LBNL/PUB-3183

Integrated Safeguards and Security Management Self-Assessment 2004

Dan Lunsford
Security and Emergency Operations Manager

Dwayne Ramsey
Computer Protection Program Manager

James Rothfuss, Computer Protection Program
Erik Richman, Operations
Nicole De Jager, Security and Emergency Operations Group

Ernest Orlando Lawrence Berkeley National Laboratory
Berkeley, CA 94720

May 2005

Approved by:

_____

Phyllis Pei
Division Director
Environment, Health and Safety Division
Security and Emergency Operations

_____

A. X. Merola
Division Director
Information Technologies and Services Division

This work was supported by the Director, Office of Science, of the U.S. Department of Energy under Contract No. DE-AC03-76SF00098.

ACKNOWLEDGMENTS

This survey and report would not have been possible without the exceptional staff support and technical expertise from:

James Rothfuss, Computer Protection Program, was instrumental in establishing new specific and measurable goals for the survey, while applying sound analytical thinking and keeping the ISSM Survey Team (IST) on target.

Erik Richman, Operations, provided the technical competency necessary, while isolating survey characteristics in need of improvement; his tireless technical efforts contributed to a successful survey.

Nicole De Jager, Security and Emergency Operations Group, coordinated and facilitated the survey and displayed a keen sense of ingenuity in anticipating and meeting unexpected survey situations.

Of special note are all the **ISSM Division Liaisons** who made significant contributions to the survey's success. Their support and timely recommendations for improvement played an important role in accomplishing the goals and objectives of the survey.

Table of Contents

EXECUTIVE SUMMARY

In 2002 Ernest Orlando Lawrence Berkeley National Laboratory deployed the first Integrated Safeguards and Security Management (ISSM) Self-Assessment process, designed to measure the effect of the Laboratory's ISSM efforts. This process was recognized by DOE as a best practice and model program[1] for self-assessment and training. In 2004, the second Self-Assessment was launched. The cornerstone of this process was an employee survey that was designed to meet several objectives:

- Ensure that Laboratory assets are protected.
- Provide a measurement of the Laboratory's current security status that can be compared against the 2002 Self-Assessment baseline.
- Educate all Laboratory staff about security responsibilities, tools, and practices.
- Provide security staff with feedback on the effectiveness of security programs.
- Provide line management with the information they need to make informed decisions about security.

This 2004 Self Assessment process began in July 2004 with every employee receiving an information packet and instructions for completing the ISSM survey. The Laboratory-wide survey contained questions designed to measure awareness and conformance to policy and best practices. The survey response was excellent—90% of Berkeley Lab employees completed the questionnaire. ISSM liaisons from each division followed up on the initial survey results with individual employees to improve awareness and resolve ambiguities uncovered by the questionnaire. As with the 2002 survey, the Self-Assessment produced immediate positive results for the ISSM program and revealed opportunities for longer-term corrective actions.

Results of the questionnaire provided information for organizational profiles and an institutional summary. The overall level of security protection and awareness was very high—often above 90%. Post-survey work by the ISSM liaisons and line management consistently led to improved awareness and metrics, as shown by a comparison of profiles at the end of phase one (August 6, 2004) and phase two (November 1, 2004). The Self-Assessment confirmed that classified information is not held or processed at Berkeley Lab. The survey results also identified areas where increased employee knowledge and awareness of Laboratory policy would be beneficial, the two most prominent being password usage and wireless network service. Line management will be able to determine additional corrective actions based on the results of the Self-Assessment.

Future assessments will raise the ratings bar for some existing program elements and add new elements to stimulate further improvements in Laboratory security.

---

[1] Conclusion reached by the DOE/Oak Ridge Service Center Survey Team during the July 2004 Safeguards and Security Audit.

OVERVIEW

In April 2001, Berkeley Lab adopted its Integrated Safeguards and Security Management (ISSM) Plan[2] to integrate all aspects of security into the fabric of Laboratory operations. The plan outlines the Berkeley Lab ISSM program, which is designed to ensure the protection of Berkeley Lab assets, including physical and intellectual property, and is closely aligned with DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy.*

The vision and mission of the ISSM Plan are:

Vision

Integrated security supports and protection of innovative science.

Mission

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.

Six guiding principles and five security functions were developed to form the core of ISSM:

Guiding principles

1. Line management owns security.
2. Clear roles and responsibilities are defined and communicated.
3. Cyber and physical security, export control management, and counterintelligence functions are integrated.
4. An open environment supports the Berkeley Lab mission.
5. Security is a value-added activity supporting research and support operations.
6. Security controls are tailored to individual and facility requirements.

Security functions at an institutional level

1. Work planning. The tasks to be accomplished as part of any given activity are defined clearly.
2. Analyze threats to the extent possible.
3. Develop appropriate countermeasures to threats, and communicate information regarding threats, countermeasures, and controls.
4. Perform work within the controls.
5. Continuous feedback.

[2] The ISSM Plan is included as Appendix A and also is available on the Web at http://www.lbl.gov/ehs/security/issm/ISSMfinal.html.

PURPOSE

The Self-Assessment is designed to provide a baseline measurement of the Laboratory's current security status and to ensure that Laboratory assets are protected; to educate staff about security responsibilities, tools, and practices; to provide security staff with feedback on the effectiveness of security programs; and to provide line management with the information they need to make informed decisions about security.[3]

The specific purpose of the first Self-Assessment (2002) was to develop and administer a smooth process that could be easily modified and would lead to significant improvements in the future. After the success of the 2002 Self-Assessment, the 2004 Self-Assessment had the additional challenges of "raising the bar," that is, improving upon the previous assessment's standards, as well as gauging improvements since 2002.

In April 2004, Berkeley Lab initiated the second ISSM Self-Assessment process. ISSM liaisons were designated for each organization at the Laboratory to represent line management during the process. The Self-Assessment consisted of an all-employee survey. Data maintained by the physical and cyber-security staff are included in Appendix G. Results were provided to line managers in the form of organizational profiles and an institutional report, which together identified unmitigated risks in order to improve ISSM performance in specific areas and to evaluate the overall ISSM program. All of these components were developed into a Web-based system (Figure 1).

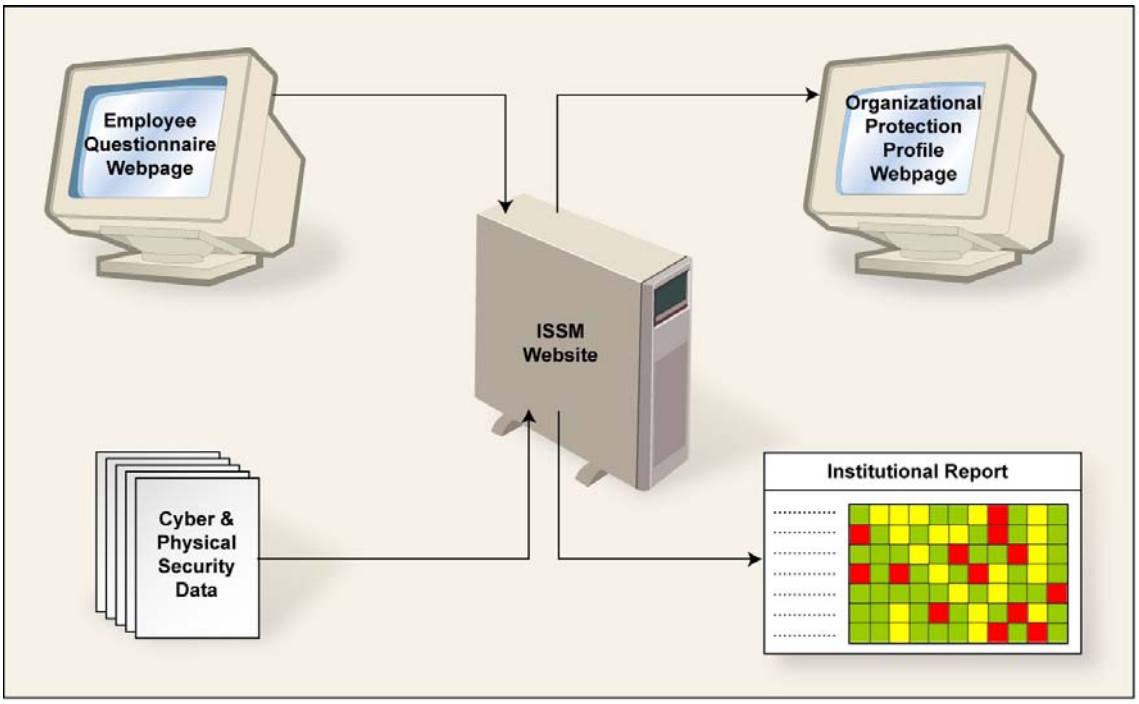


Figure 1. ISSM Self-Assessment components.

[3] This Overview is supplemented by material provided in presentation form in Appendix B.

DEVELOPMENT AND IMPLEMENTATION

The ISSM Self-Assessment development and implementation process proceeded as follows:

- The second periodic ISSM Self-Assessment was commissioned.
- The same Self-Assessment tools used in 2002 were used in 2004. No new tools were developed.
- The questions were updated to include current risks and to enhance performance.
- The Self-Assessment questionnaire was presented to the Deputy Director for Operations and the Operations management staff. More modifications were made to the questionnaire based on their review.
- The questionnaire was sent to the Division Security and Computer Protection Liaisons for their review (Table 1). Changes were made based on their review.
- The new Self-Assessment process was announced to the division directors and given the go-ahead.
- The survey was implemented.
- Results for each organization were opened to review by division and organization directors and ISSM liaisons.
- ISSM liaisons followed up on survey results.
- Improvements to survey results were officially closed.
- The ISSM Self-Assessment Report (this document) was completed.

Table 1. ISSM and Computer Protection Liaison assignments at time of survey.

Directorate	Organization	ISSM Liaison	Computer Protection Liaison
Director's Office		Karen Paris	Nancy Tallarico
Physical Sciences			
	ALS	Bernie Dixon	Eric Williams/Alan Biocca
	MS	Joel Ager	Ron Tackaberry
	PB	Jeff Pelton	Ralf Grosse-Kunstleve
	CSD	Angela Gill	Corwin H. Booth
General Sciences		Faye Mitschang	
	AFRD		Joe Chew
	PHYS		Alessandra Ciocio
	NSD		Howard Matis
Biosciences			
	LSD	Ciccina Guagliardo	Martin Boswell/Ron Huesman
	GN	Hank Glauser	Brian Yumae
Energy Sciences		Maryann Villavert	
	ESD		Bryan E. Taylor/Peter Lau
	EETD		Ken Revzan
Computing Sciences		Dwayne Ramsey	
	NERSC		Stephen Lau/Scott Campbell
	CRD		Chip Smith
	ITSD		Chris Manders
	ISS		Greg Balin/Dan Klinedinst
	NTD		Al Early
	ESnet		Dan Peterson
Operations		Jane Baynes	
	CFO	David Chen	John Speros
	HR	Cynthia Coolahan	Daisy Guerrero
	BS		Mary Clary
Resources			
	FA	John Pon	John Pon/Chinh Huynh
	EG	Weyland Wong	Chuck Lawrence
	EHS	Dan Lunsford	Stephen Abraham/Dan Lunsford

The Self-Assessment measures the Laboratory against several ISSM principles and functions:

- *Line management owns security:* The organizational profiles give the division directors and other managers the information they need to make informed decisions and improvements.
- *All security functions are integrated:* This is the first effort since the conception of the ISSM in which all security functions (physical, personnel, cyber, export control, counter-intelligence) are encompassed in one project.
- *Clear roles and responsibilities are delineated:* The questionnaire and organizational profiles reinforce each individual's responsibilities and give them the means to learn more about those responsibilities.
- *Security elements and threats are defined:* The Self-Assessment collects data from the security programs and individual employees that can be used to assess threats and risks to the Laboratory.
- *Work is performed within the controls:* The Self-Assessment measures performance data that can be used for immediate control improvements and to identify future areas for performance improvement.
- *Continuous feedback:* The Self-Assessment provides data for identifying weaknesses and measuring improvement.

The feedback loops in the Self-Assessment process (Figure 2) are designed to stimulate both short- and long-term improvements in security.

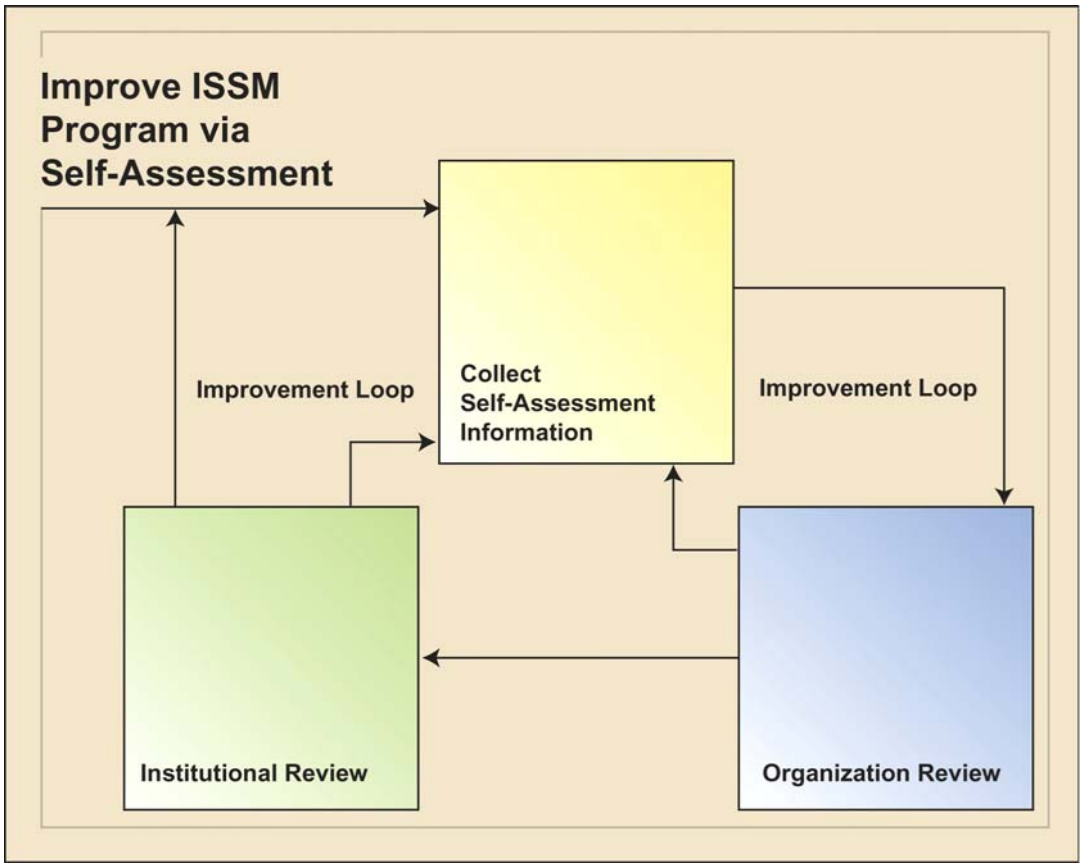


Figure 2. ISSM Self-Assessment process.

PROCESS IMPROVEMENTS AND CHANGES

In late spring 2004, the second Self-Assessment survey was completed. As expected, some 2002 metrics were removed because they did not reveal substantial information or had become outdated by better processes. Questions that carried over from the 2002 assessment were strengthened and their rating criteria were tightened. Questions were added concerning new risks, such as terrorism and wireless computing.

TOPICS REMOVED

DOE Sensitive Information and Critical Systems

The 2002 survey posed a series of inquiries about sensitive information and critical systems. These questions produced a set of employees who said they were working with information or processes that may not be adequately protected by the Laboratory's baseline measures. All of these employees were interviewed to determine whether their systems and information were actually in need of extra protection and, if they were, the extra protection was implemented. Because these

particular systems have now been identified and protected, it was decided that asking these questions again in the 2004 survey would be counterproductive.

Cracked Passwords

In the 2002 Assessment, this measurement was based on cracking the passwords on a defined set of ITSD-managed computers. Since the first assessment, password cracking on this specific set of computers has been integrated as a continuous (daily) process. Poor passwords are discovered and changed as they appear. Hence, a yearly check is a redundant endeavor. This measurement has been removed from the periodic Self-Assessment.

System Vulnerabilities

In the 2002 Assessment, the cyber security staff designed a process to uncover and correct a strictly defined and easily measurable set of high-risk computer vulnerabilities. Because vulnerabilities that appear on the network are highly dynamic, the types and duration used for this rating were fixed, limiting the actual vulnerabilities that could be measured. Since the first assessment, vulnerability discovery (scanning) has been integrated as a continuous process. Vulnerabilities are discovered and resolved within days of their introduction. A yearly check for vulnerabilities is now a redundant activity. This measurement has been removed from the periodic Self-Assessment.

DOE Warning Banners

The purpose of this question was to ensure compliance with DOE warning banner requirements. Although the first assessment found a healthy compliance of 87%, our risk assessment found that the warning banner does little to deter the most costly threats (i.e., worms, which attack regardless of warnings). It was determined that this metric would be dropped in favor of more pressing ones such as threat reporting and rules concerning foreign nationals.

Security Access Managers

Each Laboratory organization controls access to its own area. The people who control access are known as Security Access Managers (SAMs). In the 2002 survey, responses to the survey question on SAMs indicated that there was confusion about the title and responsibility. Since the 2002 survey, the title, role, and responsibility for this function has been clarified to the SAMs. Since this question only applied to a very small fraction of the Berkeley Lab population (~20), it was removed from the 2004 survey.

Employee Security Guide

During the initial rollout of the 2002 Assessment, all staff received a packet of information that included a pocket-sized pamphlet, *The Employee Security Guide*. Since this pamphlet has not been changed, it was determined that another distribution of the pamphlet was not cost effective.

RATINGS IMPROVED

The ratings for the following survey topics were changed (Table 2).

Table 2. Improved ratings for carry-over metrics.

Question Topic	Old Rating (%) (yellow range)	New Rating (%) (yellow range)
Emergency Phone Number	85–60	90–65
Proximity Card Access	70–50	80–60
Office Keys	70–50	80–60
Securing LBNL Property	85–60	90–65
Visitor Access	85–60	90–65
Crisis Action Team	70–50	70–60
Software Licenses	85–60	90–65
Password Policy	70–50	80–60
Virus Protection	85–60	80–60
Backups	70–50	80–60

TOPICS ADDED

The following questions were added to the 2004 Self-Assessment survey.

Foreign National Hire or Guest

If you hire an employee or host a guest from a sensitive or terrorist-sponsoring country to perform work or research at the Laboratory, the processing requirements are?

Gate Access

The LBNL requirements for gate access are the same for nights and weekends as during the normal work week. (True, False)

Export Control

Do you know where to find information on export controls at Berkeley Lab?

Reporting Suspicious Activities

Do you know how to report inappropriate inquiries or incidents that you suspect involve foreign intelligence collection efforts or terrorists targeting activity against Berkeley Lab?

Spam Mail

Are you aware of the Laboratory's process to reduce unsolicited e-mail (spam)?

Wireless Network Connections

Are you connecting wireless access point equipment (e.g., Access Point, Mac Airport, etc.) that has not been approved by LBLnet onto the Laboratory network?

Cyber Security Incident Summary

Lists of incident by organization for 2003 and 2004.

CHANGED QUESTIONS

The following questions were changed slightly to make their intent clearer.

Crisis Action Team

Old question: Are you aware of the Crisis Action Team and whom to contact regarding workplace violence?

New question: Are you aware of the Laboratory's policy towards workplace violence and the contact numbers for the Crisis Action Team?

Password Policy

Old question: Do you change your password according to the LBNL password policy?

New question: When was the last time you changed your passwords?

Anti-virus Software

Old question: Is anti-virus software installed for all Macintosh or Windows computers you use?

New question: Are you aware of how to protect your computer against viruses?

EMPLOYEE SURVEY

The Self-Assessment began in July 2004. Every employee was sent a letter containing instructions for completing the ISSM survey. The survey was also publicized in the weekly e-mail newsletter *Today at Berkeley Lab*. Employees were encouraged to complete the survey during the next three weeks, concluding the process on August 6, 2004.

The employee survey (Appendix C) was designed as a tool, not a test. It was intended to gather baseline data to document the Laboratory's current security status, and also to educate employees about security issues. Care was taken to make the survey easy and quick. The survey questions were very carefully chosen to be both relevant and simple, and the number of questions was limited to 19.

The survey was designed primarily as a Web-based questionnaire, and hyperlinks were provided to assist staff in finding the information they needed to answer the questions correctly. A paper version of the survey was supplied to staff who do not have regular access to a computer. The survey was designed to be easily modified in the future to assess other target areas.

After August 6, when the initial survey phase of the Self-Assessment was completed, the ISSM liaisons were encouraged to examine the initial results for their organization and to follow up on the survey results with individual employees to improve awareness, resolve ambiguities, and remedy any problems uncovered by the questionnaire. Employees who had not participated in the survey were contacted and encouraged to complete the survey. This process continued until the division and organization directors reviewed their results in October 2004. The organization results were finalized on November 1, 2004.

In all, 90% of the staff completed the survey, 2% more than in 2002. This high rate of participation suggests a high level of awareness and commitment to security at the Laboratory. No significant technical problems in the survey process were reported. There was minimal need for individual help in completing the survey.

ORGANIZATIONAL PROFILES AND INSTITUTIONAL MATRIX

Results from the employee survey were combined with the cyber and physical security data to create organizational profiles for each Laboratory division and organization. Some results were given a rating of green, yellow, or red to give managers an indication of the level of performance. The rating criteria (Appendix D) were designed to be realistic and attainable. The organizational profiles (Appendix E) are Web-based and designed to be updated automatically with the latest survey results.

The institutional matrix (Appendix F) is a color-coded chart that summarizes all the organizational profiles, giving a quick picture of the Laboratory's overall performance. The survey results reflect increased employee knowledge and awareness of security issues, and identified information and processes requiring higher levels of protection, as discussed below.

RESULTS

OBSERVATIONS

AFRD, CSD, ENG, EH&S, FAC, ITSD, DIR, and PHYS all attained "solid green."

Except for the "wireless" questions, ALS, BSD, CRD, & COMP, also attained a green rating.

The following three question topics were noted as problem areas in the first survey. Results in this survey demonstrate significant improvement.

- Crisis action team
- CPP liaison
- Legal Requirements for software

Other topics that were "solid green" for the entire Laboratory were:

- Phone number
- Hiring from terrorist country
- Where to get office keys
- How to secure property
- Visitor access
- Export control
- Reporting suspicious activity
- How to protect against viruses
- How to reduce spam
- Backups

The following topics stand out as "problem areas" and will need future attention:

- Adherence to password policy
- Adherence to wireless network policy

ASSURANCE PROVIDED BY THE ASSESSMENT

CLASSIFIED INFORMATION

The first Self-Assessment question to staff was "Do you work with classified information[5] at LBNL?" In the initial, August 6, answers of 2,101 respondents, 20 stated that they worked with classified information. The division ISSM liaisons contacted all but three of these respondents and determined that none who were contacted actually worked on classified information at Berkeley Lab. The last three people were contacted directly by Dan Lunsford, the site property protection

[5] Staff were provided with hyperlinks (denoted in this report, particularly Appendix B, by underlined text) to the appropriate definitions and other information.

manager. He found them to be confused about the meaning of "classified information." While some LBNL staff do, in fact, work with classified material at other facilities, most of the erroneous answers came from a misunderstanding of the definition of classified information. It is significant that a very small number of those surveyed believed that they work with classified information at LBNL and that their mistaken understanding was corrected during the Self-Assessment process. The outcome of this survey question gives very high assurance that employees do not work on classified information at Berkeley Lab and that they know that they cannot bring classified work to the Laboratory.

CLEARANCE HOLDERS

Although no classified work or information is allowed at Berkeley Lab, a number of Laboratory staff hold security clearances sponsored by DOE/SC and other federal entities. There is no single agency that can provide Berkeley Lab with a comprehensive list of these clearance holders. In the past, periodic requests to staff have been used to develop a list of Laboratory clearance holders. Capturing all security clearance holder employees in our database was an important aspect of the Self-Assessment. At the time the Self-Assessment was conducted, DOE required that laboratories track all clearance-holder employees who host foreign nationals from sensitive countries.[6] The ISSM Self-Assessment accomplished this goal by identifying additional employees and guests who hold security clearances from other facilities. A more comprehensive list of clearance holders gleaned by this survey has been given to the Laboratory's counterintelligence officer for follow-up.

IMPROVEMENTS MADE DURING THE ASSESSMENT PROCESS

The organizational review and follow-ups by the ISSM liaisons to the initial staff survey results produced immediate improvements in the organization and institutional profiles. The total number of yellow ratings was reduced by 46%, and the total number of red was reduced by 62% (see Figure 3 and Appendix F).

[6] DOE O 142.3, "Unclassified Foreign Visits and Assignments," June 18, 2004.

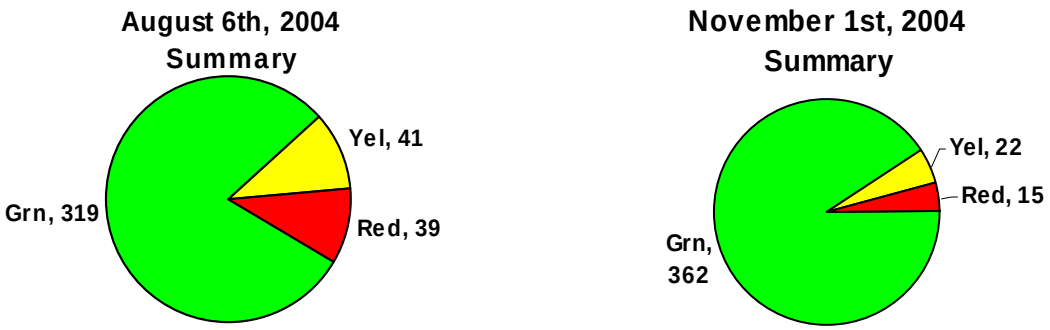


Figure 3. Institutional profile improvements resulting from organizational review and ISSM liaison follow-ups (22 organizations × 19 metrics).

CYBER SECURITY

Virus Protection

Running virus protection software is an important defense measure for Berkeley Lab considering the viruses that currently run rampant on the Internet. The questionnaire asked: "Are you aware of how to protect your computer against viruses?" The average response of 98% is excellent, gaining a 2% increase over the 2002 survey. This number confirms that most users realize the importance of running the software.

Legal Requirements for Obtaining Software

It is important that Berkeley Lab employees do not use software illegally. This survey question determines if employees know what is legal. The average rating of 92% is substantially higher than 2002's 85%. However, five divisions missed a "green" rating, indicating that there are still some who do not understand the Laboratory's policy.

Computer Protection Liaisons

Each Laboratory organization has a *computer protection liaison*, whose role is to assist the Computer Protection Program Manager in the administration of the Computer Protection Program. The goal of this question was to educate users that their division does, indeed, have a computer protection liaison to represent line management and assist in coordinating computer protection activities. In the 2002 survey this was noted as an area that needed improvement. The average of 87% is an encouraging improvement over the last survey's 77% rating.

Password Compliance

The purpose of this survey question is to ensure compliance with DOE password requirements. The 2002 survey asked the general question "Do you change your password according to the LBNL password policy?" and garnered a respectable 91% affirmative answer. The 2004 survey did not ask "if," but rather "when" were the passwords changed. Specifically, the question asked "When was the last time you changed your password?" and gave various time frames as choices. The most restrictive choice, "Less than 6 months ago," was the only time frame that meets Laboratory policy. This question garnered a low positive response of 73% and retained five "red" ratings and seven "yellow" ratings by the end of the survey. This indicates that there are many who are unable or unwilling to change their passwords within the required time frame. This is an area for further investigation.

Backups

All important information residing on a computer should be backed up, and the result of 95% affirming that backups are done is an improvement over the last survey, which gave an affirmative result of 92%. The use of the new ITSD backup service may have had an impact in raising this percentage.

Wireless Networking

Operating a wireless computer network poses a significant threat to the Laboratory's network integrity. Without proper administration, wireless networking can allow anyone with wireless networking capability to become a part of the Laboratory's network. Berkeley Lab's network group has set up a wireless networking service that has protective mechanisms to ensure that anyone connecting to this service will not cause security breaches. Laboratory policy states that all wireless services must be approved by the Laboratory's network group. Unfortunately, many Laboratory employees are unaware of this policy and have set up their own wireless services without the proper approval. This question identifies those employees who *think* they are operating an illegal wireless service. Since even a single illegal wireless service presents a significant risk, the rating on this metric required 100% compliance for a "green" rating. Anything less was deemed "red." This strict rating means that this metric garnered the highest number of "red" ratings (nine). However, this question has also created a specific list of employees to contact to resolve the wireless issue.

PHYSICAL PROTECTION

Protecting Laboratory Property

In response to the question "Do you take appropriate measures to secure the property assigned to you?" the survey indicated that 99% of Laboratory employees make a concerted effort to secure their property. The small number of thefts reported at the Laboratory supports this survey result and indicates employee diligence in protecting Berkeley Lab assets.

Requesting Visitor Access

A significant number of onsite staff (96%) understand how to request visitor access online. This is an improvement over the 2002 rating of 91%. Due to heightened security awareness after 9/11, the business need to request access for visitors has driven most employees to understand this process. The results of the survey indicate that a clear communication about visitor access processes occurred.

Crisis Action Team

In 2002, the question about the Crisis Action Team received the lowest percentage of "yes" answers (69%), indicating that information about the Crisis Action Team and other counseling resources should be more widely communicated by line management. This year's percentage of 88% shows that the communication efforts have been successful.

Proximity Card Access

Approximately 70% of Berkeley Lab employees currently use the card access system. As a result, an 85% survey response to the question ". . . do you know how to find the list of building authorizers in order to request access" is very good. However three "yellow" ratings indicated more employee education in this area is warranted.

Keys

Most individuals must have a key either to their building or to their office; 95% of employees know about the process to get keys.

Gate Access

Gate access has become more stringent since the 9/11 attack. Eighty-four percent of the Laboratory's staff now know that off-hour gate access has become more stringent. However, three "yellow" ratings indicate more employee education in this area is warranted.

FOREIGN NATIONALS AND EXPORT CONTROL

Historically, the Laboratory has not placed significant security emphasis on foreign nationality or work with other nations. However, with the recent threats of terrorist activity, Berkeley Lab has instituted a new policy to guard against those threats. Several questions were added to address these threats.

Hiring a Foreign National

New approvals must be obtained when hiring someone from a sensitive or terrorist-sponsoring country. These approvals often take a long time to acquire. Those who are unaware of the requirements may find that the person cannot be hired or cannot start work immediately. This often can cause significant problems. The survey indicates that 98% of the Laboratory staff are now aware of these hiring requirements.

Reporting Suspicious Inquiries or Incidents

With new threats of foreign intelligence collection efforts arising, it has become important that Laboratory staff know how to report such activities. The survey question pertaining to reporting these incidents has made 86% of the Laboratory aware of the process.

Export Control

Export control laws have been around for several years but, with the recent emphasis on restricting terrorist nations from obtaining potent U.S. technology, it is important that Berkeley Lab staff are aware of the Laboratory's policies concerning exports. This survey question has ensured that 82% of the Laboratory is aware of the policies.

GENERAL SECURITY AWARENESS

Emergency Telephone Number

Ninety-six percent of employees know the Laboratory's emergency telephone number. This high percentage reflects clear communication to personnel. All divisions rated very high in this category.

COMPARISON TO THE 2002 SELF-ASSESSMENT

Part of the purpose of the 2002 ISSM Self-Assessment was to set a baseline for Berkeley Lab security. Future assessment could gauge improvement on this baseline. Table 3 shows the change in the percentage ratings between 2002 and 2004.

Table 3. Changes in ratings: 2002 to 2004.

Survey Topic	2002 Positive Response (%)	2004 Positive Response (%)	Change (%)
Crisis Action Team	69	88	19
Prox Card Access	70	85	15
Computer Protection Liaisons	77	87	10
Obtaining Software	85	92	7
Requesting Visitor Access	91	96	5
Backups	92	95	3
Virus Protection	96	98	2
Emergency Phone Number	95	96	1
Protecting Lab Property	98	99	1
Keys	95	95	0
Password Compliance	91	73	–13

In the 2002 survey, the topics of *Crisis Action Team* and *Computer Protection Liaisons* were specifically noted in the action items as needing improvement. The significant change in each shows that improvement has, indeed, been made.

The marginal changes of a few percent can be attributed to a number of ancillary reasons such as changes in Laboratory population. However, the overall upward trend of all but one category seems to indicate that security awareness and knowledge imparted by the Laboratory's security program and, specifically, by the Self-Assessment process, has been effective.

The one negative issue of Password Compliance was likely driven down by the change in the question and indicates a problem area that needs to be rectified.

CONTINUOUS IMPROVEMENT PLAN

IMPROVEMENT OF THE SELF-ASSESSMENT PROCESS

Experience in carrying out the first ISSM Self-Assessment and suggestions from survey participants identified several ways in which the process can be improved in the future.

SURVEY POPULATION

Who should be included in the ISSM Self-Assessment survey? Answering this question is not as easy as one might initially expect.

Faculty and visiting post-docs were excluded from the 2002 survey because it was assumed they spend little time onsite, but all participating guests were initially included. RPM §1.06 provides clear definitions of participating guests: users of Laboratory User Facilities, scientific collaborators, students, nonscientific temporary or contract employees, and consultants. These guests, unlike casual visitors, should have a basic understanding of Laboratory safety and security measures.

In the 2002 survey, it was discovered that many who hold a faculty or visiting post-doc status often spend a significant amount of their time "on the hill" (for instance, several of the division directors hold a *faculty* status). It was also discovered that the guest category, in practice, is loosely defined and may overlap with the definition of a casual visitor. Ultimately, the 2002 assessment excluded many *guests*, who rarely actually visit the Laboratory.

In 2004, the categories and methodologies for defining and assigning status had not changed from the 2002 practices and posed the same dilemmas. For the 2004 Self-Assessment, it was decided to include all categories, except for guests. Guests who spent time at the Laboratory could take the survey, thereby increasing the overall security awareness of the general Laboratory population, but the absence of guest participation would not count against a division's *ratings*. The question of who is included in the survey was the primary source of logistic problems in the 2004 process.

In a hindsight analysis of the assessment process, we now believe that the highest impact of the assessment comes from participation by those who routinely work onsite on a continuous basis. There is no Laboratory *status* that categorizes the Laboratory populous by physical time spent onsite. Hence, Laboratory *status* has been the wrong criterion to use for determining survey participation. It is anticipated that the next survey will use an opening question that will determine if the user spends a significant amount of time on site. If a user does not work on site for a substantial amount of time during the year, he or she will be able to disregard the rest of the survey and will not be counted as a participant.

STAFF COMMUNICATION METHODS

Secure communication with staff and guests who have LDAP usernames and passwords is easily accomplished, but communication with staff and guests without LDAP usernames is more problematic.[7] In both the 2002 and 2004 ISSM Self-Assessment surveys, both LDAP users and non-LDAP users participated. The participation of non-LDAP users was accomplished by dissemination of paper copies of the survey. Compared with the computer-only survey, the paper-plus-data-entry method increased the cost of the Self-Assessment and introduced a greater potential for errors. In 2002, Facilities and Engineering were the two divisions with prominent numbers of non-LDAP employees. After 2002, the Engineering Division resolved to have all of their employees sign up for LDAP accounts by 2004. This alleviated a great deal of the administrative effort during the 2004 survey. Since LDAP is used for many other Laboratory functions besides the ISSM Self-Assessment, this issue needs to be addressed from a Laboratory-wide perspective.

RAISING THE BAR

As with the 2004 Self-Assessment, continuing improvements in security will be encouraged by making the rating criteria more stringent in future Self-Assessments. Expectations of continued improvement will generate expectations of excellent security.

NEW TARGETED QUESTIONS

Security threats to the Laboratory change, and it is important that the ISSM program address the most prominent threats, not simply the threats that have existed in the past. It is also important to keep the questionnaire short to encourage a high response rate and promote good retention of the material presented. These two factors mean that the topic areas of future surveys will continue to change as needed. New questions about newly developing threats will be added and questions that don't seem to add substantial improvement to the security of the Laboratory will be dropped.

CONTINUOUS RATHER THAN PERIODIC

It has been suggested that the ISSM Self-Assessment survey be incorporated as a continuous process, whereby the schedule for taking the survey is based on an individual employees periodic requirements, not a Laboratory-wide survey *window*. This concept would be similar to the EH&S ISM requirements for individual periodic training. It has also been suggested that the ISSM survey could be part of the EH&S training process. While many aspects of the survey are simplified by a

[7] LDAP, which stands for Lightweight Directory Access Protocol, is an Internet standard database. At Berkeley Lab, LDAP is the primary database for the telephone directory, IMAP4 e-mail, online calendar, Novell networking, employee self-service, and other functions. Everyone with an employee number is entered into LDAP, but not all employees have LDAP usernames/passwords, which would give them secure computer access to LDAP-based Laboratory services.

continuous process, there are some difficulties with such a system, such as changing questions, changing ratings, year-round administration, and clear, equivalent metrics for gauging improvement. While continuous evaluation may be beneficial, it is an option that needs to be evaluated closely.

IMPROVEMENT OF THE LABORATORY'S SECURITY PROGRAM

The Self-Assessment results identified several areas of the Laboratory's security program that need improvement. These areas are discussed below.

PASSWORD COMPLIANCE

It is clear from the survey results that many employees are not in compliance with the Laboratory policy to change passwords every six months. Several divisions rated "yellow" and "red" on this metric, even after the *corrections period* had passed. This seems to indicate that a number of people are unwilling to change their passwords irrespective of the policy. This policy and the reasons for this high level of noncompliance need to be reviewed. If the policy is deemed to be unworkable, it should be modified. If it is found to be workable, it should be enforced through technical or administrative means.

WIRELESS

Wireless computer networking is a relatively new technology that has become cheap and easy for the individual to implement. Unfortunately, allowing employees to set up their own wireless networks has several serious drawbacks. Having hundreds of small networks as opposed to a single, centrally managed network is financially unsound, technologically confusing, and presents a significant computer security risk. In recent years, a centralized wireless service for the Laboratory has been built and a policy has been implemented requiring prior authorization for wireless systems at the Laboratory. The survey reveals that there are still those who are unaware of this policy. As a follow-up to the Self-Assessment, all of those who claim to be running wireless services will be contacted. We suspect many misunderstood the question and are not actually running services. Those who we find actually are running services will be asked to justify why the central system does not suffice, or will be shut down.

PROXIMITY CARD, GATE ACCESS, AND SOFTWARE LICENSE

Although the overall average percentages are high in each of these areas, some remaining "yellows" in specific divisions indicated that further employee education may be warranted. The education efforts may have to target the specific divisions that retained low ratings.

IMPROVEMENT OF RELATED LABORATORY-WIDE PROCESSES

STAFF COMMUNICATION METHODS

As discussed above, secure communication with staff and guests who have LDAP usernames is easily accomplished, but communication with staff and guests without LDAP usernames is more expensive and, in cases like the Self-Assessment survey, more susceptible to error. Some staff do not have LDAP usernames because they do not use a computer in their everyday work, some may use computer systems that are not compatible with LDAP, and some may simply choose not to have an LDAP username.

The 2002 ISSM Self Assessment report noted that many Laboratory functions depend on LDAP authentication (e.g., calendar, e-mail, Human Resources data, vehicle registration, and other functions). That report recommended that Laboratory management adopt LDAP usernames and passwords as the Laboratory standard for authentication and access to institutional resources for all employees and guests. As a result, all new employees are automatically issued an LDAP username and password when they are issued their Laboratory badge. *We encourage this effort to make the LDAP authentication ubiquitous throughout Berkeley Lab and recommend that it now extend to current employees who still do not possess an LDAP password.*

ACTION ITEMS

LINE MANAGEMENT

- Continue to adopt LDAP usernames and passwords as the Laboratory standard for authentication and access to institutional resources for all employees and guests. Other access methods will not be supported.
- Ensure that all employees and guests have LDAP usernames and access to a networked computer.

ISSM STAFF

- Require LDAP usernames and passwords for all employees and guests participating in the next Self-Assessment Survey.
- Assess the existing password policy and either change the policy or use technical and/or administrative means to enforce the requirement to change passwords every six months.
- Contact all those who claim to be running wireless network services and either correct their notion of “a wireless service,” justify their need for their own wireless network, or shut down their wireless service.

- Develop and implement an awareness program concerning gate access, proximity cards, and software license.

APPENDIX A: INTEGRATED SAFEGUARDS AND SECURITY MANAGEMENT PLAN

Contents

Final
Effective Date: April 16, 2001

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

PREPARED FOR THE U.S. DEPARTMENT OF ENERGY UNDER
CONTRACT NUMBER DE-AC03-76SF00098

Approved By:

Charles V. Shank
Director
Lawrence Berkeley National Laboratory

Richard H. Nolan
Director & Site Manager
DOE Berkeley Site Office

Approved By:

Functional Managers

A.X. Merola
Division Director
Information Technologies and Services Division

Donald W. Bell
Property Protection, Life Safety Manager
Environment, Health and Safety Division

Cheryl A. Fragiadakis
Technology Transfer Department Head
Technology Transfer Department

David J. Aston
Export Control Officer
Directorate

Guy Bear
(Acting) Human Resources Head
Human Resources Department

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
Appendix B. Cyber Security Protection Plan
Appendix C. Export Control Document
Appendix D. Counter Intelligence Plan
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.

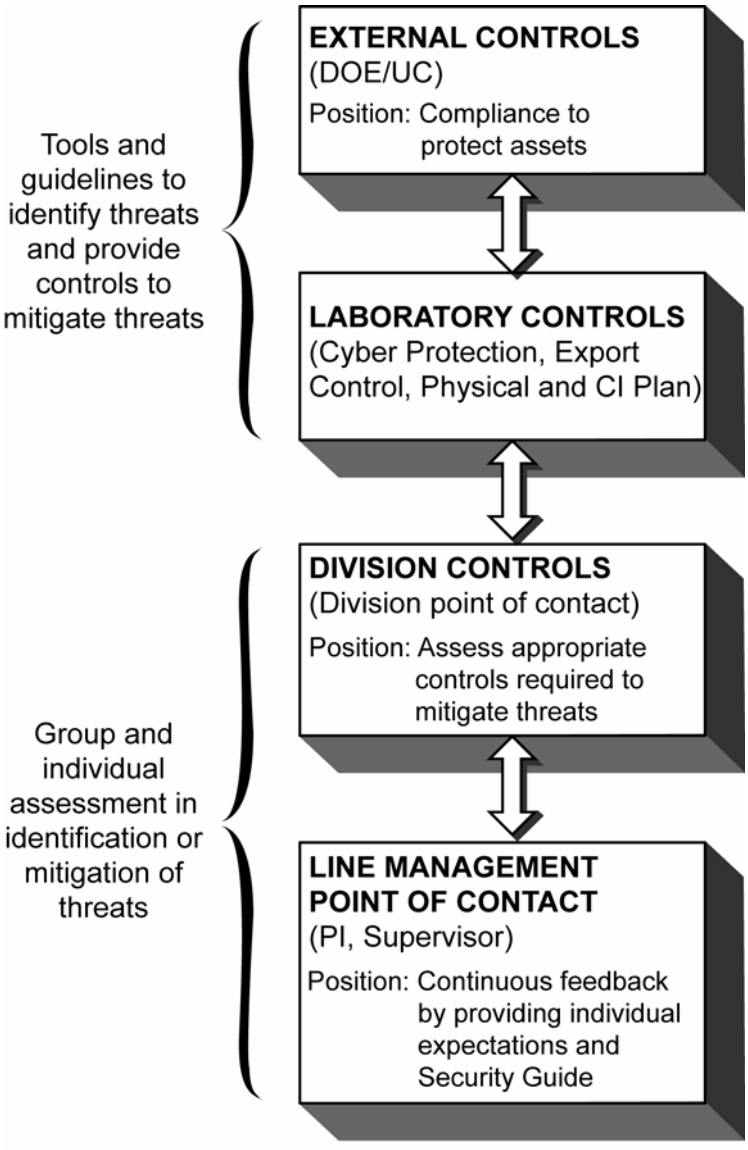


Figure A. Integrated Controls

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.

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.

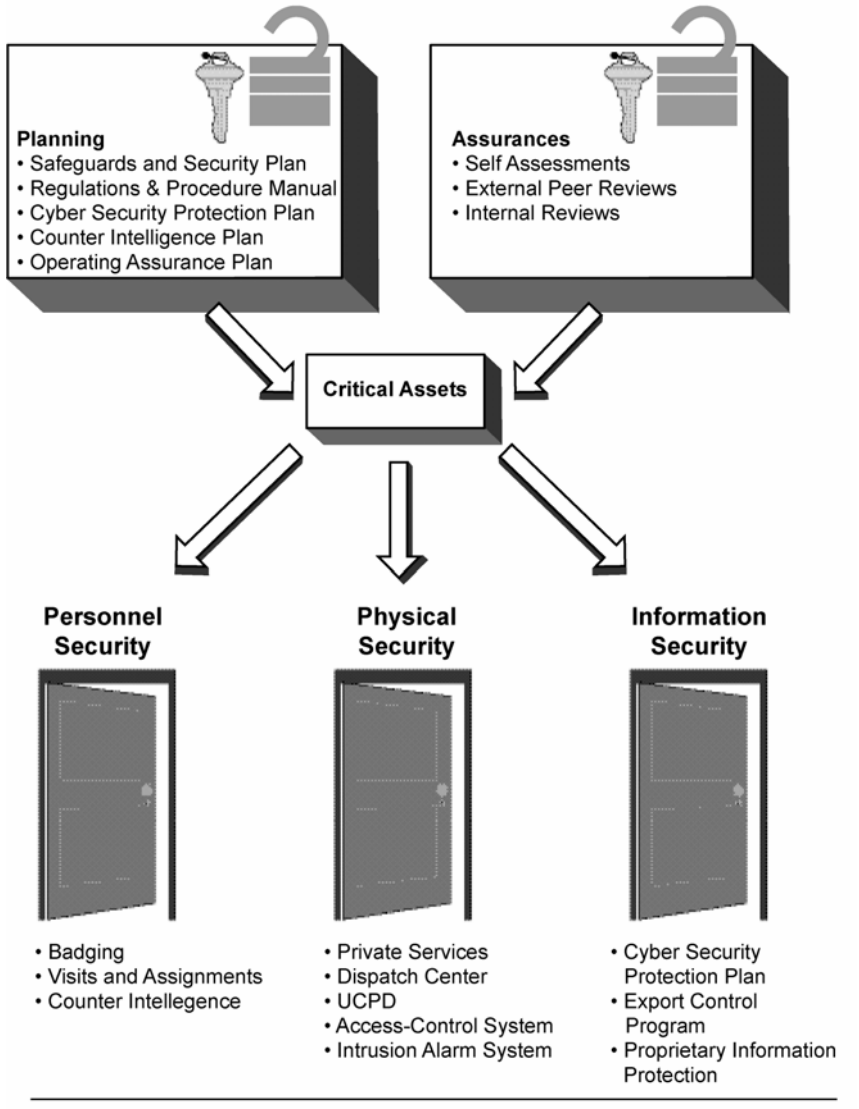


Figure B. Berkeley Lab employs integrated security elements to protect critical assets.

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.

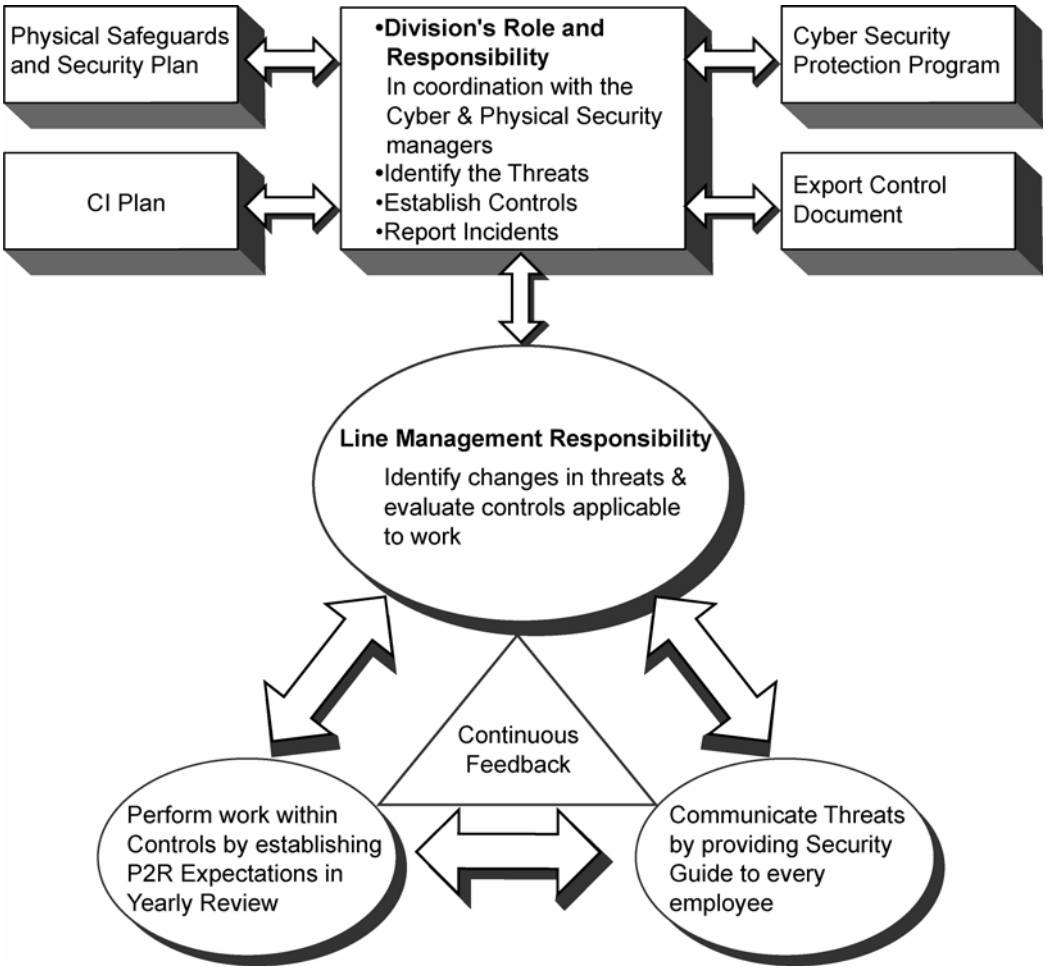


Figure C. Roles and responsibilities of an Integrated Security Management Plan.

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:

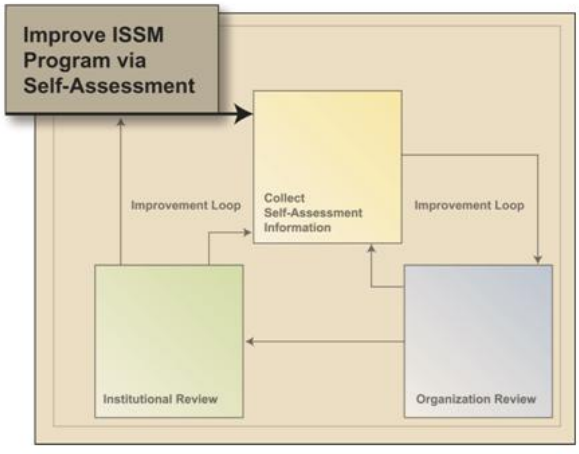
- Line management owns security.
- Security roles and responsibilities are clearly defined and communicated.
- Security functions are integrated.
- An open environment supports the Laboratory's Mission.
- The security program must support the scientific and operational missions of the Laboratory and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

APPENDIX B: SELF-ASSESSMENT PROCESS (PRESENTATION FORM)

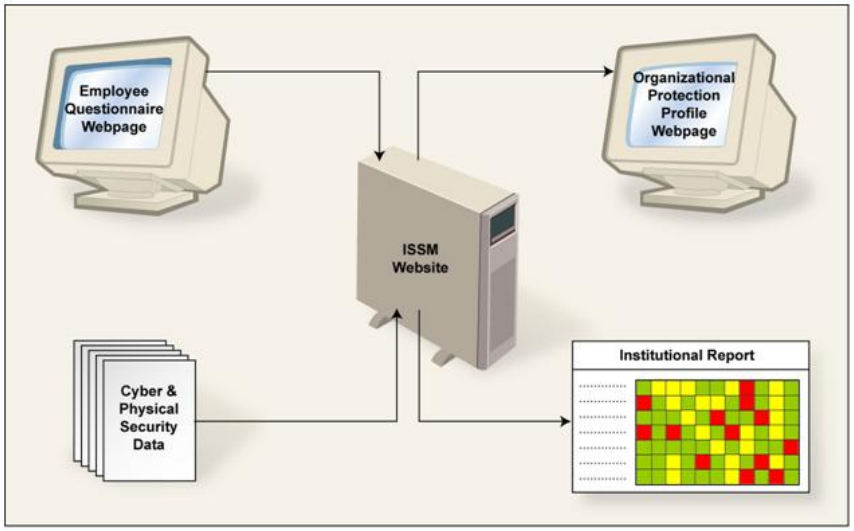
ISSM Self-Assessment 2004

Self-Assessment Development Goals

- Same Goals as in 2002
- Provide a baseline measurement of security
- Educate lab staff
- Provide security staff with feedback
- Provide management with information to make knowledgeable decisions

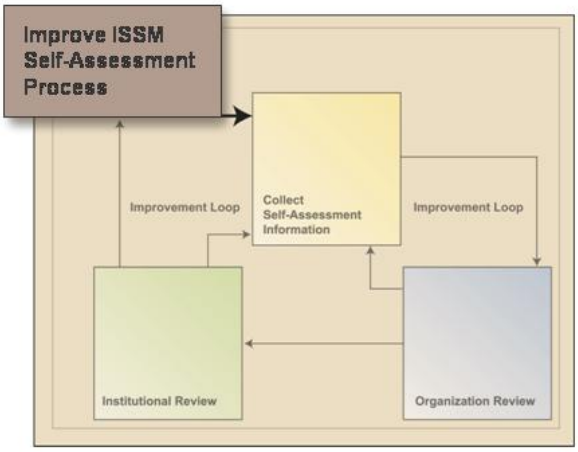


ISSM Self-Assessment Components



Survey Improvements & Changes Since 2003

- **Outdated topics removed**
- **Rating criteria increased (raise the bar)**
- **Weak questions reworded**
- **New questions for new risks**



Survey Improvements: Outdated Topics Removed

- DOE Sensitive Information and Critical Systems
  - 2002 identification process still valid
- Cracked Passwords
  - Replaced by continuous, year-around cracking
- System Vulnerabilities
  - Replaced by continuous, year-around scanning
- DOE Warning Banners
  - No longer a significant issue
- Thefts
  - Reported through several other venues
- Security Access Managers
  - 2002 identification process still valid
- Employee Security Guide
  - Deemed not cost effect to distribute at each assessment

Survey Improvements: Ratings Increased

Question topic	Old Rating (yellow range)	New Rating (yellow range)
Emerg. Phone Number	85% - 60%	90% - 65%
Proximity Card access	70% - 50%	80% - 60%
Office Keys	70% - 50%	80% - 60%
Securing Lab Property	85% - 60%	90% - 65%
Visitor Access	85% - 60%	90% - 65%
Crisis Action Team	70% - 50%	70% - 60%
Software Licenses	85% - 60%	90% - 65%
Password Policy	70% - 50%	80% - 60%
Virus Protection	85% - 60%	80% - 60%
Backups	70% - 50%	80% - 60%

Survey Improvements: Questions Changed

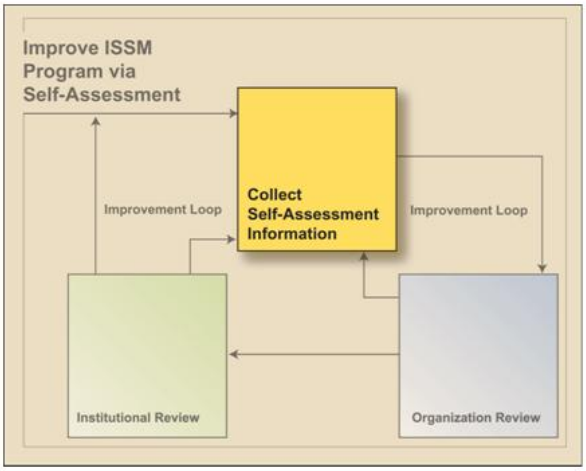
- Crisis Action Team
  - Directed towards knowing the Lab's policy, not people
- Password Policy
  - Directly asks if policy is being followed
- Anti-virus Software
  - Asked "do you know how?", not "have you installed?"

Survey Improvements: New Topics Added

- Foreign National Guests and New Hires
  Do you know the requirements?
- Export Control
  Do you know were to find information?
- Reporting Suspicious Activities
  Report intelligence collection or terrorist activity
- Gate Access
  Do you know the requirements?
- Spam Mail
  Are you aware of the Lab's spam reduction processes?
- Wireless Network Connections
  Are you using approved equipment?

2004 Data Collection Process

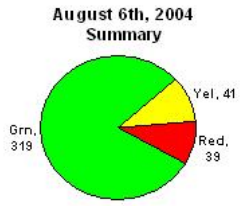
- Survey was completed On August 6th, 2004
- ISSM Security Liaisons followed up on survey results
- Organization results were finalized on November 1st, 2004



Data Collection Was Successful

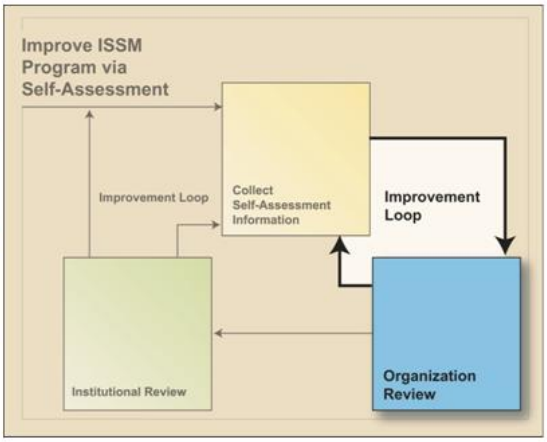
- 3014 staff completed the survey (90%)
- No significant technical problems
- Minimal need for individual help
- As in 2002, most problems involved participation by guests.

Organizational Review Drives Immediate Improvement



Reds reduced by 61%

Yellows reduced by 46%



Organization Performance August 2004

August Chart

Classified	Phone	Prox Card	Hire FN	Keys	Secure Prop	Gate Access	Visitor Access	Crisis Team	Export Control	Suspicious	Software	Password	Virus Prot	Spam	CP Liaision	Backup	Wireless
1	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
100%	100%	80%	100%	98%	98%	86%	98%	86%	90%	86%	96%	56%	100%	96%	84%	96%	96%
100%	97%	89%	96%	91%	98%	84%	97%	83%	79%	76%	90%	53%	98%	93%	84%	93%	98%
98%	96%	89%	98%	97%	99%	78%	97%	93%	80%	89%	92%	82%	97%	96%	89%	90%	97%
98%	89%	89%	96%	92%	96%	92%	91%	82%	71%	76%	89%	44%	96%	85%	71%	100%	100%
97%	97%	80%	98%	92%	100%	84%	95%	84%	83%	85%	98%	81%	98%	95%	90%	97%	97%
100%	100%	88%	100%	100%	100%	88%	88%	88%	88%	100%	100%	88%	100%	100%	88%	88%	88%
99%	88%	77%	97%	91%	98%	79%	96%	81%	77%	81%	89%	57%	100%	97%	85%	98%	99%
100%	98%	87%	94%	98%	99%	86%	98%	91%	83%	89%	93%	75%	98%	98%	87%	93%	98%
100%	100%	91%	92%	97%	98%	78%	98%	95%	74%	85%	86%	74%	96%	92%	89%	85%	100%
100%	96%	90%	98%	98%	98%	84%	97%	92%	81%	84%	92%	74%	100%	94%	92%	98%	99%
97%	95%	87%	95%	96%	99%	78%	95%	93%	65%	79%	78%	74%	92%	90%	87%	84%	100%
100%	92%	83%	98%	96%	100%	75%	96%	90%	84%	89%	93%	55%	100%	95%	85%	89%	96%
99%	97%	90%	98%	95%	99%	84%	99%	92%	84%	92%	93%	80%	99%	100%	96%	98%	100%
100%	92%	62%	93%	86%	95%	68%	86%	70%	59%	65%	68%	88%	95%	86%	66%	87%	98%
97%	94%	88%	96%	96%	98%	82%	94%	86%	78%	82%	91%	47%	96%	92%	78%	93%	98%
98%	93%	80%	99%	94%	98%	84%	93%	74%	70%	75%	85%	45%	99%	91%	73%	93%	100%
100%	95%	90%	100%	95%	100%	81%	100%	95%	90%	97%	97%	90%	100%	100%	95%	100%	100%
100%	98%	74%	96%	89%	100%	82%	96%	79%	70%	74%	84%	43%	94%	100%	70%	93%	100%
100%	100%	75%	95%	90%	100%	85%	95%	85%	85%	85%	90%	80%	100%	95%	85%	100%	95%
100%	97%	84%	95%	95%	92%	74%	92%	80%	81%	77%	90%	52%	100%	94%	82%	97%	100%
100%	93%	78%	98%	95%	100%	92%	98%	86%	76%	84%	92%	61%	100%	95%	87%	93%	98%

Organization Performance November 2004

November Chart

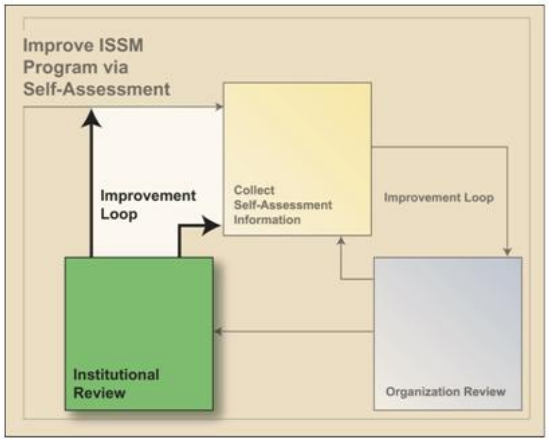
	Classified	Phone	Prox Card	Hire FN	Keys	Secure Prop	Gate Access	Visitor Access	Crisis Team	Export Control	Suspicious	Software	Password	Virus Prot	Spam	CP Liaision	Backup	Wireless
	1	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
AF	100%	97%	78%	100%	97%	98%	87%	96%	86%	85%	80%	92%	84%	100%	96%	76%	95%	100%
AL	100%	100%	91%	97%	92%	98%	84%	97%	85%	78%	74%	90%	79%	98%	94%	86%	94%	98%
BU	100%	97%	89%	96%	97%	99%	89%	97%	93%	78%	89%	94%	82%	97%	95%	89%	92%	99%
CH	100%	93%	92%	100%	96%	100%	86%	95%	87%	81%	87%	95%	83%	98%	87%	92%	96%	100%
CR	100%	96%	80%	100%	92%	100%	86%	95%	86%	82%	84%	97%	78%	98%	97%	91%	97%	96%
CS	100%	100%	84%	100%	100%	100%	92%	92%	92%	92%	100%	100%	84%	100%	100%	100%	100%	92%
EE	100%	90%	81%	97%	89%	97%	83%	97%	83%	75%	81%	96%	56%	99%	95%	82%	97%	100%
EG	100%	98%	86%	94%	98%	99%	83%	98%	91%	82%	88%	91%	90%	97%	96%	86%	90%	100%
EH	100%	100%	92%	93%	99%	100%	89%	99%	95%	76%	87%	89%	79%	95%	93%	86%	88%	100%
ES	100%	96%	89%	98%	97%	98%	88%	97%	94%	84%	87%	92%	73%	100%	96%	91%	98%	99%
FA	100%	99%	95%	97%	98%	100%	88%	99%	98%	91%	90%	94%	92%	98%	96%	97%	97%	100%
GN	100%	95%	86%	98%	98%	100%	76%	96%	90%	87%	87%	93%	54%	100%	95%	85%	92%	96%
IC	100%	97%	90%	97%	95%	99%	83%	98%	91%	82%	90%	93%	80%	99%	100%	96%	97%	100%
LD	100%	94%	82%	100%	91%	100%	85%	91%	82%	79%	85%	79%	73%	97%	94%	88%	88%	100%
LS	100%	94%	85%	96%	95%	98%	82%	94%	84%	76%	80%	89%	45%	96%	91%	76%	93%	99%
MS	98%	93%	81%	98%	93%	98%	83%	93%	79%	75%	78%	86%	43%	98%	91%	74%	91%	98%
NE	100%	96%	88%	100%	96%	100%	77%	98%	94%	89%	98%	98%	93%	100%	100%	94%	100%	100%
NS	100%	94%	77%	97%	91%	98%	83%	95%	76%	70%	78%	83%	66%	96%	95%	77%	93%	100%
OP	100%	100%	77%	95%	90%	100%	86%	95%	86%	86%	86%	90%	72%	100%	95%	86%	100%	95%
PB	100%	97%	88%	96%	97%	92%	76%	95%	84%	84%	84%	92%	52%	100%	96%	82%	97%	100%
PH	100%	92%	81%	98%	92%	100%	90%	96%	86%	82%	85%	90%	83%	98%	95%	88%	91%	100%

Assurance

- Lab does not have CLASSIFIED information on site
- All security clearance holders have been identified
- Lab staff is aware of major policy

Institutional Review Drives Continuous Improvement

- **Baseline bar raised**
- **2002 issues resolved**
- **Areas for ISSM and Self-Assessment improvement have been identified**



Improvement Since 2002

Survey Topic	2002 Positive Response	2004 Positive Response	Change
Crisis Action Team*	69%	88%	19%
Prox Card Access	70%	85%	15%
Computer Protection Liaisons*	77%	87%	10%
Obtaining Software	85%	92%	7%
Requesting Visitor Access	91%	96%	5%
Backups	92%	95%	3%
Virus Protection	96%	98%	2%
Emergency Phone Number	95%	96%	1%
Protecting Lab Property	98%	99%	1%
Keys	95%	95%	0%
Password Compliance	91%	73%	-13%

* **Recognition of the *Crisis Action Team* and *Computer Protection Liaisons* were specifically noted in the 2002 survey as needing improvement. The 2004 survey confirms improvement efforts were effective.**

Completed Actions as a Result of 2002 Assessment

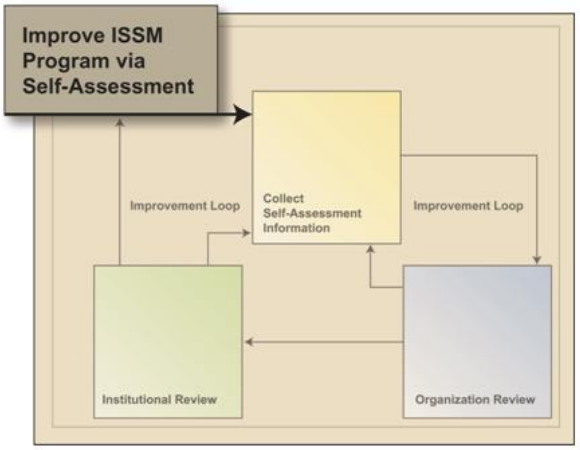
- Assisted line management in creating individual protection plans for targeted data and/or systems that need extra protection
- Adapted LDAP passwords as a Lab standard, now issued to ALL new employees
- Improved employee awareness of Crisis Action Team and CPIC Liaisons
- Computer data backup capability provided by ITSD to improve data backup

New Targets for 2005

- Improve conformance to Lab's password policy
- Improve conformance to Lab's wireless computing policy
- Continue to propagate the LDAP authentication mechanism as a Lab Standard

Self-Assessment Goals Achieved!

- **Provide a baseline measurement of security**
- **Weaknesses identified in 2002 strengthened**
- **Educate lab staff**
- **Provide security staff with feedback**
- **Provide management with information to make knowledgeable decisions**



APPENDIX C: ISSM DIVISION SELF-ASSESSMENT QUESTIONNAIRE

Employee/Guest Name: _____ Date: _____

Employee/Guest ID Number: _____ Division: _____

Q1. Do you work with Classified Information at LBNL?

- ☐ Yes
- ☐ No

Q2. Do you currently hold a security clearance that allows access to classified information?

- ☐ Yes
- ☐ No

Q3. Do you know the emergency phone number for the Laboratory?

- ☐ Yes
- ☐ No

Q4. If a building has the proximity card access system, do you know where to find the list of building authorizers in order to request access?

- ☐ Yes
- ☐ No

Q5. If you hire an employee or host a guest from a sensitive or terrorist-sponsoring country to perform work or research at the Lab, the processing requirements are:

- ☐ No different from U.S. citizens
- ☐ The same for sensitive and terrorist country nationals and require no special approvals
- ☐ Different for sensitive and terrorist country nationals and require approvals from Lab management and DOE

Q6. Do you know whom to contact regarding keys to your office building?

- ☐ Yes
- ☐ No

Q7. Do you take appropriate measures to secure the property assigned to you?

- ☐ Yes
- ☐ No

Q8. The LBNL requirements for gate access are the same for nights and weekends as during the normal work week.

- ☐ True
- ☐ False

Q9. Do you know how to request access for your visitors?

- ☐ Yes
- ☐ No

Q10. Are you aware of the Lab's policy towards workplace violence and the contact numbers for the Crisis Action Team?

- ☐ Yes
- ☐ No

Q11. Do you know where to find information on export controls at Berkeley Lab?

- ☐ Yes
- ☐ No

Q12. Do you know how to report inappropriate inquiries or incidents that you suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab?

- ☐ Yes
- ☐ No

Q13. Do you know the Lab's legal requirements for obtaining software?

- ☐ Yes
- ☐ No
- ☐ I do not use a computer

Q14. When was the last time you changed your passwords?

- ☐ Over a year ago
- ☐ 9 months to one year ago
- ☐ 6 months to 9 months ago
- ☐ Less than 6 months ago
- ☐ I do not use a computer

Q15. Are you aware of how to protect your computer against viruses?

- ☐ Yes
- ☐ No
- ☐ I do not use a computer

Q16. Are you aware of the Lab's process to reduce unsolicited e-mail (spam)?

- ☐ Yes
- ☐ No
- ☐ I do not use a computer

Q17. Do you know who your Computer Protection Liaison is?

- ☐ Yes
- ☐ No
- ☐ I do not use a computer

Q18. Do you back up all information that you deem important to your work?

- ☐ Yes

- ☐ No
- ☐ I do not use a computer

Q19. Are you connecting wireless access point equipment (e.g., Access Point, Mac Airport, etc.) that has not been approved by LBLnet onto the Lab network?

- ☐ Yes
- ☐ No

APPENDIX D: PERFORMANCE RATING CRITERIA

Question or statistic	Green	Yellow	Red
Employees in Division who have completed the Self-Assessment Questionnaire	>80%	79-60%	<60
Do you work with classified information at LBNL?	0%	N/A	>0%
Do you currently hold a security clearance that allows access to classified information?	N/A	N/A	N/A
Do you know the emergency phone number for the Laboratory?	>90%	89-65%	<65
If a building has the proximity card access system, do you know where to find the list of building authorizers in order to request access?	>80%	79-60%	<60
If you hire an employee or host a guest from a sensitive or terrorist-sponsoring country to perform work or research at the Lab, the processing requirements are: No different from US citizens/The same for sensitive and terrorist country nationals and require no special approvals/Are different for sensitive and terrorist country nationals and require approvals from Lab management and DOE	>80%	79-60%	<60
Do you know whom to contact regarding keys to your office building?	>80%	79-60%	<60
Do you take appropriate measures to secure the property assigned to you?	>90%	89-65%	<65
The LBNL requirements for gate access are the same for nights and weekends as during the normal work week. [True/False]	>80%	79-60%	<60
Do you know how to request access for your visitors?	>90%	89-65%	<65
Are you aware of the Lab's policy towards violence in the workplace and the contact numbers for the Crisis Action Team?	>70%	69-50%	<50
Do you know where to find information on export controls at Berkeley Lab?	>70%	69-50%	<50
Do you know how to report inappropriate inquiries or incidents that you suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab?	>70%	69-50%	<50
Do you know the Lab's legal requirements for obtaining software?	>90%	89-65%	<65
When was the last time you changed your passwords? Over a year ago/9 months to one year ago/6 months to 9 months ago/Less than 6 months ago	>80%	79-60%	<60
Are you aware of how to protect your computer against viruses?	>80%	79-60%	<60
Are you aware of the Lab's process to reduce unsolicited e-mail (spam)?	>70%	69-50%	<50
Do you know who your Computer Protection Liaison is?	>70%	69-50%	<50
Do you back up all information you deem important to your work?	>80%	79-60%	<60
Are you connecting wireless access point equipment (e.g., Access Point, Mac Airport, etc.) that has not been approved by LBLnet onto the Lab network?	0%	N/A	>0%

APPENDIX E: ORGANIZATIONAL PROFILES

Accelerator & Fusion Research Division Information

Division Director:	Gough, Richard A		
ISSM Liaison:	Mitschang, Linda F		
CPP Liaison:	Chew, Joseph T		
Security Access Managers:	Kono, Joy N		
Employees in Division (as surveyed):	105		
Results of Survey Questions			
	Employees Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	95		90.55%
	Employees Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	93		97.85%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	75		78.95%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	95		100%
Employees who know whom to contact regarding keys to their office or building:	93		97.85%
Employees who take appropriate measures to secure the property assigned to them:	94		98.95%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	86		87.35%
Employees who know how to request visitor access:	92		96.8%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	82		86.3%
Employees who are familiar with export controls at Berkeley Lab:	82		85.25%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	77		81.05%
Employees who know the Lab's legal requirements for obtaining software:	88		92.6%
Employees who change their passwords according to the LBNL password policy:	80		84.2%
Employees who are aware of how to protect their computer against viruses:	95		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	92		96.8%
Employees who know who their CPP Liaison is:	73		76.8%
Employees who back up all information they deem important to their work:	91		95.75%
Employees who have an LBLnet-approved connection on their wireless network equipment:	95		100%

Advanced Light Source Division Information

Division Director:	Kirz, Janos		
ISSM Liaison:	Dixon, Bernadette B.		
CPP Liaisons:	Biocca, Alan K. Williams, Eric C.		
Security Access Managers:	Denlinger, Jonathan Troutman, Jeffrey		
Employees in Division (as surveyed):	110		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	89		87.5%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	89		100%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	82		92.1%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	87		97.75%
Employees who know whom to contact regarding keys to their office or building:	83		93.25%
Employees who take appropriate measures to secure the property assigned to them:	88		98.85%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	76		85.35%
Employees who know how to request visitor access:	88		98.85%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	77		86.5%
Employees who are familiar with export controls at Berkeley Lab:	70		78.65%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	68		76.4%
Employees who know the Lab's legal requirements for obtaining software:	80		89.85%
Employees who change their passwords according to the LBNL password policy:	72		80.9%
Employees who are aware of how to protect their computer against viruses:	88		98.85%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	84		94.35%
Employees who know who their CPP Liaison is:	78		87.6%
Employees who back up all information they deem important to their work:	83		93.25%
Employees who have an LBLnet-approved connection on their wireless network equipment:	88		98.85%

Business Services Division Information

Division Director:	McGraw, David C.		
ISSM Liaison:	Chen, David T. Coolahan, Cynthia C. Paris, Karen M. Wuy, Linda D.		
CPP Liaisons:	Clary, Mary M. Guerrero, Daisy C. Speros, John P.		
Security Access Managers:	Attia, Diana M. Matyas, Linda J. Wuy, Linda D.		
Employees in Division (as surveyed):	448		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	448		100%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	437		97.5%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	400		89.25%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	434		96.85%
Employees who know whom to contact regarding keys to their office or building:	438		97.75%
Employees who take appropriate measures to secure the property assigned to them:	446		99.55%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	401		89.5%
Employees who know how to request visitor access:	435		97.1%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	419		93.5%
Employees who are familiar with export controls at Berkeley Lab:	355		79.2%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	401		89.5%
Employees who know the Lab's legal requirements for obtaining software:	427		95.3%
Employees who change their passwords according to the LBNL password policy:	375		83.7%
Employees who are aware of how to protect their computer against viruses:	436		97.3%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	430		95.95%
Employees who know who their CPP Liaison is:	399		89.05%
Employees who back up all information they deem important to their work:	413		92.15%
Employees who have an LBLnet-approved connection on their wireless network equipment:	447		99.75%

Chemical Sciences Division Information

Division Director:	Neumark, Daniel M.		
ISSM Liaison:	Gill, Angela A.		
CPP Liaisons:	Booth, Corwin H.		
Security Access Managers:	Lukens Jr., Wayne W. Shuh, David K.		
Employees in Division (as surveyed):	72		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	68		99.75%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	64		94.1%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	63		92.65%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	68		100%
Employees who know whom to contact regarding keys to their office or building:	66		97.05%
Employees who take appropriate measures to secure the property assigned to them:	68		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	59		86.75%
Employees who know how to request visitor access:	65		95.55%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	60		88.2%
Employees who are familiar with export controls at Berkeley Lab:	56		82.35%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	60		88.2%
Employees who know the Lab's legal requirements for obtaining software:	64		95.1%
Employees who change their passwords according to the LBNL password policy:	57		83.8%
Employees who are aware of how to protect their computer against viruses:	67		98.5%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	60		88.2%
Employees who know who their CPP Liaison is:	63		92.65%
Employees who back up all information they deem important to their work:	66		97.05%
Employees who have an LBLnet-approved connection on their wireless network equipment:	68		100%

Computational Research Division Information

Division Director:	Simon, Horst D.		
ISSM Liaison:	Ramsey, Dwayne		
CPP Liaisons:	Smith III, George D.		
Security Access Managers:	Dooly, Martin K.		
Employees in Division (as surveyed):	112		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	98		87.5%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	95		96.9%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	80		81.6%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	98		100%
Employees who know whom to contact regarding keys to their office or building:	91		92.85%
Employees who take appropriate measures to secure the property assigned to them:	98		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	85		86.7%
Employees who know how to request visitor access:	94		95.9%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	85		86.7%
Employees who are familiar with export controls at Berkeley Lab:	82		83.65%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	83		84.65%
Employees who know the Lab's legal requirements for obtaining software:	96		97.95%
Employees who change their passwords according to the LBNL password policy:	78		79.55%
Employees who are aware of how to protect their computer against viruses:	97		98.95%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	96		97.95%
Employees who know who their CPP Liaison is:	90		91.8%
Employees who back up all information they deem important to their work:	96		97.95%
Employees who have an LBLnet-approved connection on their wireless network equipment:	95		96.9%

Computing Sciences Directorate Information

Division Director:	None identified		
ISSM Liaison:	Ramsey, Dwayne		
CPP Liaisons:	Manders, Chris J.		
Security Access Managers:	Dooly, Martin K.		
Employees in Division (as surveyed):	21		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	13		87.05%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	13		100%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	11		84.6%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	13		100%
Employees who know whom to contact regarding keys to their office or building:	13		100%
Employees who take appropriate measures to secure the property assigned to them:	13		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	12		92.3%
Employees who know how to request visitor access:	12		92.3%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	12		92.3%
Employees who are familiar with export controls at Berkeley Lab:	12		92.3%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	12		100%
Employees who know the Lab's legal requirements for obtaining software:	13		100%
Employees who change their passwords according to the LBNL password policy:	11		84.6%
Employees who are aware of how to protect their computer against viruses:	13		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	13		100%
Employees who know who their CPP Liaison is:	13		100%
Employees who back up all information they deem important to their work:	13		100%
Employees who have an LBLnet-approved connection on their wireless network equipment:	12		92.3%

Environmental Energy Technologies Division Information

Division Director:	Levine, Mark D.		
ISSM Liaison:	Lucas, Donald		
CPP Liaisons:	Revzan, Kenneth L.		
Security Access Managers:	Cordell-Breckinridge, Joyce D.		
Employees in Division (as surveyed):	220		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	198		90%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	180		90.9%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	162		81.8%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	193		97.45%
Employees who know whom to contact regarding keys to their office or building:	178		89.9%
Employees who take appropriate measures to secure the property assigned to them:	195		98.45%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	166		83.8%
Employees who know how to request visitor access:	195		98.45%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	166		83.8%
Employees who are familiar with export controls at Berkeley Lab:	151		76.25%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	163		82.3%
Employees who know the Lab's legal requirements for obtaining software:	188		96.45%
Employees who change their passwords according to the LBNL password policy:	109		57.05%
Employees who are aware of how to protect their computer against viruses:	194		99.45%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	188		96.45%
Employees who know who their CPP Liaison is:	162		82.8%
Employees who back up all information they deem important to their work:	191		96.45%
Employees who have an LBLnet-approved connection on their wireless network equipment:	198		100%

Engineering Division Information

Division Director:	Robinson, Kem Edward		
ISSM Liaison:	Wong, Weyland		
CPP Liaisons:	Lawrence, Charles E.		
Security Access Managers:	Luke, Paul N. Palaio, Nicholas P. Wong, Weyland		
Employees in Division (as surveyed):	305		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	284		92%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	280		98.55%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	246		86.6%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	269		94.7%
Employees who know whom to contact regarding keys to their office or building:	280		98.55%
Employees who take appropriate measures to secure the property assigned to them:	283		99.65%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	239		84.15%
Employees who know how to request visitor access:	279		98.2%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	259		91.2%
Employees who are familiar with export controls at Berkeley Lab:	234		82.35%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	251		88.35%
Employees who know the Lab's legal requirements for obtaining software:	257		91.9%
Employees who change their passwords according to the LBNL password policy:	256		90.45%
Employees who are aware of how to protect their computer against viruses:	275		97.85%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	271		96.45%
Employees who know who their CPP Liaison is:	242		86.25%
Employees who back up all information they deem important to their work:	252		90.45%
Employees who have an LBLnet-approved connection on their wireless network equipment:	284		100%

Environment, Health & Safety Division Information

Division Director:	Pei, Phyllis C.		
ISSM Liaison:	Lunsford, Dan S.		
CPP Liaisons:	Abraham, Stephen B. Lunsford, Dan S.		
Security Access Managers:	Floyd, James G. Grondona, Connie E. Rothermich, Nancy E. Sohner, Stephen L. Wong, June J.		
Employees in Division (as surveyed):	108		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	108		100%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	108		100%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	100		92.55%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	101		93.5%
Employees who know whom to contact regarding keys to their office or building:	107		99.05%
Employees who take appropriate measures to secure the property assigned to them:	108		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	97		89.8%
Employees who know how to request visitor access:	107		99.05%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	103		95.35%
Employees who are familiar with export controls at Berkeley Lab:	84		77.75%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	95		87.95%
Employees who know the Lab's legal requirements for obtaining software:	95		89.8%
Employees who change their passwords according to the LBNL password policy:	83		80.55%
Employees who are aware of how to protect their computer against viruses:	100		95.35%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	98		93.5%
Employees who know who their CPP Liaison is:	91		87%
Employees who back up all information they deem important to their work:	92		88.85%
Employees who have an LBLnet-approved connection on their wireless network equipment:	108		100%

Earth Sciences Division Information

Division Director:	Bodvarsson, Gudmundur S.		
ISSM Liaison:	Villavert, Maryann		
CPP Liaisons:	Lau, Peter K. Taylor, Bryan E.		
Security Access Managers:	Hazen, Terry C. Villavert, Maryann		
Employees in Division (as surveyed):	166		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	136		82%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	131		96.3%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	122		89.7%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	135		99.25%
Employees who know whom to contact regarding keys to their office or building:	133		97.75%
Employees who take appropriate measures to secure the property assigned to them:	134		98.5%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	117		86%
Employees who know how to request visitor access:	132		97.75%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	126		93.35%
Employees who are familiar with export controls at Berkeley Lab:	112		83.05%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	115		85.25%
Employees who know the Lab's legal requirements for obtaining software:	125		93.35%
Employees who change their passwords according to the LBNL password policy:	96		72.05%
Employees who are aware of how to protect their computer against viruses:	135		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	129		96.3%
Employees who know who their CPP Liaison is:	123		91.9%
Employees who back up all information they deem important to their work:	132		98.5%
Employees who have an LBLnet-approved connection on their wireless network equipment:	135		99.25%

Facilities Division Information

Division Director:	Reyes, George D.		
ISSM Liaison:	Pon, John		
CPP Liaisons:	Huynh, Chinh Pon, John		
Security Access Managers:	Berninzoni, Robert A. Llewellyn, William E. McPherson, David L. Murphy, James W. Reese Jr., Thomas A. Rosas, George A. Trigales, Kevin P. Weber, Donald F. Wu, William H.		
Employees in Division (as surveyed):	224		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	192		86%
	Employee Responses	**Rating**	**% Complete Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	191		99.45%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	183		95.3%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	186		96.85%
Employees who know whom to contact regarding keys to their office or building:	190		98.95%
Employees who take appropriate measures to secure the property assigned to them:	192		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	171		89.05%
Employees who know how to request visitor access:	191		99.45%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	189		98.4%
Employees who are familiar with export controls at Berkeley Lab:	176		91.65%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	174		90.6%
Employees who know the Lab's legal requirements for obtaining software:	161		95.3%
Employees who change their passwords according to the LBNL password policy:	154		92.15%
Employees who are aware of how to protect their computer against viruses:	165		98.95%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	157		96.35%
Employees who know who their CPP Liaison is:	164		97.9%
Employees who back up all information they deem important to their work:	162		97.4%
Employees who have an LBLnet-approved connection on their wireless network equipment:	192		100%

Genomics Division Information

Division Director:	Rubin, Edward M.		
ISSM Liaison:	None identified		
CPP Liaisons:	None identified		
Security Access Managers:	None identified		
Employees in Division (as surveyed):	85		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	62		76%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	59		95.15%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	53		85.45%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	62		100%
Employees who know whom to contact regarding keys to their office or building:	62		100%
Employees who take appropriate measures to secure the property assigned to them:	62		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	47		75.8%
Employees who know how to request visitor access:	60		96.75%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	57		91.9%
Employees who are familiar with export controls at Berkeley Lab:	55		88.7%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	55		88.7%
Employees who know the Lab's legal requirements for obtaining software:	57		93.55%
Employees who change their passwords according to the LBNL password policy:	34		56.45%
Employees who are aware of how to protect their computer against viruses:	60		96.75%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	57		95.15%
Employees who know who their CPP Liaison is:	52		87.1%
Employees who back up all information they deem important to their work:	55		91.9%
Employees who have an LBLnet-approved connection on their wireless network equipment:	61		98.35%

Information Technologies & Services Division Information

Division Director:	Merola, Alexander X.		
ISSM Liaison:	Ramsey, Dwayne		
CPP Liaisons:	Balin, Greg A. Early, Alfred E. Klinedinst, Dan Manders, Chris J.		
Security Access Managers:	Dooly, Martin K. Pon, John		
Employees in Division (as surveyed):	203		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	196		97%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	192		97.95%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	177		90.3%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	192		97.95%
Employees who know whom to contact regarding keys to their office or building:	188		95.9%
Employees who take appropriate measures to secure the property assigned to them:	195		99.45%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	164		83.65%
Employees who know how to request visitor access:	194		98.95%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	180		91.8%
Employees who are familiar with export controls at Berkeley Lab:	163		83.15%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	178		90.8%
Employees who know the Lab's legal requirements for obtaining software:	185		94.35%
Employees who change their passwords according to the LBNL password policy:	158		80.6%
Employees who are aware of how to protect their computer against viruses:	195		9.459%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	196		100%
Employees who know who their CPP Liaison is:	191		97.45%
Employees who back up all information they deem important to their work:	193		98.45%
Employees who have an LBLnet-approved connection on their wireless network equipment:	196		100%

Laboratory Directorate Information

Division Director:	Oddone, Piermaria J.		
ISSM Liaison:	Baynes, Jane H.		
CPP Liaisons:	Tallarico, Nancy J.		
Security Access Managers:	Magee, Janice A.		
Employees in Division (as surveyed):	65		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	48		84%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	47		97.9%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	43		89.55%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	48		100%
Employees who know whom to contact regarding keys to their office or building:	46		95.8%
Employees who take appropriate measures to secure the property assigned to them:	47		97.9%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	41		85.4%
Employees who know how to request visitor access:	45		93.75%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	42		87.5%
Employees who are familiar with export controls at Berkeley Lab:	41		85.4%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	42		87.5%
Employees who know the Lab's legal requirements for obtaining software:	42		87.5%
Employees who change their passwords according to the LBNL password policy:	40		83.3%
Employees who are aware of how to protect their computer against viruses:	48		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	47		97.9%
Employees who know who their CPP Liaison is:	45		93.75%
Employees who back up all information they deem important to their work:	45		93.75%
Employees who have an LBLnet-approved connection on their wireless network equipment:	48		100%

Life Sciences Division Information

Division Director:	Gray, Joe W.		
ISSM Liaison:	Guagliardo, Francesca		
CPP Liaisons:	Boswell, Martin S. Huesman, Ronald H.		
Security Access Managers:	Blakely, Eleanor A. Linard, Anthony M. O'Neil, James P. Rydberg, Bjorn E. Torok, Tamas		
Employees in Division (as surveyed):	303		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	280		92%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	266		95%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	239		85.35%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	269		96.05%
Employees who know whom to contact regarding keys to their office or building:	268		95.7%
Employees who take appropriate measures to secure the property assigned to them:	274		97.85%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	232		82.85%
Employees who know how to request visitor access:	263		93.9%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	237		84.6%
Employees who are familiar with export controls at Berkeley Lab:	212		75.7%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	222		79.25%
Employees who know the Lab's legal requirements for obtaining software:	242		87.85%
Employees who change their passwords according to the LBNL password policy:	124		49%
Employees who are aware of how to protect their computer against viruses:	270		97.1%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	254		91.4%
Employees who know who their CPP Liaison is:	210		75.7%
Employees who back up all information they deem important to their work:	257		93.2%
Employees who have an LBLnet-approved connection on their wireless network equipment:	279		99.6%

Materials Sciences Division Information

Division Director:	Alivisatos, Paul A.		
ISSM Liaison:	Ager, Joel W. Mitchell, Wayne G.		
CPP Liaison:	Tackaberry, Ron E.		
Security Access Managers:	Cavlina, Jane L. Saiz, Eduardo		
Employees in Division (as surveyed):	196		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	174		89%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	3		1.7%
Employees who know the emergency phone number for the Laboratory:	162		93.1%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	143		82.15%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	171		98.25%
Employees who know whom to contact regarding keys to their office or building:	164		94.25%
Employees who take appropriate measures to secure the property assigned to them:	171		98.25%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	146		83.9%
Employees who know how to request visitor access:	163		93.65%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	140		80.45%
Employees who are familiar with export controls at Berkeley Lab:	133		76.4%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	138		79.3%
Employees who know the Lab's legal requirements for obtaining software:	146		86.75%
Employees who change their passwords according to the LBNL password policy:	72		44.25%
Employees who are aware of how to protect their computer against viruses:	166		98.25%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	154		91.35%
Employees who know who their CPP Liaison is:	127		75.85%
Employees who back up all information they deem important to their work:	154		91.35%
Employees who have an LBLnet-approved connection on their wireless network equipment:	172		98.85%

NERSC Division Information

Division Director:	Simon, Horst D.		
ISSM Liaison:	Ramsey, Dwayne		
CPP Liaison:	Campbell, Scott Lau Jr., Stephen		
Security Access Managers:	Dooly, Martin K.		
Employees in Division (as surveyed):	69		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	59		89%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	58		98.3%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	53		89.8%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	59		100%
Employees who know whom to contact regarding keys to their office or building:	57		96.6%
Employees who take appropriate measures to secure the property assigned to them:	59		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	47		79.65%
Employees who know how to request visitor access:	58		98.15%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	57		96.6%
Employees who are familiar with export controls at Berkeley Lab:	53		89.8%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	58		98.3%
Employees who know the Lab's legal requirements for obtaining software:	58		98.3%
Employees who change their passwords according to the LBNL password policy:	55		93.2%
Employees who are aware of how to protect their computer against viruses:	59		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	59		100%
Employees who know who their CPP Liaison is:	56		94.9%
Employees who back up all information they deem important to their work:	59		100%
Employees who have an LBLnet-approved connection on their wireless network equipment:	59		100%

Nuclear Science Division Information

Division Director:	Symons, Timothy J.		
ISSM Liaison:	Mitschang, Linda F.		
CPP Liaison:	Matis, Howard S.		
Security Access Managers:	Kono, Joy N. Norris, Margaret A.		
Employees in Division (as surveyed):	120		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	99		82.5%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	94		94.95%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	77		77.75%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	97		97.95%
Employees who know whom to contact regarding keys to their office or building:	89		89.9%
Employees who take appropriate measures to secure the property assigned to them:	98		98.95%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	83		83.8%
Employees who know how to request visitor access:	95		95.95%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	75		75.75%
Employees who are familiar with export controls at Berkeley Lab:	70		70.7%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	76		76.75%
Employees who know the Lab's legal requirements for obtaining software:	81		82.8%
Employees who change their passwords according to the LBNL password policy:	65		66.65%
Employees who are aware of how to protect their computer against viruses:	95		96.95%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	92		94.95%
Employees who know who their CPP Liaison is:	75		76.75%
Employees who back up all information they deem important to their work:	92		93.9%
Employees who have an LBLnet-approved connection on their wireless network equipment:	99		100%

Operations Information

Division Director:	Benson, Sally M.		
ISSM Liaison:	Baynes, Jane H.		
CPP Liaison:	Tallarico, Nancy J.		
Security Access Managers:	Magee, Janice A.		
Employees in Division (as surveyed):	28		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	22		79.5%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	22		100%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	17		77.25%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	21		95.45%
Employees who know whom to contact regarding keys to their office or building:	20		90.15%
Employees who take appropriate measures to secure the property assigned to them:	22		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	19		86.35%
Employees who know how to request visitor access:	21		95.45%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	19		86.35%
Employees who are familiar with export controls at Berkeley Lab:	19		86.35%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	19		86.35%
Employees who know the Lab's legal requirements for obtaining software:	20		90.9%
Employees who change their passwords according to the LBNL password policy:	16		72.7%
Employees who are aware of how to protect their computer against viruses:	22		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	21		95.45%
Employees who know who their CPP Liaison is:	19		86.35%
Employees who back up all information they deem important to their work:	22		100%
Employees who have an LBLnet-approved connection on their wireless network equipment:	21		95.45%

Physical Biosciences Division Information

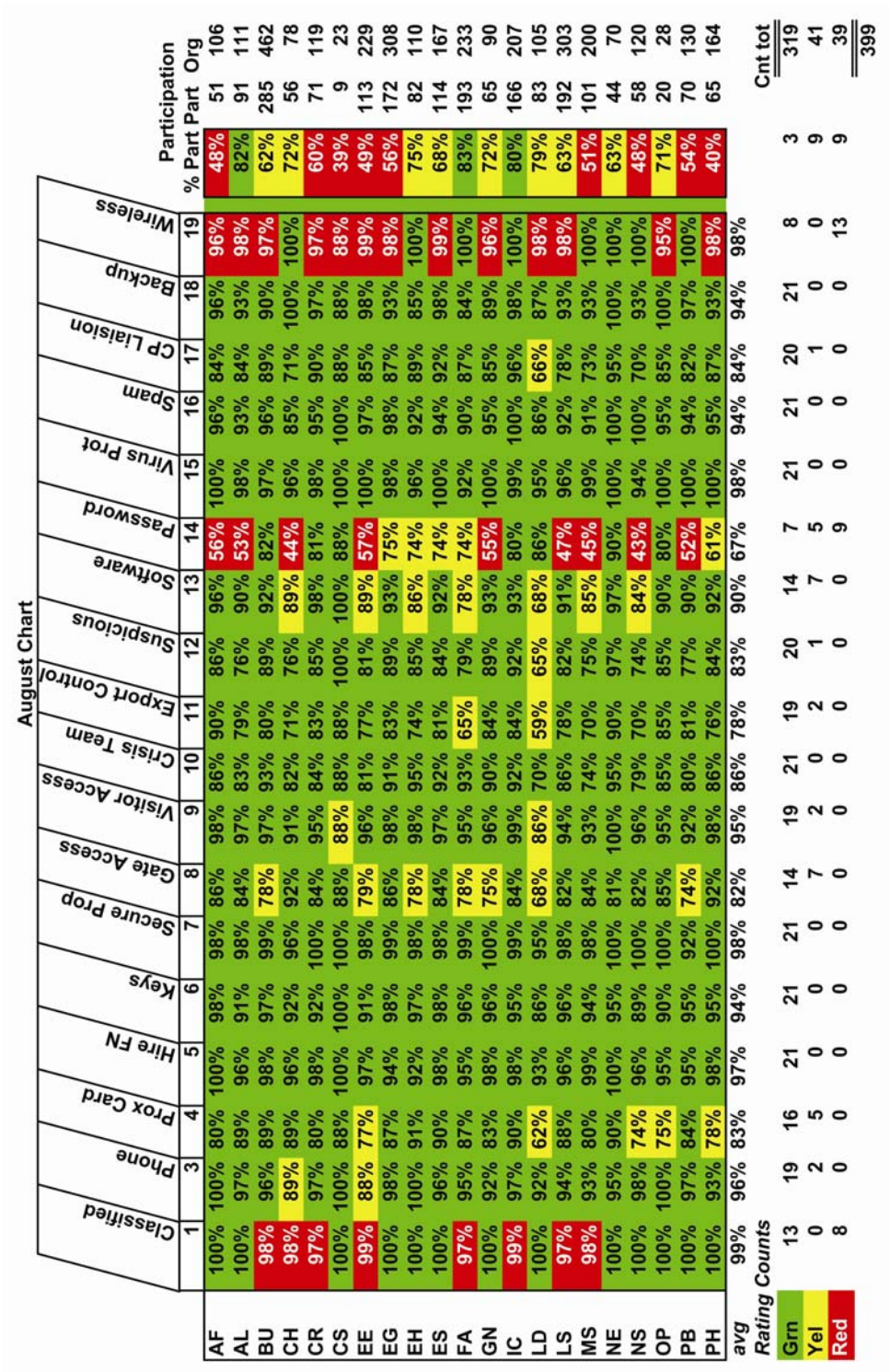
Division Director:	Fleming, Graham R.		
ISSM Liaison:	Pelton, Jeffrey G.		
CPP Liaison:	Grosse-Kunstleve, Ralf Wilhelm		
Security Access Managers:	Berry, Edward A. Ford, Ellen		
Employees in Division (as surveyed):	127		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	93		74%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	90		96.75%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	82		88.15%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	91		97.85%
Employees who know whom to contact regarding keys to their office or building:	90		96.75%
Employees who take appropriate measures to secure the property assigned to them:	87		93.55%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	71		76.3%
Employees who know how to request visitor access:	88		94.6%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	78		83.85%
Employees who are familiar with export controls at Berkeley Lab:	79		84.95%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	78		83.85%
Employees who know the Lab's legal requirements for obtaining software:	85		92.45%
Employees who change their passwords according to the LBNL password policy:	52		55.9%
Employees who are aware of how to protect their computer against viruses:	91		100%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	89		95.7%
Employees who know who their CPP Liaison is:	76		82.8%
Employees who back up all information they deem important to their work:	90		97.85%
Employees who have an LBLnet-approved connection on their wireless network equipment:	93		100%

Physics Division Information

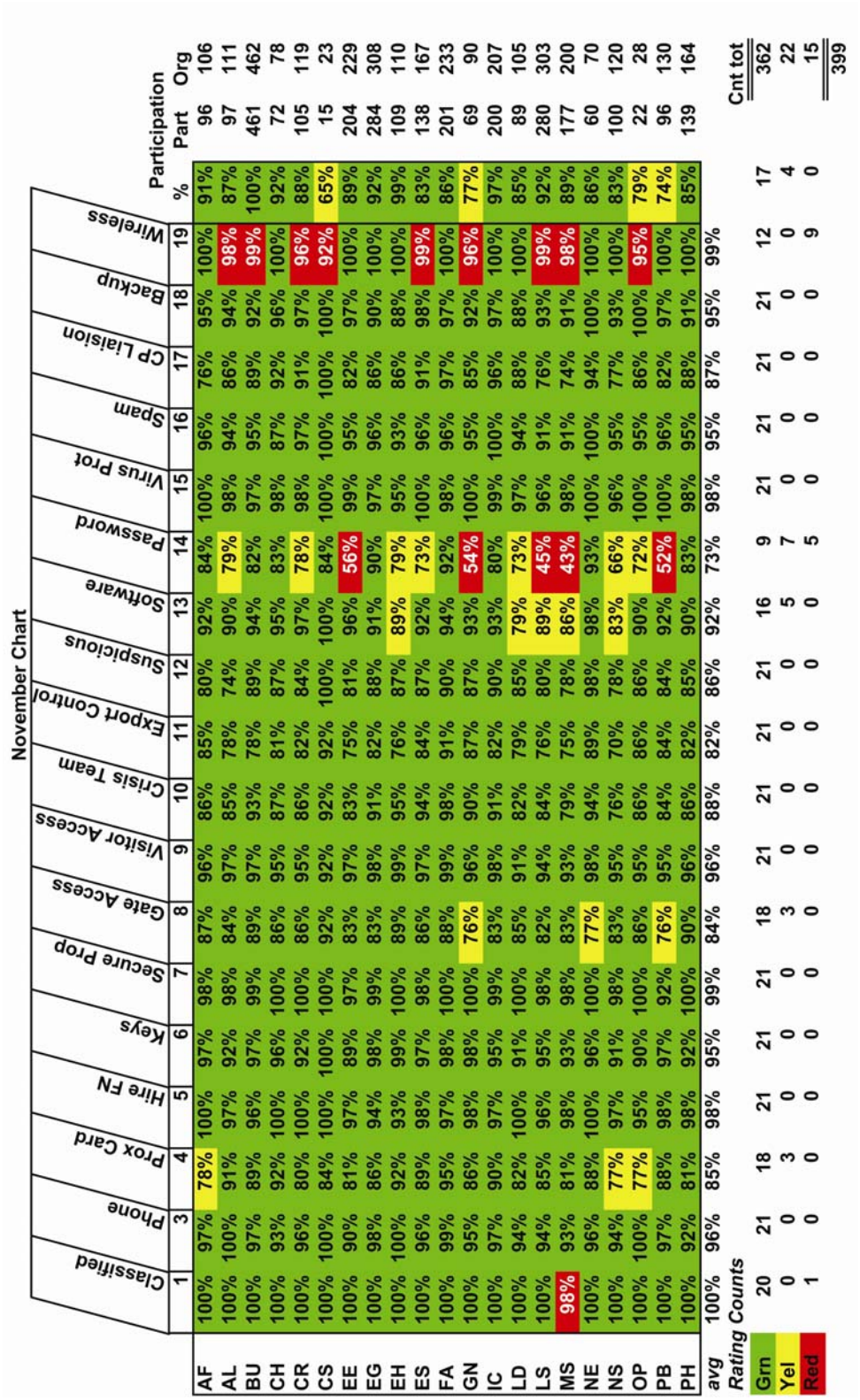
Division Director:	Siegrist, James L.		
ISSM Liaison:	Mitschang, Linda F.		
CPP Liaison:	Ciocio, Alessandra		
Security Access Managers:	Kono, Joy N.		
Employees in Division (as surveyed):	162		
Results of Survey Questions			
	Employee Responses	**Rating**	**% Division Employees**
Employees in Division who have completed the Self-Assessment Questionnaire:	137		85%
	Employee Responses	**Rating**	**% Completed Survey**
Employees who work with Classified Information at LBNL:	0		100%
Employees who know the emergency phone number for the Laboratory:	126		91.95%
Employees who know how to find the list of building authorizers if access is required to a proximity card-enabled building:	111		81%
Employees who know where to find information on special processing requirements if they hire an employee or host a guest from a sensitive or terrorist sponsoring country to perform work or research at the Lab:	135		98.5%
Employees who know whom to contact regarding keys to their office or building:	128		93.4%
Employees who take appropriate measures to secure the property assigned to them:	137		100%
Employees who are aware of the LBNL requirements for gate access during normal work hours and at night and on weekends:	122		89.05%
Employees who know how to request visitor access:	132		96.35%
Employees who are aware of the Crisis Action Team and know whom to contact regarding workplace violence issues:	118		86.1%
Employees who are familiar with export controls at Berkeley Lab:	110		80.25%
Employees who know how to report inappropriate inquiries or incidents they suspect involve foreign intelligence collection efforts or terrorists targeting activity against the Berkeley Lab:	117		85.4%
Employees who know the Lab's legal requirements for obtaining software:	120		90.5%
Employees who change their passwords according to the LBNL password policy:	112		84.65%
Employees who are aware of how to protect their computer against viruses:	131		98.5%
Employees who are aware of the Lab's process to reduce unsolicited e-mail (spam):	126		94.85%
Employees who know who their CPP Liaison is:	118		89.05%
Employees who back up all information they deem important to their work:	123		92.7%
Employees who have an LBLnet-approved connection on their wireless network equipment:	137		100%

APPENDIX F: INSTITUTIONAL PROFILES

Phase One



Phase Two



November Chart

	1 Classified	3 Phone	4 Prox Card	5 Hire FN	6 Keys	7 Secure Prop	8 Gate Access	9 Visitor Access	10 Crisis Team	11 Export Control	12 Suspicious	13 Software	14 Password	15 Virus Prot	16 Spam	17 CP Liaison	18 Backup	19 Wireless	Participation %	Part	Org	Cnt tot
AF	100%	97%	78%	100%	97%	98%	87%	96%	86%	85%	80%	92%	84%	100%	96%	76%	95%	100%	91%	96	106	362
AL	100%	100%	91%	97%	92%	98%	84%	97%	85%	78%	74%	90%	79%	98%	94%	86%	94%	98%	87%	97	111	
BU	100%	97%	89%	96%	97%	99%	89%	97%	93%	78%	89%	94%	82%	97%	95%	89%	92%	99%	100%	461	462	22
CH	100%	93%	92%	100%	96%	100%	86%	95%	87%	81%	87%	95%	83%	98%	87%	92%	96%	100%	92%	72	78	
CR	100%	96%	80%	100%	92%	100%	86%	95%	86%	82%	84%	97%	78%	98%	97%	91%	97%	96%	88%	105	119	15
CS	100%	100%	84%	100%	100%	100%	92%	92%	92%	92%	100%	100%	84%	100%	100%	100%	100%	92%	65%	15	23	
EE	100%	90%	81%	97%	89%	97%	83%	97%	83%	75%	81%	96%	56%	99%	95%	82%	97%	100%	89%	204	229	399
EG	100%	98%	86%	94%	98%	99%	83%	98%	91%	82%	88%	91%	90%	97%	96%	86%	90%	100%	92%	284	308	
EH	100%	100%	92%	93%	99%	100%	89%	99%	95%	76%	87%	89%	79%	95%	93%	86%	88%	100%	99%	109	110	
ES	100%	96%	89%	98%	97%	98%	86%	97%	94%	84%	87%	92%	73%	100%	96%	91%	98%	99%	83%	138	167	
FA	100%	99%	95%	97%	98%	100%	88%	99%	98%	91%	90%	94%	92%	98%	96%	97%	97%	100%	86%	201	233	
GN	100%	95%	86%	98%	98%	100%	76%	96%	90%	87%	87%	93%	54%	100%	95%	85%	92%	96%	77%	69	90	
IC	100%	97%	90%	97%	95%	99%	83%	98%	91%	82%	90%	93%	80%	99%	100%	96%	97%	100%	97%	200	207	
LD	100%	94%	82%	100%	91%	100%	85%	91%	82%	79%	85%	79%	73%	97%	94%	88%	88%	100%	85%	89	105	
LS	100%	94%	85%	96%	95%	98%	82%	94%	84%	76%	80%	89%	45%	96%	91%	76%	93%	99%	92%	280	303	
MS	98%	93%	81%	98%	93%	98%	83%	93%	79%	75%	78%	86%	43%	98%	91%	74%	91%	98%	89%	177	200	
NE	100%	96%	88%	100%	96%	100%	77%	98%	94%	89%	98%	98%	93%	100%	100%	94%	100%	100%	86%	60	70	
NS	100%	94%	77%	97%	91%	98%	83%	95%	76%	70%	78%	83%	66%	96%	95%	77%	93%	100%	83%	100	120	
OP	100%	100%	77%	95%	90%	100%	86%	95%	86%	86%	86%	90%	72%	100%	95%	86%	100%	95%	79%	22	28	
PB	100%	97%	88%	98%	97%	92%	76%	95%	84%	84%	84%	92%	52%	100%	96%	82%	97%	100%	74%	96	130	
PH	100%	92%	81%	98%	92%	100%	90%	96%	86%	82%	85%	90%	83%	98%	95%	88%	91%	100%	85%	139	164	
avg	100%	96%	85%	98%	95%	99%	84%	96%	88%	82%	86%	92%	73%	98%	95%	87%	95%	99%				

Rating Counts

	20	21	18	21	21	21	18	21	21	21	21	16	9	21	21	21	21	12	17
Grn	0	0	3	0	0	0	3	0	0	0	0	5	7	0	0	0	0	0	4
Yel	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	9	0
Red	1	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0

APPENDIX G: 2003 & 2004 STATISTICAL DATA

Government Thefts by Division

DIVISION	2003	2004
AFRD	1	
ALS		1
ASD	1	
Business Services		1
Directorate	1	1
Earth Sciences		3
EH&S	2	
Engineering	2	
Facilities	3	
ITSD	1	1
Life Sciences	5	
Materials Sciences	1	1
NERSC		1
Nuclear Science		1
Physical Biosciences	3	3
Physics	1	
Total	**21**	**13**

2003 LBNL Cyber Security Incident Summary

DIV	Root compromise	Account compromise	Malicious code	Improper use	Other	Total
AFRD	2		14	11		27
ALS	2		61	46	1	110
ASD			4	3		7
CFO			7	2		9
CRD	3		8	7	2	20
CSD			9	2		11
DIRC			8	16		24
EET			26	30	1	57
EH&S			10	8		18
ENG	2	1	49	21		73
ESD			17	7	2	26
ESNET	1		2			3
FCLT			6	3		9
HR			3	5		8
ISS		1	1	2		4
ITSD	2		19	13		34
JGI	1		1	1		3
LSD			61	43		104
MSD	2		42	27	1	72
NERSC	2		6	2		10
NSD			12	16		28
NTD	1	1	20			22
PB			24	24	1	49
PHYS	1		16	8		25
unknown			19	12		31
Total	19	3	445	309	8	784

Root Compromise An attacker broke into and gained full control over a computer.

Account Compromise An attacker broke into a computer, but their access on the computer was restricted.

Malicious Code A computer became infected with a worm, virus, Trojan horse, or other malicious program.

Improper Use The owner of the computer was detected using Lab computing resources for uses that are unacceptable per Lab policy.

Other There are a number of incident types that are rarely seen. These are all grouped under 'other.' They include, but are not limited to, Lab computers used as e-mail spam servers, users logging into their computer with a clear text password, ftp servers co-opted by attackers for use as storage space.

2004 LBNL Cyber Security Incident Summary

DIV	Root compromise	Account compromise	Malicious code	Improper use	Other	Total
AFRD			18	4		22
ALS			40	22		62
ASD			7	4		11
CFO			41	1		42
COMP	16		3			19
CRD	2		7	5	1	15
CSD	1	1	8	4		14
DIRC			20	4		24
EET	2		42	3	2	49
EH&S			28	6		34
ENG	14		87	8	2	111
ESD	4	1	37	7	2	51
ESNET	1			1		2
FCLT	2		59	12		73
HR			21	4		25
ISS			1			1
ITSD			15	5	2	22
JGI			7	4		11
LSD	11	1	42	25	3	82
MSD			41	12		53
NERSC		10	10			20
NSD	1	3	10	10		24
NTD			6	2		8
PB	2		28	12		42
PHYS	21	4	11	6		42
unknown	1		10	8		19
Total	78	20	599	169	12	878

Root Compromise An attacker broke into and gained full control over a computer.

Account Compromise An attacker broke into a computer, but their access on the computer was restricted.

Malicious Code A computer became infected with a worm, virus, Trojan horse, or other malicious program.

Improper Use The owner of the computer was detected using Lab computing resources for uses that are unacceptable per Lab policy.

Other There are a number of incident types that are rarely seen. These are all grouped under 'other.' They include, but are not limited to, Lab computers used as e-mail spam servers, users logging into their computer with a clear text password, ftp servers co-opted by attackers for use as storage space.

DISCLAIMER

This work was supported by the Director, Office of Science, of the U.S. Department of Energy under Contract No. DE-AC03-76SF00098.