DE-AC03-76SF00098

Table of Contents

A. Vision Statement	1
B. Mission Statement	1
C. Introduction	1
D. Guiding Security Principles	1
E. External Controls	3
F. Security Functions at the Institutional Level	4
G. Security Functions at the Division, Project or Activity Level	5
H. Security Management Plan Summary	8

The following informative Appendices do not appear in this document. For information concerning this material, see the web sites provided.

- Appendix A. Safeguards and Security Plan http://www.lbl.gov/ehs/security/04sec_phys/SS_Plan_Title.html
- Appendix B. Cyber Security Protection Plan <http://www.lbl.gov/ICSD/Security/>
- Appendix C. Export Control Document <http://www.lbl.gov/ehs/security/01export/index.html>
- Appendix D. Counter Intelligence Plan http://www.lbl.gov/ehs/security/02intl_emp/index.html
- Appendix E. Security Reference Guide (Future Site)

A. Vision Statement

Integrated security supports and protects innovative science.

B. Mission Statement

The Berkeley Lab Security program assures all visitors and employees of an open and secure work environment that fosters the continuation of creative scientific advances. Integrated security management ensures the protection of Laboratory assets, including physical and intellectual property, and establishes programs for cyber security, export control and counterintelligence.

C. Introduction

Ernest Orlando Lawrence Berkeley National Laboratory (Berkeley Lab) is a multidisciplinary national research laboratory, located on land belonging to the Regents of the University of California and operated with funds furnished by the U.S. Department of Energy (DOE). As stewards of this public trust, the staff and management of Berkeley Lab must protect the public's interest and investment in the people, the land and environment, the equipment and facilities and the intellectual property that make up Berkeley Lab.

Berkeley Lab sets policy to ensure a secure working environment for all employees and visitors. As a designated Tier Three laboratory managed by the University of California and under contract to DOE, all practices established must ensure an open, collaborative work environment that facilitates scientific excellence. The Laboratory must achieve a balance between protecting its critical assets and maintaining this open working environment that supports collaborative science. Since the Laboratory is engaged in an unclassified mission, the security threats are deemed to be relatively low compared to other DOE sites in the Tier I and II categories.

The Laboratory's mission includes not only fundamental science in partnership with research universities and other national laboratories, but also collaborative research in participation with industry and the world scientific community. Research is reviewed for export controls designed to protect items and information determined to be important to the national interest.

D. Guiding Security Principles

High standards of performance and clearly defined expectations result in a safe and secure working environment. In its commitment to scientific excellence, Berkeley Lab adheres to the following guiding security principles:

- *Line management owns security.* Every laboratory manager is responsible for integrating appropriate security controls into his/her work and for ensuring active communications of security expectations up and down the management line and with the workforce.
- *Clear roles and responsibilities are defined and communicated.* Clear lines of authority and responsibility for security assurances are established and met. At Berkeley Lab this principle is manifested in position descriptions, and performance reviews, as well as feedback up and down the line.

- *Cyber and physical security, export control management, and counterintelligence functions are integrated.* All employees are provided with the necessary resources to identify the functions that affect their work environment. They not only have the information required, but also understand their individual responsibility to guard and protect these assets.
- *An open environment supports the Berkeley Lab mission.* As a Tier Three Laboratory, it is vital that collaborative research be conducted with Tier One and Tier Two laboratories, as well as with industry, universities, and the international scientific community. The Laboratory must be open and accessible.
- *Security is a value-added activity supporting research and support operations.* Security must support the Laboratory's mission.
- *Security controls are tailored to individual and facility requirements.* Each division will designate a security point of contact. This contact will work directly with the Environment, Health & Safety (EH&S) and Computing Sciences (CS) security managers to lay out an integrated security plan to meet the business needs of the group. The point of contact will develop both individual and group approaches for Laboratory security requirements. Not every aspect of security requirements, such as counter intelligence issues or export control requirements, will affect every individual or group. However, every group should be able to identify when these requirements affect their work.

While these security principles apply to all work performed at Berkeley Lab, the implementation of these principles continues to be flexible as we maintain an open, collaborative work environment while at the same time identifying and mitigating any threats. Therefore, policy, performance, and review standards should be commensurate with those for a low-risk, unclassified laboratory. Clear communication between all Laboratory visitors and employees is an essential ingredient to maintain this climate while protecting our assets. Principal investigators (PI)s, managers and supervisors are expected to incorporate these principles into the management of their work activities. Not only does the Laboratory maintain an open facility on site, but we also manage facilities on campus at UC Berkeley, as well as downtown Berkeley, Oakland and Walnut Creek. These on-site and off-site facilities follow the same program principle.

Figure A illustrates the relationship that must exist between the external organization, the Laboratory, the division and line management to protect Berkeley Lab's assets and provide the necessary controls.

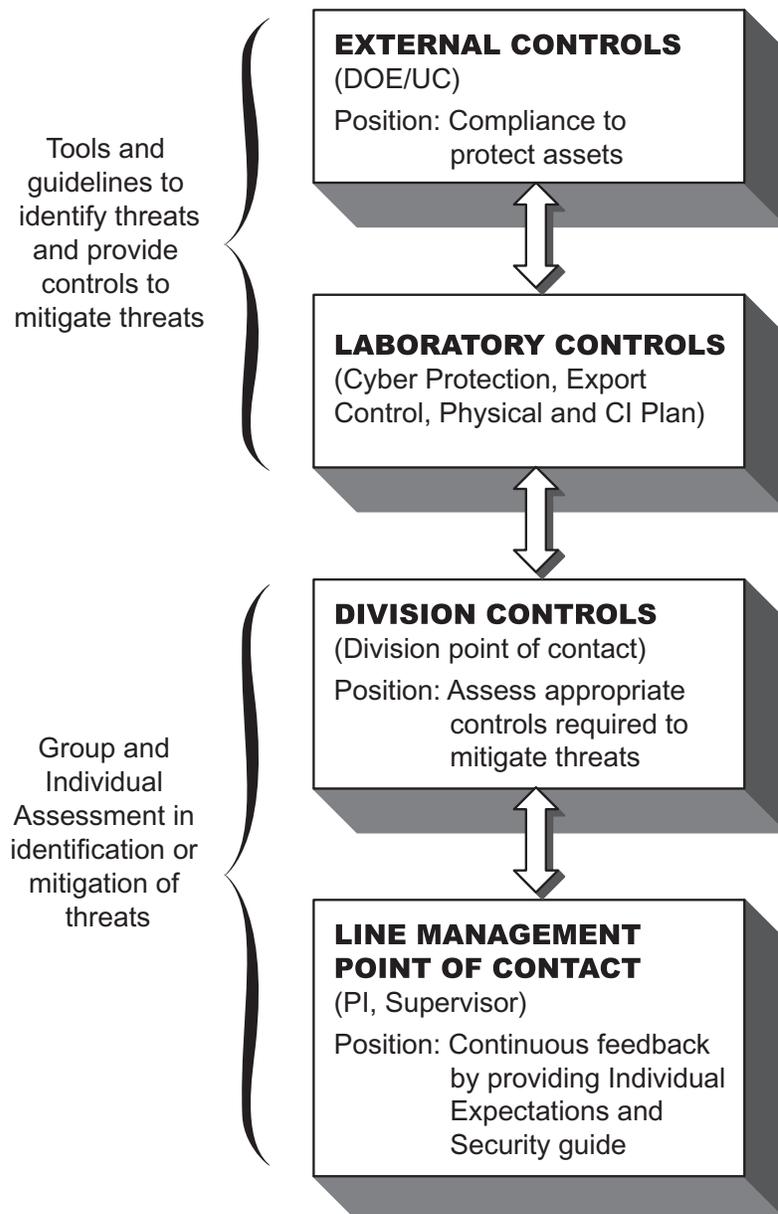


Figure A. Integrated Controls.

E. External Controls

The Laboratory’s principal role for DOE is fundamental science. Our multidisciplinary research environment and unique location serve to strengthen partnerships with industry, universities and other government laboratories. These roles support DOE’s Strategic Laboratory Missions Plan and are based on core competencies. How to maintain an open collaborative environment and still protect its assets will require that the Laboratory engage in an ongoing dialogue with its stakeholders. As we attempt to achieve the proper balance between collaboration and

security, this Security Management Plan will provide the tools for analysis and feedback. External and internal institutional assessment will govern the future direction of the plan. Ongoing feedback will be the relevant tool to ensure that science is not encumbered and that the necessary resources are provided without jeopardizing our security principles.

Some of the organizations with the more significant roles include:

- DOE – Office of Security Operations (SO)
- DOE – Office of Science (SC)
- DOE –BSO
- University of California President’s Council on Security
- University of California Office of the President
- Computer Incident Advisory Council (CIAC)

Security policy is initiated at the institutional level and from DOE headquarters. As indicated in Section II of the Institutional Plan, “the Laboratory implements physical security programs appropriate for the protection of its employees and Lab property. The adequacy of Berkeley Lab’s security management systems is reviewed periodically by senior management. Mechanisms for conducting this review include independent peer reviews.

F. Security Functions at the Institutional Level

It is the responsibility of Computing Sciences and the Property Protection, Life Safety Group (PPLS) in the EH&S Division to provide guidance to each Berkeley Lab division in assessing and mitigating security threats. Security threats for LBNL are found in Appendices A and B. This procedure guarantees high quality standards and clearly defined expectations that will result in a safe, secure working environment for every employee and visitor. Based on guidance provided by the managers of the cyber and physical security programs, divisions may identify the threats applicable to their work. Working in coordination with the institutional program managers, divisions must institute controls commensurate with the threat. The following items are examples of security functions at the institutional level.

1. *Work planning.* The tasks to be accomplished as part of any given activity are defined clearly.

As stated in the Laboratory Institutional Plan, programmatic goals are managed through divisions that implement DOE and other sponsors’ research programs. These divisions have line and project management responsibility to assure that intellectual, property, computational, and other resources are properly protected to sustain the scientific mission and operational requirements. Security planning is integrated with scientific and operations planning.

2. *Analyze threats to the extent possible.* Security vulnerabilities associated with performing planned work are clearly identified and understood before beginning work. Threats to Berkeley Lab work are stated in the Cyber and Physical Security Plans.
3. *Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures and controls.* Appropriate counter measures are in place. These measures are based on best standards and are reviewed periodically. All visitors and

employees receive the required information regarding threats and methods for mitigating threats.

The following documents provide the necessary controls adopted at the Laboratory:

- Safeguards and Security Plan
- Cyber Security Protection Program
- Export Control Document
- Counter Intelligence Plan

Since all work at the Laboratory is carried out under contract with the Regents of the University of California and the U.S. Department of Energy, fundamental controls are developed and agreed upon by the Laboratory.

4. *Perform work within the controls.* Once controls are identified, line management must ensure that work is executed within those controls.
5. *Continuous feedback.* Security measures are continually assessed for effectiveness through operational awareness. In addition, periodic reviews, such as external peer reviews, are conducted.

G. Security Functions at the Division, Project or Activity Level

In order to provide an appropriate level of security and meet DOE and statutory requirements, Berkeley Lab requires commitment and leadership from management in communicating to our visitors and employees our value-added security program. It is the responsibility of Computing Sciences and the Property Protection, Life Safety Group (PPLS) in the EH&S Division to provide guidance to each division in assessing and mitigating security threats. This process guarantees high standards and clearly defined controls that will result in a secure working environment for every employee and visitor.

The Laboratory has established a unified set of security elements to protect critical assets. A Security Reference Guide will be provided to all Laboratory employees and visitors. External peer reviews and internal reviews afford the essential feedback to ensure that all security controls are in place. The critical assets of personnel, physical and information security are continually evaluated.

Figure B illustrates the correlation that exists in protecting the critical assets of the Laboratory and the documentation and review process necessary for continual feedback.

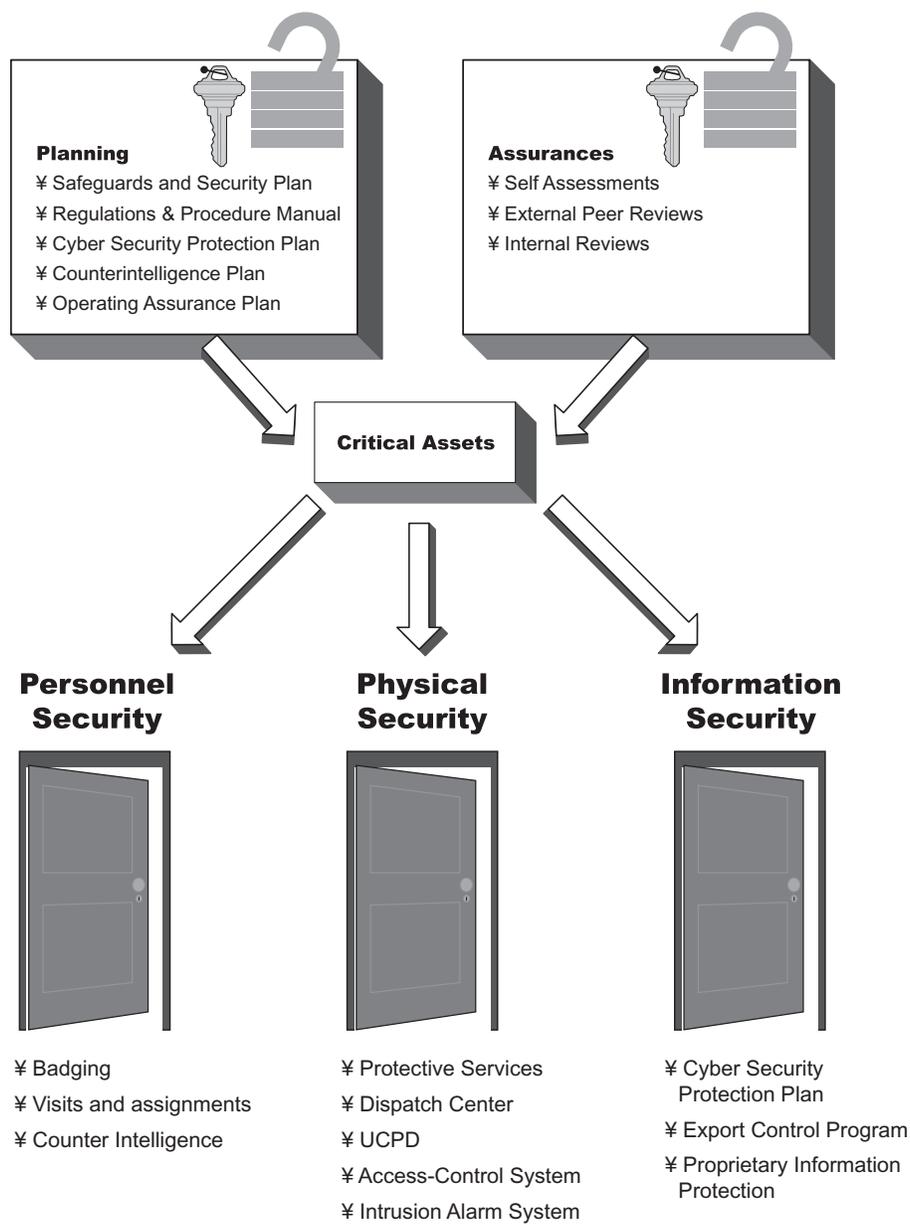


Figure B. Berkeley Lab employs integrated security elements to protect critical assets.

Berkeley Lab's research and support divisions vary widely in the type of work performed, size, location and customers. Accordingly, each division's threats and assets are different. While following broad Laboratory security policy, it is appropriate for each division, with assistance from the institution, to tailor its security programs to its needs.

1. *Work planning.* At the beginning of any new initiative or building construction, the division in partnership with the Cyber and Physical Security managers will define the work and function within that environment. Consideration will be given to cost and building location, and ensure that all credible threats have been identified and all preventive measures implemented.

2. *Define the required security elements and threats.* As part of the planning process, PIs, managers and supervisors are required to consider what threats are present and to implement appropriate controls as outlined in the Security Reference Guide. They are required to assure that every employee is in conformance with security requirements. For the majority of the work, the threats are minimal and security precautions are routine.
3. *Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures and controls.* Appropriate controls for activities at Berkeley Lab are described in the Site Safeguards and Security Plan. Four countermeasure strategies used include access denial, access control, intrusion warning, and intervention. The degree to which these strategies are employed depends on the level of risk the threat presents.
4. *Perform work within those controls.* Use security tools, guidelines and resources to ensure that work is performed within the established controls. A printed security guide will be distributed to every employee; the guide will contain information about security threats, methods for mitigation, and resources or points of contact. Expectations for each employee will be clearly stated in the yearly appraisal process.
5. *Continuous feedback.* All security measures are assessed on an ongoing basis through operational awareness. In addition, periodic reviews, such as external peer reviews, are conducted.

Figure C clarifies the roles and responsibilities of an integrated security management plan. The relationship between senior management, the division and line management requires continuous feedback to ensure that all work performed meets all security criteria.

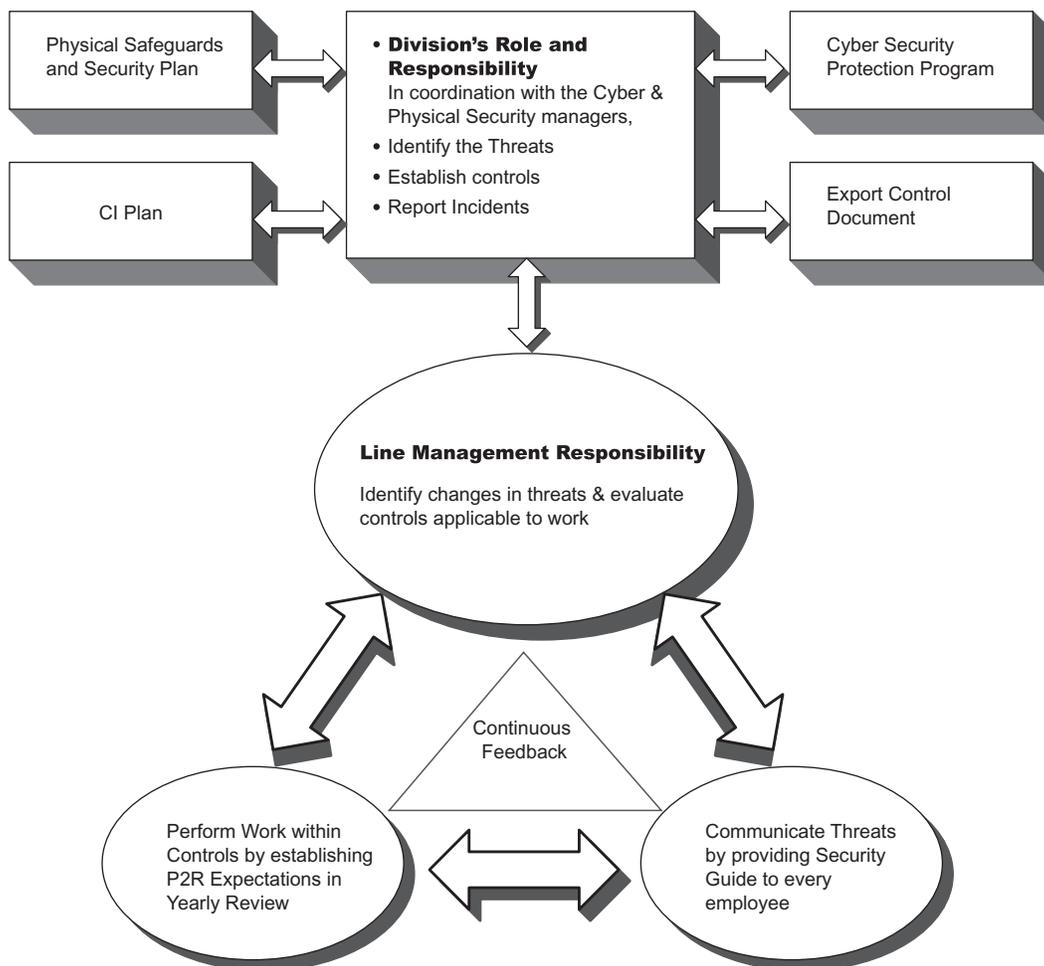


Figure C. Roles and responsibilities of an Integrated Security Management Plan.

H. Security Management Plan Summary

Berkeley Lab is committed to scientific excellence and stewardship of its assets. While security principles apply to all work performed at the Laboratory, their implementation is flexible. Berkeley Lab adheres to the following principles:

- Line management owns security.
- Security roles and responsibilities are clearly defined and communicated.
- Security functions are integrated.
- An open environment supports the Laboratory's Mission.
- The security program must support the scientific and operational missions of the Laboratory and must be value added.
- Security controls are tailored to individual and facility requirements.