Cyber Security

Assurance Plan

June 2010

Approved By:

____(signed version on file_)_____ _____

Rosio Alvarez, Chief Information Officer Date

TABLE OF CONTENTS

RECORD OF REVISIONS

Rev. No.	Date	Description

1.0 INTRODUCTION

The LBNL Cybersecurity Assurance Plan is designed to ensure that LBNL Cybersecurity systems are effective, meet contractual requirements, and support the LBNL mission. LBNL establishes, with the Department of Energy (DOE), an understanding of acceptable risk and develops and tailors controls in an ongoing way to meet this standard. LBNL develops and implements the appropriate controls and provides, for itself, assurance that the system is functioning as intended. This Plan describes the Cybersecurity assurance mechanisms that inform management if controls are working as designed and if the set of controls is appropriately protecting the institution. Implementing this Plan drives performance improvement by self-identifying, preventing, and correcting issues. These assurance mechanisms will be used to demonstrate to DOE, the University of California (UC), and LBNL management that the cyber security mechanisms themselves are adequate to reduce risk to the agreed upon level, and that controls are functioning as intended.

2.0 INDEPENDENT ASSESSMENTS

2.1 Overview

The LBNL Cyber Security Program is designed to provide independent assessment of the security controls of those who operate and manage IT hardware. Roles and responsibilities are split in such a way as to allow Cyber Security Program staff autonomy in terms of reviewing configurations and practices, both from automated tools such as configuration/vulnerability scanning systems as well from from more in-depth deep dives. These operations are covered under Self Assessments and Reporting since they are not completely independent, but they are core to understanding how the Cyber Security Program approach to independent assessments works.

2.2 External Assessments Contracted As Part of Authorizing Systems

The Cyber Security Program analyzes risk and documents its controls and compliance through a process called the Risk Management Framework (formerly, the Certification and Accreditation Process or the System Authorization Process). This process describes a series of steps necessary to manage and analyze technical, operational, and management controls, evaluate risks and residual risks, and assess system function and risk management. While the process for managing is continuous, on a cycle that usually lasts three years, a full evaluation of the systems are undertaken.

During this process, LBNL engages external assessors, either through Peer Review or through contracted external auditors, to evaluate system operation. These are the most in-depth and risk-informed evaluations we undertake. In the past, these reviews have taken multiple weeks and included both technical testing and document review. The results of these reviews become part of the authorization package and are available to DOE for review.

2.3 Internal Audit

UC operates an independent Internal Audit system for LBNL, Internal Audit Services (IAS). IAS's mission is to assess and monitor the Laboratory community in the performance of their oversight, management and operating responsibilities in relation to governance processes, systems of internal controls, and compliance with laws, regulations, contracts and Laboratory, UC, and DOE policies.

IAS has been granted authority through its charter and the UC Internal Audit Management Charter approved by the Regents of UC. IAS functions under the policies established by the Regents and Laboratory management under delegated authority. IAS is authorized full, free and unrestricted access to information including records, computer files, property, and personnel of the Laboratory required in the performance of audits. The work of IAS is unrestricted except where limited by law. IAS is free to review and evaluate all policies, procedures and practices of any Laboratory activity, program or function.

In practice, IA conducts at least one IT focused audit each year,. Results are shared with UC and LBNL management.

2.4 Inspector General Operations Audits and Reviews

The DOE IG performs audits of contractor cyber security operations. Results from these reviews must be carefully calibrated due to the IG's focus on cost-savings opportunities regardless of impact on mission achievement.

2.5 DOE Financial Statement Audit

Pursuant to 31 U.S.C. § 3515, Financial Statements of Agencies, the head of the agency is required to prepare and submit to the Congress and the Director of the Office of Management and Budget (OMB) an audited financial statement for the preceding fiscal year, covering all accounts and associated activities of each office and the agency not later than March 1. This audit is in support of the Federal Managers' Financial Integrity Act **(FMFIA)**.

2.6 DOE Financial Information Security Audit

The DOE also annually conducts intensive audits in support of the Financial Information Security Management Act (FISMA). These audits are sometimes,

but not always, coordinated with the FMFIA audits. Both the annual Financial Statement audit and the annual FISMA audit typically contain IT related testing and evaluation.

2.7 Other DOE Reviews

The DOE Berkeley Site Office (BSO) conducts graded oversight reviews of the Laboratory's Cyber Security Program. These reviews include ongoing operational awareness activities, and scheduled assessments and reviews into particular risks or control families. Assessment topics are generally planned and calendared at the start of the performance year. LBNL's safeguards and security program is often subject to an extensive DOE BSO review.

Historically, DOE Office of Health, Safety and Security (HSS) has conducted both assistance visits and red team/full evaluations of Laboratory cyber security programs. Additionally, LBNL can engage HSS at our request to review our systems and practices.

2.8 Peer Reviews

LBNL makes targeted use of peer reviews on an as needed basis. In the past three years, separate peer reviews of ESnet security and the 800-53 Certification and Accreditation process were conducted. LBNL utilizes peer reviews where internal expertise or external oversight is judged to be insufficient, or where the only reasonable form of oversight is peer review (for instance, where expertise about a specific issue is limited to the peer group).

3.0 SELF ASSESSMENTS

3.1 Ongoing Review of Operations and Incidents

The core of the LBNL's Contractor Assurance System for Cyber Security revolves around the continuous monitoring system and the management of the Cyber Security Program. This program is dynamic; and the Chief Information Officer and Computer Protection Program Manager are involved in a continuous process of evaluating existing controls, the changing threat environment, and demonstrated risks/damages to optimize the controls in place (including reducing such controls when they are not cost-benefit positive). Monitoring systems also verify the technical functioning of the controls and support root cause reviews for incidents.

At ongoing meetings and through day to day email communication, the cyber security team evaluates these factors to determine if new controls (policy, management, and technical) are required to address the changing environment.

These priorities are reflected in changes to the focus of the team, and in funding reallocations as appropriate.

Quarterly, the incidents of concern are discussed with representatives from the Divisions on the Computer Protection Implementation Committee to spread awareness of the trends and seek feedback on controls.

Annually, the entire incident and control framework is formalized and judged against the Berkeley Lab-Carnegie Mellon cost model for damages with comprehensive evaluation of mission damage in qualitative form, informed by expert opinion, to further evaluate and refine the program. This process is discussed further under

3.2 Annual Risk and Self Assessment

The Office of the CIO and the Cyber Security Program undertake annual risk and self assessments of its information technology posture. The risk-assessment process is designed to provide transparency to DOE and the Laboratory Community on current and emerging threats, as well as residual risks from our security posture. The self-assessment process seeks to verify the effectiveness of technical, administrative, and operational controls.

Both processes are consistent with National Institute of Standards and Technology guidance. However, LBNL's approach is unique in that it utilizes a cost-damage model collaboratively developed with Carnegie Mellon University, and uses extensive narrative description to ensure that LBNL community members and oversight organizations can understand the risks clearly and in lay, comprehensible terms.

Results are transmitted to DOE and are used as input for strategic planning and service management in the coming year**.**

3.3 University of California Self Assessment

UC conducts assessments of various aspects of the cyber security program in parallel with its assessment of the campuses. A scorecard process helps to ensure similarity with other UC campuses and cross campus comparisons. The scorecard is normalized across the campuses and LBNL and presented to the Regents for review. This typically happens annually.

3.4 Management Controls and Compliance Program

The Managment Controls and Compliance Program (MCC) is a comprehensive program for analyzing internal controls to meet financial and related compliance objectives. The MCC Program supports legislative requirements such as the Chief Financial Officers Act, the Inspector

General Act of 1978, as amended, FMFIA, FISMA, and the Improper Payments Information Act of 2002 (IPIA).

Analysis of internal controls typically involves key cyber security and IT assurance mechansisms such as change managment, alternate checking routines, and access and audit management.

The Office of the Chief Financial Officer will implement the Management Controls and Compliance Program for LBNL. For Fiscal Year 2010, the effort will take place between March 1 and July 16.

3.5 IAS Advisory Services

IAS may be requested to perform advisory services for various areas of cyber security. Advisory services are activities designed to mitigate risk, improve operations, and/or assist management in achieving its business objectives, in which the nature and scope of the engagements are agreed upon with the management of the subject matter being evaluated. Examples include informational resources, counsel, advice, facilitation, process design, and training.

4. 0 PERFORMANCE MEASURES

4.1 Performance Evaluation and Measurement Plan (PEMP)

The Cyber Security Program includes the development of cyber performance metrics, currently under PEMP Goal 8, Integrated Safeguards & Security and Emergency Management. Cyber metrics are developed annually with BSO and UC Office of the President (UCOP), supported by SC-wide guidance, and documented at the beginning of the performance year. The cyber metrics are designed to reflect real enhancements and efforts related to efficiently protecting LBL resources and encouraging integrated safeguards and security management.

4.2 Cyber Security Performance Measures

Delivering efficient, effective and responsive cyber security and resources that enable the successful achievement of laboratory missions is a key objective of the Cyber Security Program. Cyber Security Performance Measures are a strategic planning and management tool to monitor organization performance against operational/functional goals. These measures are listed in Attachment B.

5.0 REPORTING

5.1 PEMP

PEMP reporting for Cyber Security is contained in Performance Goal 8, Integrated Safeguards & Security and Emergency Management.. Quarterly, performance at the Cyber Security Objective level is discussed with DOE-BSO, UCOP, and LBNL management. Topics include PEMP progress to date, areas of risk or concern, and any noteworthy accomplishments and improvements. At year end, a self appraisal document is submitted to DOE. Although the PEMP is a primary means for determining performance, the evaluation by DOE may also use other available performance information, including results from reviews and performance measures described in this assurance plan, to determine success in meeting the Objective.

5.2 Federal Manager's Financial Integrity Act

FMFIA requires agencies to establish and maintain internal controls. The agency head must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations.

The University of California Office of the President's (UCOP) Laboratory Management Office will issue an opinion regarding the Laboratory's system of internal accounting and management controls in effect during the fiscal period. Included with its internal control assertion is information about the internal accounting and management controls, reportable issues, and corrective action plans provided by the Laboratory Director based on input from CFO management and staff. The Cyber Security Program provides input to this opinion.

5.3 Annual Risk Letter

The Cyber Security Program provides an annual risk evaluation to the Berkeley Site Office. See also section 3.3. The Risk Letter summarizes the annual risk assessment and provides assurance that the Laboratory is managing within the agreed upon acceptable risk envelope.

5.4 Authority to Operate

The Cyber Security Program provides extensive program evaluation to DOE as part of its authority to operate process, typically on a three year cycle. The

Program evaluation information includes information related to all aspects of external and internal testing of cyber security program controls.

5.5 Cyber Security Incident Tracking and Reporting

Cyber security incident reports follow defined reporting channels, with primary reporting to the Department of Energy's Computer Incident Response Center (CIRC) or equivalent, with copies to Counterintelligence, the Office of the

Inspector General, and the Berkeley Site Office. Incident reports are shared internally with key stakeholders to assure broad knowledge of current risks. Likewise, the Laboratory's cyber security staff remains abreast of new trends in attacks and threats primarily from public sector sources, but also from DOE sources such as CIAC alerts. As appropriate, briefing and discussions of cyber security incidents are entered into the LBNL Lessons Learned and Best Practices database and disseminated to target staff. These inputs, along with broad based incident review, allow the Laboratory to adjust its protection mechanisms continuously to ensure optimal protection. Incident trends and actions are communicated to the Computer Protection Implementation Committee, with membership from across the divisions.

5.6 FISMA Reporting

LBNL reports the status of its systems and authority to operate quarterly as part of DOE's overall approach to FISMA compliance.

6.0 ISSUES MANAGEMENT

The Cyber Security Program follows the LBNL Issues Management Program (LBNL PUB-5519) for managing issues. This program encompasses the continuous monitoring of work programs, performance to promptly identify issues to determine their risk and significance, their causes, and to identify and effectively implement corrective actions to ensure successful resolution and prevent the same or similar problems from occurring.

Cyber security issues are identified through self-assessments, incident assessments, and audits and reviews. At a graded approach, proper issues management includes causal analysis, development and implementation of corrective actions, and verification and validation of corrective action implementation and effectiveness.

6.1 Corrective Actions

As part of the Laboratory's Issues Management Program (IMP), all cyber security issues and associated corrective actions (except for those that are immediately corrected or rectified) are entered into the LBNL Corrective Action Tracking System (CATS) database. This database enables LBNL employees to identify,

track, manage, resolve, and search for issues and associated corrective actions. Corrective Actions are tracked to completion and validated

Major corrective actions are also reported to DOE (through the Office of Science) through the Plan of Actions and Milestones Process or POAMs. POAMs are an integral part of quarterly Federal Information Security Management Act reporting.

6.2 Incident Tracking

All cyber security incidents are tracked and identified with the goal of identifying proximate and root causes. See earlier discussion.

6.3 General Tracking

Issues related to the functioning of systems or from users are tracked either through the help desk ticketing system or through internal trouble reports. All issues are worked to completion. Automated systems ensure attention to unresolved issues. Weekly meetings discuss any open incident issues.

6.4 Trending

All incident and damage statistics are tracked for trends based on nine years of data and growing. The quarterly and annual risk assessments provide an opportunity to review trends and make adjustments to controls as appropriate. In addition, the Laboratory keeps summary connection information indefinitely so that long term studies of trends in attacks and connections can be conducted. These are often used to answer questions such as "what are the trends in password guessing attacks," and "how our our connections from other countries changing?"

7.0 LESSONS LEARNED AND BEST PRACTICES

The Program shares information gleaned from incidents as well as best practices from other labs and within the Laboratory widely. Generally, such information is shared via the CPP website as recommendations. In certain cases, the Laboratory's Lessons Learned system is utilized.

ATTACHMENT A

UC ASSURANCE PLAN SECTION REFERENCE

UC ASSURANCE PLAN		CYBER SECURITY ASSURANCE PLAN	
Section Description	**Section**	**Section Description**	**Section**
External Review	**2.3.3**	**Independent Assessment**	**2.0**
Self Assessments **Internal Review**	**2.3.1** **2.3.2**	**Self Assessments**	**3.0**
Performance Metrics	**2.2**	**Performance Measures**	**4.0**
Reporting	**2.4**	**Reporting**	**5.0**
Issues Management	**3.2**	**Issues Management**	**6.0**
Corrective Action Tracking System	**3.2.1.3**	**Corrective Action Tracking System**	**6.1**
Lessons Learned and Best Practices	**3.3**	**Lessons Learned and Best Practices**	**7.0**

ATTACHMENT B

FY10 LABORATORY MANAGEMENT PERFORMANCE MEASURES FOR CYBER SECURITY

Performance Measures monitored by LBNL management routinely:

- **Cyber Security Incident Analysis**

  Number of incidents and extent/ severity of incidents experienced at LBNL. Measured and reported in an ongoing manner to cyber security staff and direct management. Reported at least semi-annually to the cyber security representatives of divisions (CPIC), Reported monthly to CIO. Reported quarterly to Berkeley Site Office.

- **Customer Service and Response**

  Feedback from community members on interaction with and response from helpdesk and secondary cyber security and IT contacts as gathered from post-interaction satisfaction surveys. Surveys are sent immediately following ticket resolution with ongoing feedback provided to managers of operations and quarterly reports shared with management.

- **System Availability and Function Data**

  Functioning and availability of infrastructure and cyber critical systems measured by automated systems. Reported as problems arise to system administrators automatically. Reported monthly for network systems and quarterly for business systems to IT management. Reported as a percentage of target uptime.

- **System Configuration Data**

  Patch levels for systems during periods of high risk. (For example, if a new MS patch is released for an "in the wild" vulnerability, LBNL will track the patch numbers until the numbers dwindle to baseline vulnerability expectations.) This data is gathered on an ad hoc basis. When gathered, it is typically reported every few days to cyber security management. Reported as a number or percentage of vulnerable systems as a percent of total systems.

- **Training Completion**

Percent of LBNL staff that have completed required cyber security training. Reported in real-time on demand as part of overall training reports to divsion representatives, and quarterly to cyber security management. Reported as a percentage of individuals completing training per requirements.

- **Training Feedback**

  Numerical calculations of LBNL staff cyber security training evaluations. Reported on demand with real time information to cyber security management and reported quarterly to cyber security management. Reported as the average of a rating number on a scale of 1-5.

ATTACHMENT C

CONSOLIDATED ASSESSMENT SCHEDULE

Assessment Title	Date Performed	Performed By
External Authorizing System Assessments	Triennial cycle	Peer Review/ External assessors
Department of Energy Financial Statement Audit	Throughout year - completed by 3/1 of following fiscal year	DOE External Auditor - KPMG
Department of Energy Financial Information Security Audit		
Department of Energy Berkeley Site Office Oversight Activities	Varies	DOE-BSO
Department of Energy Office of Health, Safety and Security Oversight Activities	Varies	DOE-HSS
Internal Audits and Advisory Services	Per IAS Audit Plan	LBNL Internal Audit Services
Management Controls and Compliance Program	Completed by 7/1.	LBNL Management
Annual Risk and Self-Assessment	Completed by 10/1	Office of the CIO / Cyber Security Program
University of California Self	Completed by 10/1	UC

Assessment		

ATTACHMENT D

Outcome	Assurance System	How we demonstrate the system is working	Reporting Period
Systems are securely configured and meet requirements.	Vulnerability scanning, continuous and on demand, to identify insecurely configured or vulnerable systems with actions in response to a finding of vulnerability.	On request access to blocked host history lists, web site information with current scans.	Ongoing
Systems are not infected or attacking other systems.	Monitoring systems provide indications of vulnerable systems.	On request access to Bro logs and incident investigation reports.	Ongoing
Attackers cannot search for targets indiscriminately.	Monitoring systems (Bro, Syslog, Netflow) provide defenses against indiscriminate attackers.	On request access to Bro logs.	Ongoing
Users are trained.	LBL Training Database	Report outputs on training rates and percentages	Quarterly
Security systems are operational.	Monitoring and alerting systems to detect failures in critical cyber defense systems.	On request access to Nagios and related logging reports.	Ongoing
DOE and LBL jointly understands residual risk.	Annual risk assessment and ongoing briefings as necessary. Cost-benefit analysis of cyber program.	Dialogue with site office.	Quarterly and Annually